УТВЕРЖДАЮ
Генеральный директор
ООО «Автолицей Автокурс»
ИНН 7727467182

_____К.Ю. Боровик

М.П.

Пр.№ 01 от 10.01.2025 г.

ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ОПЕРАТОРА (ООО «Автолицей Автокурс»)

Москва 2025

ОГЛАВЛЕНИЕ:

ВВЕДЕНИЕ

Политика обработки персональных данных (далее, - Политика) разработана оператором – обществом ограниченной ответственности «Автолицей Автокурс» (сокращенное наименование ООО «Автолицей Автокурс») ИНН 7727467182 ОГРН 1217700273560 (далее, – «Общество») в соответствие с Федеральным законом «О персональных данных», Трудовым кодексом Российской Федерации, Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Правилами внутреннего трудового распорядка Общества.

В силу ст. 3 Федерального закона № 152 – ФЗ «О персональных данных», Общество является оператором персональных данных, принадлежащих субъектам персональных данных, с которыми, Общество взаимодействует по роду своей деятельности.

Настоящая Политика в отношении обработки персональных данных:

— определяет цели, перечни и категории обрабатываемых данных и субъектов данных, способы, сроки их обработки и хранения, а также порядок уничтожения данных в случаях, когда Общество обрабатывает персональные данные;

— разъясняет принципы обработки персональных данных Обществом как Оператором, права и обязанности при обработке данных, права субъектов данных, а также включает перечень мер по обеспечению безопасности персональных данных при их обработке с целью защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;

— является документом, декларирующим концептуальные основы деятельности Оператора (Общества) при обработке и защите персональных данных.

Политика содержит отдельные положения по обработке персональных данных выделенных субъектов: работников; контрагентов; третьих лиц.

Политика является общедоступной и подлежит размещению на официальном веб-сайте Общества, или иным образом обеспечивается неограниченный доступ к настоящему документу.

I. ОСНОВНЫЕ ПОНЯТИЯ ПОЛИТИКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Понятия, используемые в политике обработки персональных данных определяются в соответствии Федеральным законом № 152 – ФЗ «О персональных данных»:

— персональные данные (сокращенно, - ПДн) – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

— субъект персональных данных — это физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных;

— персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;

— 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;

— 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;

— автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

— распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

— предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

— конфиденциальность персональных данных - обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным работников, требование не допускать их распространения без согласия работника или иного законного основания;

— использование персональных данных - действия (операции) с персональными данными, совершаемые должностным лицом Организации в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

— блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных работников, в том числе их передачи;

— уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных работников или в результате которых уничтожаются материальные носители персональных данных работников;

— обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному работнику;

— общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

— информация - сведения (сообщения, данные) независимо от формы их представления[2];

— документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель;

— информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

— трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

— контрагент – физическое лицо, официальный представитель – физическое лицо юридического лица и/или индивидуального предпринимателя, вступившее в договорные отношения с Обществом;

— персональные данные Контрагента – персональные данные, необходимые Оператору в связи с исполнением договорных отношений и касающаяся конкретного Контрагента, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, образование, профессия (должность), номер контактного телефона, адрес электронной почты;

— защита персональных данных – это деятельность уполномоченных лиц Общества по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер конфиденциальности информации о конкретном физическом лице;

— конфиденциальность персональных данных – обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать их распространения и передачи третьим лицам без согласия субъекта персональных данных или наличия иного законного основания;

— персональные данные третьих лиц (далее - персональные данные) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

— обработка персональных данных третьих лиц – это любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными третьих лиц, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

— под угрозой или опасностью (или риском угрозы) утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

II. ОСНОВНЫЕ ПРАВА И ОБЯЗАННОСТИ ОПЕРАТОРА И СУБЪЕКТАПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. При взаимодействии между оператором персональных данных и субъектом персональных данных, их права и обязанности, определяются в соответствие с требованиями, установленными Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных».Вышеназванный закон устанавливает запрет на принятие решений оператором, которые приводят к негативным правовым последствиям в отношении субъекта персональных данных. На оператора накладывается обязательство сразу прекратить использование сведений о персональных данных, если субъект подает соответствующий запрос. При наличии обоснованных подозрений, что используемые сведения неполные, ошибочные либо получены незаконным способом субъект ПДн вправе потребовать их немедленной блокировки и уничтожения в предусмотренные действующим законодательством сроки. В этой связи, основные права и обязанности оператора и субъекта персональных данных с учетом требований закона определены следующим.

2.2. Права и обязанности Оператора при взаимодействии с персональными данными субъекта.

2.2.1. Оператор при сборе персональных данных обязан предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его персональных данных в том числе:

— разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные;

— обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Федеральном законе «О персональных данных»;

— принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами в отношении Оператора;

— опубликовать или иным образом обеспечить неограниченный доступ к настоящей Политике, к сведениям о реализуемых требованиях к защите персональных данных. Оператор в случае осуществления сбора персональных данных с использованием информационно-телекоммуникационных сетей обязан опубликовать в соответствующей информационно-телекоммуникационных сетях Политику и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием соответствующих информационно-телекоммуникационных сетях;

— принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

— вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора;

— лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных».;

— в поручении Оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

2.3. Права и обязанности Субъекта при взаимодействии с персональными данными Оператора.

2.3.1. Субъект персональных данных вправе требовать от Оператора:

— уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

— обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных;

— принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы разрешается только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных;

— если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

— Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;

— Субъект персональных данных обязан предоставлять Оператору достоверные персональные данные.

III. СБОР, ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Оператор обрабатывает персональные данные субъекта для:

– оформления трудовых отношений, ведения кадрового делопроизводства, содействия в трудоустройстве, обучении, повышении по службе, пользовании различными льготами и гарантиями, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и сохранности имущества;

— заключения, исполнения и прекращения гражданско-правовых договоров/сделок;

— выполнения требований действующего законодательства;

— иных случаев, установленных в законе, уставе Оператора.

3.2. Обработка персональных данных должна осуществляться на законной и справедливой основе.

3.3. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.4. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.5. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

3.6. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

3.7. Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных.

3.8. Оператор обрабатывает персональные данные на основании:

— Закона о персональных данных и принятых на его основе нормативных правовых актов, регулирующих отношения, связанные с обработкой персональных данных;

— Трудового кодекса Российской Федерации;

— Гражданского кодекса Российской Федерации;

— иных федеральных законов и прочих нормативных правовых актов;

— устава Оператора;

— договоров, заключаемых между Оператором и контрагентами

— субъектами персональных данных;

— согласий на обработку персональных данных;

— согласий на обработку персональных данных, разрешенных субъектом для распространения.

3.9. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении 75 лет срока их хранения, или продлевается на основании заключения экспертной комиссии Общества, если иное не определено законом.

IV. КАТЕГОРИИ СУБЪЕКТОВ И ОБЪЕМ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Субъекты, чьи персональные данные обрабатываются Оператором (Обществом), подразделяются на следующие категории:

4.1.1. Работники Оператора, бывшие работники, кандидаты на трудоустройство (далее – работники), а также члены семей указанных лиц.

4.1.2. Участвующие в мероприятиях (процессах), организуемых Оператором, их законные представители.

4.1.3. Контрагенты Оператора (физические лица).

4.1.4. Представители/работники контрагентов Оператора (юридических лиц).

4.2. Объем обрабатываемых персональных данных включает в себя:

4.2.1. В отношении работников (за исключением членов семей) обрабатываются:

— фамилия, имя, отчество;

— дата рождения;

— место рождения;

— адрес регистрации;

— адрес фактического места жительства;

— гражданство;

— серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;

— образование, квалификация;

— серия и номер документа об образовании/квалификации, сведения о выдаче указанного документа и выдавшем его образовательном учреждении;

— сведения о повышении квалификации, о профессиональной переподготовке; − сведения о трудовой деятельности;

— профессия, должность;

— стаж работы;

— сведения о семейном положении, наличии детей;

— данные страхового свидетельства государственного пенсионного страхования; − идентификационный номер налогоплательщика;

— сведения о доходах (за 2 предыдущих года для расчета пособий);

— сведения о воинском учете;

— сведения о наградах (поощрениях), почетных званиях;

— сведения о социальных гарантиях;

— сведения о состоянии здоровья, влияющие на выполнение трудовой функции;

— банковские реквизиты счета;

— сведения о заработной плате;

— содержание трудового договора;

— контактный телефон;

— адрес электронной почты.

4.2.2. Персональные данные членов семей работников обрабатываются в объеме, переданном работником и необходимом для предоставления гарантий и компенсаций работнику, предусмотренных трудовым законодательством:

— фамилия, имя, отчество;

— дата рождения;

— место рождения;

— серия и номер документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;

— серия и номер свидетельства о рождении ребенка, сведения о выдаче указанного документа и выдавшем его органе;

— серия и номер свидетельства о заключении брака, сведения о выдаче указанного документа и выдавшем его органе.

4.2.3. В отношении участвующих в мероприятиях, организуемых Оператором, обрабатываются:

— фамилия, имя, отчество;

— дата рождения;

— место рождения;

— адрес регистрации;

— адрес фактического места жительства;

— гражданство;

— серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;

— серия и номер свидетельства о рождении ребенка, сведения о выдаче указанного документа и выдавшем его органе (для несовершеннолетних, не достигших 14 лет);

— серия и номер документа об образовании/квалификации, сведения о выдаче указанного документа и выдавшем его образовательном учреждении;

— данные страхового свидетельства государственного пенсионного страхования;

— место работы/учебы;

— должность;

— контактный телефон;

— адрес электронной почты.

4.2.4. В отношении контрагентов (физических лиц) обрабатываются:

— фамилия, имя, отчество;

— дата рождения;

— место рождения;

— адрес регистрации;

— гражданство;

— серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;

— данные страхового свидетельства государственного пенсионного страхования; − идентификационный номер налогоплательщика;

— сведения о постановке на учёт в качестве физического лица, являющегося налогоплательщиком налога на профессиональный доход;

— банковские реквизиты счета;

— контактный телефон;

— адрес электронной почты.

Дополнительно для индивидуальных предпринимателей:

— − адрес регистрации ИП;

— − почтовый адрес;

— ОГРНИП;

— ОКПО.

4.2.5. В отношении представителей/работников контрагентов Оператора (юридических лиц/третьих лиц) обрабатываются:

— фамилия, имя, отчество;

— дата рождения;

— место рождения;

— адрес регистрации;

— контактный телефон;

— адрес электронной почты;

— серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;

— сведения о документе, который подтверждает полномочия представителя.

4.2.6. В отношении законных представителей или представителей по доверенности указанных лиц обрабатываются:

— фамилия, имя, отчество;

— дата рождения;

— адрес регистрации;

— серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;

— сведения о документе, который подтверждает полномочия представителя;

— контактный телефон;

— адрес электронной почты.

4.2.7. В случае необходимости могут обрабатываться иные категории и объемы персональных данных, не указанные в настоящем разделе, но регламентированные требованиями закона, договора, либо с согласия субъекта персональных данных.

V. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБЩИЙ

5.1. Обработка персональных данных осуществляется после принятия необходимых мер по защите персональных данных.

5.2. Оператор не вправе обрабатывать персональные данные субъекта персональных данных без его письменного согласия, за исключением случаев, предусмотренных статьей 6 Закона о персональных данных.

5.3. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

5.4. Письменное согласие субъекта персональных данных должно включать:

— фамилию, имя, отчество;

— адрес регистрации субъекта персональных данных;

— номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

— наименование и адрес Оператора;

— цель обработки персональных данных;

— перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

— перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Оператором способов обработки персональных данных;

— срок, в течение которого действует согласие;

— способ его отзыва;

— подпись субъекта персональных данных.

5.5. Обработка персональных данных осуществляется Оператором следующими способами:

— неавтоматизированная обработка персональных данных;

— автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;

— смешанная обработка персональных данных.

5.6. Оператор организует обработку персональных данных в следующем порядке:

— назначает ответственного работника за организацию обработки персональных данных, устанавливает перечень лиц, имеющих доступ к персональным данным;

— издает Политику, локальные акты по вопросам обработки персональных данных;

— применяет правовые, организационные и технические меры по обеспечению безопасности персональных данных;

— осуществляет внутренний контроль соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным актам Оператора;

— осуществляет оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», определяет соотношение указанного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных данным Федеральным законом;

— знакомит работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, настоящей Политики, локальных нормативных актов по вопросам обработки персональных данных, и (или) организует обучение указанных работников.

5.7. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры, в том числе:

— определяет угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;

— применяет организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

— применяет прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации;

— оценивает эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

— учитывает машинные носители персональных данных;

— обнаруживает факты несанкционированного доступа к персональным данным и принимает меры;

— восстанавливает персональные данные, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;

— устанавливает правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечивает регистрацию и учет всех действий, совершаемых с персональными данными в информационной системе персональных данных.

5.8. 5При обработке персональных данных Оператор выполняет, в частности, сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

5.9. В целях обеспечения сохранности и конфиденциальности персональных данных все операции с персональными данными должны выполняться только работниками Оператора, осуществляющими данную работу в соответствии с трудовыми обязанностями.

5.10. Оператор получает персональные данные непосредственно от субъектов персональных данных или их представителей, наделенных соответствующими полномочиями. Согласия субъекта на получение его персональных данных от третьих лиц не требуется в случаях, когда согласие субъекта на передачу его персональных данных третьим лицам получено от него в письменном виде при заключении договора с Оператором, а также в случаях, установленных федеральным законом.

5.11. Запрещается хранение документов с персональными данными и их копий на рабочих местах и (или) в открытом доступе, оставлять металлические шкафы открытыми в случае выхода работника из рабочего помещения.

5.12. В электронном виде документы, содержащие персональные данные, разрешается хранить в специализированных базах данных или в специально отведенных

для этого директориях с ограничением и разграничением доступа. Копирование таких данных запрещено.

5.13. При увольнении работника, имеющего доступ к персональным данным, прекращении доступа к персональным данным, документы и иные носители, содержащие персональные данные, сдаются работником своему непосредственному руководителю.

VI. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

6.1. Обработка персональных данных в информационных системах осуществляется после реализации организационных и технических мер по обеспечению безопасности персональных данных, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

6.2. Обеспечение безопасности при обработке персональных данных, содержащихся в информационных системах осуществляется в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

6.3. Уполномоченному работнику, имеющему право осуществлять обработку персональных данных в информационных системах, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется в соответствии с функциями, предусмотренными должностными обязанностями работника.

6.4. Информация может вноситься как в автоматическом режиме при получении персональных данных с официального сайта в сети интернет, так и в ручном режиме при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

6.5. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах органов, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным.

6.6. В случае выявления нарушений порядка обработки персональных данных уполномоченными работниками незамедлительно принимаются меры по установлению причин нарушений и их устранению.

6.7. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

— идентификация и аутентификация субъектов доступа и объектов доступа;

— управление доступом субъектов доступа к объектам доступа;

— ограничение программной среды;

— защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;

— регистрация событий безопасности;

— антивирусная защита;

— обнаружение (предотвращение) вторжений;

— контроль (анализ) защищенности персональных данных;

— обеспечение целостности информационной системы и персональных данных;

— − обеспечение доступности персональных данных;

— защита среды виртуализации и технических средств;

— защита информационной системы, ее средств, систем связи и передачи данных;

— выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них;

— управление конфигурацией информационной системы и системы защиты персональных данных.

6.8. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом, которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия. Угрозы первого типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе. Угрозы второго типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе. Угрозы третьего типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Закона о персональных данных.

6.9. В соответствии с пунктом 11 статьи 19 Закона о персональных данных под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. При обработке персональных данных в информационных системах устанавливаются четыре уровня защищенности персональных данных.

6.9.1. Необходимость обеспечения первого уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

— для информационной системы актуальны угрозы первого типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

— для информационной системы актуальны угрозы второго типа и информационная система обрабатывает специальные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора.

6.9.2. Необходимость обеспечения второго уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

— для информационной системы актуальны угрозы первого типа и информационная система обрабатывает общедоступные персональные данные;

— для информационной системы актуальны угрозы второго типа и информационная система обрабатывает специальные категории персональных данных

сотрудников Оператора или специальные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;

— для информационной системы актуальны угрозы второго типа и информационная система обрабатывает биометрические персональные данные;

— для информационной системы актуальны угрозы второго типа и информационная система обрабатывает общедоступные персональные данные более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;

— для информационной системы актуальны угрозы второго типа и информационная система обрабатывает иные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;

— для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает специальные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора.

6.9.3. Необходимость обеспечения третьего уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

— для информационной системы актуальны угрозы второго типа и информационная система обрабатывает общедоступные персональные данные сотрудников Оператора или общедоступные персональные данные менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;

— для информационной системы актуальны угрозы второго типа и информационная система обрабатывает иные категории персональных данных сотрудников Оператора или иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;

— для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает специальные категории персональных данных сотрудников Оператора или специальные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;

— для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает биометрические персональные данные; д) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает иные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора.

6.9.4. Необходимость обеспечения четвертого уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

— для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает общедоступные персональные данные;

— для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает иные категории персональных данных сотрудников Оператора или иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора.

6.10. Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении к Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в

информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

VII. АКТУАЛИЗАЦИЯ (ОБНОВЛЕНИЕ), ИСПРАВЛЕНИЕ, УДАЛЕНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОТВЕТЫ НА ЗАПРОСЫ СУБЪЕКТОВ НА ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

7.1. Согласно ст. 21 ФЗ «О персональных данных», персональные данные должны быть актуализированы оператором, если подтвержден факт неточности. То же касается и подтверждения факта неправомерности обработки. Персональные данные подлежат уничтожению при достижении целей их обработки и в случае отзыва субъектом согласия на их обработку, если: иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных; иное не предусмотрено иным соглашением между оператором и субъектом персональных данных. Оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами.

На основании ст. 20 ФЗ «О персональных данных», оператор обязан сообщить субъекту персональных данных информацию об осуществляемой им обработке по запросу.

В свою очередь, Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

— подтверждение факта обработки персональных данных оператором;

— правовые основания и цели обработки персональных данных;

— цели и применяемые оператором способы обработки персональных данных;

— наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;

— обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

— сроки обработки персональных данных, в том числе сроки их хранения;

— порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

— информацию об осуществленной или о предполагаемой трансграничной передаче данных;

— наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;

— иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

7.2. Указанные выше сведения должны быть предоставлены субъекту персональных данных Оператором в доступной форме и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

7.3. Сведения, указанные в пункте 7.1, предоставляются субъекту персональных данных или его представителю Оператором при обращении либо при получении запроса

субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

7.4. В случае если сведения, указанные в пункте 7.1, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 7.1, и ознакомления с такими персональными данными не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

7.5. Субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 7.1, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 7.4, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 7.1, должен содержать обоснование направления повторного запроса.

7.6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 7.4 и 7.5. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

7.7. Оператор обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение 30 дней 18 с даты получения запроса субъекта персональных данных или его представителя.

7.8. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

7.9. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Оператор обязан внести в них необходимые изменения.

7.10. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Оператор обязан уничтожить такие персональные данные.

7.11. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

7.12. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя, либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки.

7.13. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

7.14. В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

7.15. В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Оператора. В случае если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

7.16. В случае достижения цели обработки персональных данных Оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и уничтожить персональные данные или обеспечить их

уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

7.17. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий 30 дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

7.18. В случае отсутствия возможности уничтожения персональных данных в течение указанных сроков Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

7.19. Внешний доступ к персональным данным предоставляется только при наличии заявления запросившего их лица с указанием перечня необходимой информации, целей для которых она будет использована, с письменного согласия лица, персональные данные которого затребованы. При передаче персональных данных третьим лицам, в том числе представителям работников и других категорий субъектов персональных данных, передаваемая информация ограничивается только теми персональными данными, которые необходимы для выполнения третьими лицами их функций.

VIII. ПОЛОЖЕНИЯ ПО СУБЪЕКТАМ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. С учетом разграничения субъектов персональных данных на основании деятельности Общества, настоящим определены отдельные Положения по обработке персональных данных субъектов персональных данных (далее – Положение) следующих категорий: работников, контрагентов, третьих лиц.

8.2. Настоящие Положения субъектов персональных данных работников, контрагентов, третьих лиц являются неотъемлемой частью Политики.

8.3. Условия, определенные для применения в настоящей Политике в отношении обработки персональных данных распространяются на все правоотношения, связанные с оператором или с субъектами персональных данных, в том числе, выделенных по отдельным Положениям, если применяемые условия в Политике прямо или косвенно не противоречат условиям, применяемым в конкретном Положении по обработке персональных данных по субъектам персональных данных (далее – Положение) конкретных категорий: работников, контрагентов, третьих лиц.

VIII.I. ПОЛОЖЕНИЕ ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

8.1.1. Настоящее Положение по обработке персональных данных работников является сводом условий (правил) составленным в соответствие с требованиями закона, определяющих порядок обработки персональных данных работников Общества, персональные данные которых подлежат обработке, на основании полномочий оператора; обеспечение защиты прав и свобод работника Общества, при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

8.1.2. К персональным данным работника, получаемым и подлежащим хранению у работодателя в порядке, предусмотренном действующим законодательством и настоящим Положением, относятся следующие сведения, содержащиеся в личных делах работников:

— паспортные данные работника;

— ИНН;

— копия страхового свидетельства государственного пенсионного страхования;

— документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета, в том числе в форме электронного документа; • копия документа воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);

— копия документа об образовании, квалификации или наличии специальных знаний (при поступлении на работу, требующую специальных знаний или специальной подготовки);

— анкетные данные, заполненные работником при поступлении на работу или в процессе работы (в том числе – автобиография, сведения о семейном положении работника, перемене фамилии, наличии детей и иждивенцев);

— документы о возрасте малолетних детей и месте их обучения; • документы о состоянии здоровья детей и других родственников (включая справки об инвалидности, о наличии хронических заболеваний);

— документы о состоянии здоровья (сведения об инвалидности, о беременности и т.п.);

— иные документы, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть предъявлены работником при заключении трудового договора или в период его действия (включая медицинские заключения, предъявляемые работником при прохождении обязательных предварительных и периодических медицинских осмотров);

— трудовой договор;

— заключение по данным психологического исследования (если такое имеется); • копии приказов о приеме, переводах, увольнении, повышении заработной платы, премировании, поощрениях и взысканиях;

— личная карточка по форме Т-2;

— заявления, объяснительные и служебные записки работника;

— документы о прохождении работником аттестации, повышения квалификации;

— иные документы, содержащие сведения о работнике, нахождение которых в личном деле работника необходимо для документального оформления трудовых правоотношений с работником (включая приговоры суда о запрете заниматься педагогической деятельностью или занимать руководящие должности).

8.1.3. Размещение на официальном сайте фотографий работников, видео с работниками сотрудники разрешают путем предоставления согласия на обработку персональных данных в Обществе.

8.1.4. Персональные данные работников Общества являются конфиденциальной информацией и не могут быть использованы сотрудниками Общества в личных целях.

8.1.5. В целях обеспечения прав и свобод человека и гражданина работодатель (Общество) и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

— Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

— При определении объема и содержания, обрабатываемых персональных данных работника Общество руководствуется ст. 24 Конституции Российской Федерации, ст. 65 Трудового Кодекса и иными федеральными законами;

— Все персональные данные работника следует получать у него самого. Если персональные данные работника, возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

— Работодатель не имеет права получать и обрабатывать сведения о работнике, относящиеся (в соответствии со статьей 10 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных») к специальным категориям персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, если:

— субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных, в частности:

1) фамилию, имя, отчество, адрес проживания, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных;

— обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных условиями настоящего Положения;

— обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации;

— обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 года N 8-ФЗ "О Всероссийской переписи населения";

— обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;

— обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

— обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медикосоциальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

— обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

— обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;

— обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;

— обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;

— обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

— обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами,

муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;

— обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.

8.1.5.1. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым Кодексом или иными федеральными законами.

8.1.5.2. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

8.1.5.3. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном Трудовым Кодексом и иными федеральными законами.

8.1.5.4. Работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

8.1.5.5. Работники не должны отказываться от своих прав на сохранение и защиту тайны.

8.1.5.6. Работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

8.1.6. Согласно ст.10.1 Федерального закона «О персональных данных», особенностями обработки персональных данных, разрешенных субъектом персональных данных для распространения являются:

8.1.6.1. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Работник образовательной организации (оператор) обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

8.1.6.2. В случае раскрытия персональных данных неопределенному кругу лиц самим субъектом персональных данных без предоставления оператору согласия, обязанность предоставить доказательства законности последующего распространения или иной обработки таких персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку.

8.1.6.3. В случае, если персональные данные оказались раскрытыми неопределенному кругу лиц вследствие правонарушения, преступления или обстоятельств непреодолимой силы, обязанность предоставить доказательства законности последующего распространения или иной обработки таких персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку.

8.1.6.4. В случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных согласился с распространением персональных данных, такие персональные данные обрабатываются оператором, которому они предоставлены субъектом персональных данных, без права распространения.

8.1.6.5. В случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных не установил запреты и условия на обработку персональных данных, или если в предоставленном субъектом персональных данных таком согласии не указаны категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты, такие персональные данные обрабатываются оператором, которому они предоставлены субъектом персональных данных, без передачи (распространения, предоставления, доступа) и возможности осуществления иных действий с персональными данными неограниченному кругу лиц.

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

— непосредственно;

— с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.

8.1.6.7. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, должно содержать следующую информацию:

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

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

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

— сведения об операторе - физическом лице - фамилия, имя, отчество (при наличии), место жительства или место пребывания;

— сведения об операторе-гражданине, являющемся индивидуальным предпринимателем, - фамилия, имя, отчество (при наличии), идентификационный номер налогоплательщика, основной государственный регистрационный номер (если он известен субъекту персональных данных);

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

— цель (цели) обработки персональных данных;

— категории и перечень персональных данных, на обработку которых дается согласие субъекта персональных данных: персональные данные (фамилия, имя, отчество (при наличии), год, месяц, дата рождения, место рождения, адрес, семейное положение, образование, профессия, социальное положение, доходы, другая информация, относящаяся к субъекту персональных данных); специальные категории персональных данных (расовая, национальная принадлежности, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимной жизни, сведения о судимости); биометрические персональные данные;

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

— условия, при которых полученные персональные данные могут передаваться оператором, осуществляющим обработку персональных данных, только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников, либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных персональных данных (заполняется по желанию субъекта персональных данных);

— срок действия согласия

8.1.6.8. Правила использования информационной системы уполномоченного органа по защите прав субъектов персональных данных, в том числе порядок взаимодействия субъекта персональных данных с оператором, определяются уполномоченным органом по защите прав субъектов персональных данных.

8.1.6.9. Молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

8.1.7. В согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ оператора в установлении субъектом персональных данных запретов и условий не допускается. Оператор обязан в срок не позднее трех рабочих дней с момента получения соответствующего согласия субъекта персональных данных опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения.

8.1.8. Установленные субъектом персональных данных запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных субъектом персональных данных для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.

8.1.9. Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению. Указанные в данном требовании персональные данные могут обрабатываться только оператором, которому оно направлено.

8.1.10. Действие согласия субъекта персональных данных на обработку персональных данных, разрешенных субъектом персональных данных для распространения, прекращается с момента поступления оператору требования, указанного по условиям настоящего Положения.

8.1.11. Субъект персональных данных вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных субъектом персональных данных для распространения, к любому лицу, обрабатывающему его персональные данные, в случае условия настоящего Положения или обратиться с таким требованием в суд. Оператор (Работодатель -

Общество) обязан прекратить передачу (распространение, предоставление, доступ) персональных данных в течение трех рабочих дней с момента получения требования субъекта персональных данных или в срок, указанный во вступившем в законную силу решении суда, а если такой срок в решении суда не указан, то в течение трех рабочих дней с момента вступления решения суда в законную силу.

8.1.12. Требования прекратить передачу (распространение, предоставление, доступ) персональных данных не применяются Оператора в отношении субъекта в случае обработки персональных данных в целях выполнения возложенных законодательством Российской Федерации на государственные органы, муниципальные органы, а также на подведомственные таким органам организации функций, полномочий и обязанностей.

8.1.13. Общество определяет объем, содержание обрабатываемых персональных данных работников, руководствуясь Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

8.1.14. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

8.1.15. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

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

8.1.17. Хранение и использование персональных данных работников.

8.1.17.1. Хранение персональных данных работников должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

8.1.17.2. Персональные данные работников Общества хранятся на бумажных и электронных носителях (к доступу имеется определенный код), в специально предназначенных для этого помещениях.

8.1.17.3. В процессе хранения персональных данных работников должны обеспечиваться:

— требования нормативных документов, устанавливающих правила хранения конфиденциальных сведений;

— сохранность имеющихся данных, ограничение доступа к ним, в соответствии с законодательством Российской Федерации и настоящим Положением;

— контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

8.1.17.4. Доступ к персональным данным работников имеют:

— генеральный директор;

— заместители генерального директора;

— специалист по персоналу;

— юрисконсульт;

— иные работники, определяемые приказом директора Общества в пределах своей компетенции.

8.1.17.5. Помимо лиц, указанных по условиям настоящего Положения, право доступа к персональным данным работников имеют лица, уполномоченные действующим законодательством.

8.1.17.6. Лица, имеющие доступ к персональным данным обязаны использовать персональные данные работников лишь в целях, для которых они были предоставлены.

8.1.17.7. Ответственным за организацию и осуществление хранения персональных данных работников Общества является генеральный директор Общества, в соответствии с приказом.

8.1.17.8. Персональные данные работника отражаются в личной карточке работника (форма Т-2) при её наличии в Обществе (необязательно), которая заполняется после издания приказа о его приеме на работу. Личные карточки работников хранятся в специально оборудованных несгораемых шкафах в алфавитном порядке.

8.1.18. Передача персональных данных работника

8.1.18.1. При передаче персональных данных работника работодатель (Общество) должен соблюдать следующие требования:

— не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым Кодексом или иными федеральными законами;

— не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

— предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

— Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном Трудовым Кодексом и иными федеральными законами;

— Осуществлять передачу персональных данных работника в пределах Общества в соответствии с данным Положением, с которым работник должен быть ознакомлен под роспись;

— Разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

— Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

— Передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

8.1.19. Права работника в целях обеспечения защиты персональных данных, хранящихся у работодателя (Общества).

8.1.19.1. В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право:

— получать полную информацию о своих персональных данных и их обработке;

— на свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральными законами. Получение указанной информации о своих персональных данных возможно при личном обращении работника, – к руководителю Общества, ответственному за организацию и осуществление хранения персональных данных работников;

— на определение своих представителей для защиты своих персональных данных;

— требовать об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований действующего законодательства (указанное требование должно быть оформлено письменным заявлением работника на имя руководителя Общества);

— требовать об извещение организацией всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника обо всех произведенных в них исключениях, исправлениях или дополнениях;

— обжаловать в суде любые неправомерные действия или бездействия Общества при обработке и защите его персональных данных.

8.1.19.2. В целях обеспечения достоверности персональных данных работники обязаны:

— при приеме на работу в Общество, представлять уполномоченным работникам достоверные сведения о себе в порядке и объеме, предусмотренном законодательством Российской Федерации;

— в случае изменения персональных данных работника: фамилия, имя, отчество, адрес места жительства, паспортные данные, сведения об образовании, состоянии здоровья (вследствие выявления в соответствии с медицинским заключением противопоказаний для выполнения работником его должностных, трудовых обязанностей и т.п.) сообщать об этом в течение 5 рабочих дней с даты их изменений Работодателю.

8.1.20. Уничтожение персональных данных.

8.1.20.1. В соответствии с Приказом Роскомнадзора №179 от 28 октября 2022 года, определены требования к документальному оформлению факта уничтожения персональных данных работников общеобразовательной организации:

— в случае если обработка персональных данных осуществляется оператором без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных;

— в случае если обработка персональных данных осуществляется оператором с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в информационной системе персональных данных (далее - выгрузка из журнала).

Акт об уничтожении персональных данных должен содержать:

— наименование общеобразовательной организации или фамилию, имя, отчество (при наличии) оператора персональных данных и его адрес;

— наименование общеобразовательной организации или фамилию, имя, отчество (при наличии) лица, осуществляющего обработку персональных данных субъекта

персональных данных по поручению оператора (если обработка была поручена такому лицу;

— фамилию, имя, отчество (при наличии) субъекта или иную информацию, относящуюся к определенному физическому лицу, чьи персональные данные были уничтожены;

— фамилию, имя, отчество (при наличии), должность лиц, уничтоживших персональные данные субъекта персональных данных, а также их подпись; • перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;

— наименование уничтоженного материального носителя, содержащего персональные данные субъекта персональных данных, с указанием количества листов в отношении каждого материального носителя (в случае обработки персональных данных без использования средств автоматизации);

— наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных (в случае обработки персональных данных с использованием средств автоматизации);

— способ уничтожения персональных данных; • причину уничтожения персональных данных;

— дату уничтожения персональных данных субъекта (субъектов) персональных данных. Форма акта об уничтожении персональных данных составляется в произвольной форме.

Акт об уничтожении персональных данных может быть оформлен как на бумаге, так и в электронной форме. В первом случае он заверяется личной подписью лиц, уничтоживших персональные данные, а во втором – их электронной подписью.

8.1.20.2. Выгрузка из журнала должна содержать:

— фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному физическому лицу, чьи персональные данные были уничтожены;

— перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;

— наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных;

— причину уничтожения персональных данных;

— дату уничтожения персональных данных субъекта (субъектов) персональных данных.

При невозможности указать в выгрузке из журнала какие-либо сведения, их следует отразить в акте об уничтожении персональных данных. 7.6. Если оператор обрабатывает персональные данные, используя и не используя средства автоматизации, при их уничтожении следует оформлять акт об уничтожении и выгрузку из журнала.

8.1.20.3. Акт об уничтожении персональных данных и выгрузка из журнала подлежат хранению в течение 3 лет с момента уничтожения персональных данных.

8.1.21. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника.

8.1.21.1. Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом и иными федеральными законами, а также

привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

8.1.21.2. Персональная ответственность — одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

8.1.21.3. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

8.1.21.4. За нарушение правил хранения и использования персональных данных, повлекшее за собой материальный ущерб работодателю, работник несет материальную ответственность в соответствии с действующим трудовым законодательством.

8.1.21.5. Материальный ущерб, нанесенный субъекту персональных данных за счет ненадлежащего хранения и использования персональных данных, подлежит возмещению в порядке, установленном действующим законодательством.

8.1.21.6. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом № 152-ФЗ «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

8.1.21.7. Общество вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных лишь обработку следующих персональных данных:

— относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения (работникам);

— полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

— являющихся общедоступными персональными данными;

— включающих в себя только фамилии, имена и отчества субъектов персональных данных;

— необходимых в целях однократного пропуска субъекта персональных данных на территорию организации или в иных аналогичных целях;

— включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

— обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных. Во всех остальных случаях оператор (руководитель организации, осуществляющей образовательную деятельность, и (или) уполномоченные им лица) обязан направить в уполномоченный орган по защите прав субъектов персональных данных соответствующее уведомление.

VIII.II. ПОЛОЖЕНИЕ ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ КОНТРАГЕНТА

8.2.1. Персональные данные Контрагента относятся к категории конфиденциальной информации.

8.2.2. В целях обеспечения прав и свобод человека и гражданина Оператор и его представители при обработке персональных данных Контрагента соблюдают следующие общие требования:

— обработка персональных данных Контрагента осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия выполнения договорных обязательств в соответствии с законодательством Российской Федерации;

— все персональные данные Контрагента Оператор получает у него самого, за исключением случаев, когда их получение возможно только у третьей стороны способом, не противоречащим законодательству Российской Федерации;

— обработка персональных данных, полученных от третьих лиц, возможна только при уведомлении субъекта персональных данных об этом заранее.

8.2.3. Оператор не получает и не обрабатывает персональные данные Контрагента о его политических, религиозных и иных убеждениях и частной жизни.

8.2.4. Персональные данные не используются в целях причинения имущественного и морального вреда Контрагенту, затруднения реализации его прав и свобод.

8.2.5. При принятии решений, затрагивающих интересы Контрагента, Оператор не основывается на персональных данных Контрагента, полученных исключительно в результате их автоматизированной обработки без его письменного согласия на такие действия.

8.2.6. При идентификации Контрагента Оператор требует предъявление документов, удостоверяющих личность и подтверждающих полномочия представителя.

8.2.7. При заключении договора, как и в ходе его исполнения, в случае возникновения необходимости, Заказчик может потребовать предоставление Контрагентом иных документов, содержащих информацию о нем, с момента предоставления которых может быть связано предоставление дополнительных гарантий и компенсаций.

8.2.8. После принятия решения о заключении договора или предоставления документов, подтверждающих полномочия представителя, а также впоследствии, в процессе выполнения договора, персональные данные Контрагента, также будут включены в:

— договоры;

— иные документы, включение в которые персональных данных Контрагента необходимо согласно действующему законодательству Российской Федерации (накладные, акты, отчеты и т.д.).

8.2.9. Организация защиты персональных данных контрагентов.

8.2.10. Все работники, имеющие доступ к персональным данным Контрагентов, подписывают «Соглашение о неразглашении конфиденциальной информации».

8.2.11. Защита персональных данных Контрагентов от неправомерного их использования или утраты обеспечивается Оператором в порядке, установленном законодательством Российской Федерации, внутренними регламентирующими документами Общества.

8.2.12. Защите подлежат:

— персональные данные, содержащиеся на электронных и материальных носителях;

— носители, содержащие персональные данные.

8.2.13. Ответственные лица структурных подразделений Общества, хранящих персональные данные на бумажных и машинных носителях информации, обеспечивают их защиту от несанкционированного доступа и копирования.

8.2.14. Ответственные лица, обрабатывающие персональные данные в АИС и на машинных носителях информации, обеспечивают защиту в соответствии с требованиями законодательства Российской Федерации, нормативными и методическими документами, касающимися защиты персональных данных.

8.2.15. Хранение персональных данных контрагента:

8.2.15.1. Сведения о Контрагентах на бумажных носителях хранятся в помещениях Общества. Для хранения носителей используются шкафы (ящики), расположенные внутри контролируемой зоны Общества.

8.2.15.2. Обязанности по хранению документов, в которых содержатся персональные данные Контрагентов, возлагаются на руководителей структурных подразделений, в которых обрабатывается информация.

8.2.15.3. Ключи от шкафов /ящиков (при наличии), в которых хранятся носители ПДн, находятся у работника, обрабатывающего данную информацию.

8.2.15.4. Персональные данные Контрагентов могут также храниться в электронном виде – на электронных носителях информации, доступ к которым ограничен и регламентируется Обществом.

8.2.16. Доступ к персональным данным Контрагентов без специального разрешения имеют работники, занимающие в Обществе следующие должности:

— генеральный директор;

— заместитель генерального директора по финансово-экономической работе - главный бухгалтер;

— заместитель главного бухгалтера;

— бухгалтер;

— менеджер по кадрам;

— юрист/юрисконсульт, либо лицо, исполняющее обязанности юриста/юрисконсульта;

— к обработке персональных данных Контрагентов допускаются иные работники в соответствии с Приказом «Об утверждении перечней должностей и лиц, допущенных к обработке персональных данных».

8.2.17. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, по достижении целей обработки или в случае утраты необходимости в их достижении, если иное не предусмотрено законодательством Российской Федерации, вышеуказанные персональные данные уничтожаются.

8.2.18. Передача персональных данных контрагента:

8.2.18.1. При передаче персональных данных Контрагента Оператор соблюдает следующие требования, и выполняются следующие условия:

— осуществляет обработку персональных данных Контрагента в пределах своей организации в соответствии с настоящим Положением;

— разрешает доступ к персональным данным Контрагентов только специально уполномоченным лицам, при этом указанные лица вправе получать только те персональные данные Контрагента, которые необходимы для выполнения конкретных функций;

— вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законодательством;

— определяет требования к защите обрабатываемых персональных данных и перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, а так же устанавливает обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке;

— в случае если Оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Оператор. Лицо, осуществляющее обработку персональных данных по поручению Оператора, несет ответственность перед Оператором;

— передает персональные данные Контрагента его представителям в порядке, установленном законодательством Российской Федерации, и ограничивает эту информацию только теми персональными данными Контрагента, которые необходимы для выполнения указанными представителями их функций.

8.2.19. В случае если Оператору оказываются услуги, выполняются работы или осуществляется поставка товаров юридическими или физическими лицами на основании заключенных договоров (либо иных оснований), и в силу данных договоров эти лица должны иметь доступ к персональным данным, то необходимые персональные данные предоставляются Оператором при наличии в заключенном договоре условия о неразглашении конфиденциальной информации (в том числе содержащей персональные данные или составляющую коммерческую тайну) либо после подписания с указанными лицами Соглашения о неразглашении информации, содержащей персональные данные (неразглашении конфиденциальной информации).

8.2.20. Все сведения о передаче персональных данных Контрагентов регистрируются в Журнале учета передачи персональных данных в целях контроля правомерности использования данной информации лицами, ее получившими. В журнале фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также отмечается, какая именно информация была передана.

8.2.21. Обязанности контрагента и оператора в целях обеспечения достоверности персональных данных.

8.2.21.1. Контрагент обязан:

— при заключении договора предоставить Оператору полные и достоверные данные о себе;

— в случае изменения сведений, составляющих персональные данные Контрагента, не позднее пяти рабочих дней, предоставить обновленную информацию Оператору;

8.2.21.2. Оператор обязан:

— обеспечить защиту персональных данных от неправомерного их использования или утраты в порядке, установленном законодательством Российской Федерации;

— ознакомить субъекта персональных данных с действующими внутренними правилами обработки персональных данных;

— обеспечить защищенное хранение документов, содержащих персональные данные. При этом персональные данные не должны храниться дольше, чем этого требуют цели, для которых они были получены, или дольше, чем это требуется в интересах лиц, о которых собраны данные, или дольше, чем этого требует законодательство;

— вести учет передачи персональных данных Контрагентов третьим лицам путем ведения соответствующего Журнала учета передачи персональных данных;

— в случае реорганизации или ликвидации Оператора, учет и сохранность документов, порядок передачи их на государственное хранение осуществлять в соответствии с правилами, предусмотренными учредительными документами и действующим законодательством Российской Федерации; • вести Журнал учета обращений субъектов персональных данных;

— осуществлять передачу персональных данных субъекта только в соответствии с законодательством Российской Федерации и настоящим Положением;

— по требованию субъекта персональных данных или его законного представителя предоставить ему полную информацию о его персональных данных и обработке этих данных.

8.2.21.3. Права контрагента в целях защиты персональных данных:

В целях обеспечения защиты персональных данных, хранящихся у Оператора, Контрагент имеют право на:

— получение полной информации о составе своих персональных данных и их обработке, в частности, Контрагент имеет право знать, кто и в каких целях использует или использовал информацию о его персональных данных;

— бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные Контрагента на основании письменного запроса, за исключением случаев, если предоставление персональных данных нарушает конституционные права и свободы других лиц;

— определение своих представителей для за щиты своих персональных данных;

— требование об исключении или исправлении неверных или неполных устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для Оператора персональных данных.

— При отказе Оператора исключить или исправить персональные данные Контрагента он имеет право заявить в письменной форме Оператору о своем несогласии с соответствующим обоснованием такого несогласия;

— требование об извещении Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные Контрагента, обо всех произведенных в них исключениях, исправлениях или дополнениях;

— обжалование в суде или надзорном органе любых неправомерных действий или бездействия оператора при обработке и защите его персональных данных.

8.2.21.4. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных. Лица, виновные в нарушении норм, регулирующих обработку персональных данных, привлекаются к ответственности в соответствии с действующим законодательством Российской Федерации.

VIII.III. ПОЛОЖЕНИЕ ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИХ ЛИЦ

8.3.1. К третьим лицам настоящее положение относит физических лиц, отношения с которыми возникают у Общества при осуществлении предусмотренной Уставом деятельности.

8.3.2. Настоящее Положение устанавливает порядок обработки персональных данных третьих лиц с использованием и без использования средств автоматизации.

8.3.3. Персональные данные третьих лиц не могут быть использованы в целях причинения им имущественного и морального вреда, затруднения реализации их гражданских прав и свобод.

8.3.4. К персональным данным третьих лиц, обрабатываемым Обществом и подлежащим хранению в порядке, предусмотренном действующим законодательством, относятся следующие сведения:

— фамилия, имя, отчество; число, месяц, год рождения; место рождения; серия, номер документа, подтверждающего личность, наименование органа, выдавшего его, дата выдачи;

— контактные данные: адрес (места жительства, регистрации), контактный телефон, адрес электронной почты;

— документы, которые предоставляются в виде копий следующих документов: документ, удостоверяющий личность, паспорт, домовая книга, договоры найма жилого помещения, купли-продажи, дарения, передачи в собственность в порядке наследования, свидетельство о государственной регистрации права, акты приема-передачи недвижимости, выписки из ЕГРН, ордера, технические паспорта жилого (нежилого) помещения, кадастровые паспорта жилого (нежилого) помещения, справки с паспортного стола, свидетельства о рождении, свидетельства о смерти, свидетельства и заключении (расторжении) брака, свидетельства о праве на наследство по закону или по завещанию, справка о временном проживании, свидетельства ИНН, свидетельства о постановке на учет в налоговом органе, уставы и протоколы юридических лиц, чеки, квитанции об оплате, соглашения об оплате, удостоверения (пенсионные и др.), реестры членов дачных и садоводческих товариществ, карточки лицевых счетов других управляющих организаций, командировочные удостоверения, проездные билеты, страховые полисы, справки о составе семьи, доверенности, платежные реквизиты счетов, решения судов.

8.3.5. Персональные данные, перечисленные в п.8.3.4. настоящего положения, являются конфиденциальными. Под конфиденциальностью персональных данных третьих лиц понимается обязательное для соблюдения лицом, получившим доступ к персональным данным третьего лица, требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания. Сбор, хранение, использование и распространение информации о частной жизни третьих лиц не допускаются.

8.3.6. В целях обеспечения прав и свобод человека и гражданина при обработке персональных данных третьих лиц обязательно соблюдаются следующие общие требования.

8.3.6.1. Обработка персональных данных должна осуществляться на основе принципов законности целей и способов обработки персональных данных и добросовестности; соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных; соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных; достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных.

8.3.6.2. Обработка персональных данных может осуществляться Обществом с согласия субъекта персональных данных, за исключением случаев, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

8.3.6.3. Обработка персональных данных может осуществляться исключительно в целях осуществления Обществом деятельности, предусмотренной Уставом.

8.3.6.4. Объем и содержание обрабатываемых персональных данных определяются в соответствии с Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных», иными федеральными законами и нормативными правовыми актами.

8.3.6.5. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации.

8.3.6.6. В случаях достижения цели обработки персональных данных, отзыва субъектом персональных данных согласия на обработку своих персональных данных Оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, установленный действующим законодательством.

8.3.6.7. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена Обществом за счет своих средств в порядке, установленном федеральным законом.

8.3.7. Права, обязанности третьих лиц как субъектов персональных данных:

8.3.7.1. Третье лицо как субъект персональных данных обязан передавать представителю Общества комплекс достоверных документированных персональных данных, перечень которых установлен настоящим Положением в случае необходимости предоставления таких документов.

8.3.7.2. Третье лицо как субъект персональных данных в отношении которого Общество ведет делопроизводство в установленных настоящим Положением целях, имеет право:

— на полную информацию о своих персональных данных и обработке этих данных;

— на свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных законодательством Российской Федерации;

— требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований законодательства. Неправомерный отказ исключить или исправить персональные данные физического лица, а также любое иное нарушение его прав на защиту персональных данных влечет возникновение у физического лица права требовать устранения нарушения его прав и компенсации причиненного таким нарушением морального вреда;

— принимать предусмотренные законом меры по защите своих прав.

8.3.8. Порядок получения персональных данных третьих лиц.

8.3.8.1. Персональные данные следует получать лично у субъекта персональных данных. Получение персональных данных субъекта персональных данных у третьей стороны возможно в случаях, предусмотренных действующим законодательством.

8.3.8.2. Запрещается получать персональные данные третьего лица о его политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах, за исключением случаев, предусмотренных действующим законодательством.

8.3.8.3. При передаче персональных данных должны соблюдаться следующие требования:

— не сообщать персональные данные третьей стороне, третьим лицам без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных действующим законодательством;

— не использовать персональные данные третьих лиц в коммерческих целях;

— предупредить лиц, получающих персональные данные третьих лиц, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные третьих лиц, обязаны соблюдать режим конфиденциальности;

— разрешать доступ к персональным данным третьих лиц только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций.

8.3.9. Все меры конфиденциальности при обработке персональных данных третьих лиц распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

8.3.10. Доступ к персональным данным третьих лиц.

8.3.10.1. Внутренний доступ (доступ внутри Общества) к обработке персональных данных третьих лиц осуществляется допуском работников Общества в соответствии с «Перечнем должностей, допущенных к обработке персональных данных» утвержденным приказом руководства Общества.

8.3.10.2. Внешний доступ к персональным данным третьих лиц, вне Общества, обеспечивается надзорным (контрольным) органам государственной власти и управления, в пределах их компетенции.

8.3.11. Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных, обеспечивающий надежную безопасность информации в процессе деятельности Общества, подразделяется на внутреннюю и внешнюю защиту.

8.3.11.1. «Внутренняя защита» включает в себя соблюдение следующих мер в Обществе:

— ограничение и регламентация состава лиц, функциональные обязанности которых требуют конфиденциальных знаний;

— строгое избирательное и обоснованное распределение документов и информации между работниками Общества;

— рациональное размещение рабочих мест работников, исключающее бесконтрольное использование защищаемой информации;

— знание работником требований нормативно-методических документов по защите информации и сохранении тайны;

— наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

— определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника; - организация порядка уничтожения информации;

— своевременное выявление нарушения требований разрешительной системы доступа работниками структурных подразделений Общества;

— воспитательная и разъяснительная работа с работниками структурных подразделений Общества по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

— соблюдение порядка приема, учета и контроля деятельности посетителей; - наличие технических средств охраны, сигнализации;

— наличие программных и технических средств защиты информационных систем от несанкционированного доступа;

— обеспечение порядка охраны зданий, помещений.

Все лица, работники Общества, связанные с получением, обработкой и защитой персональных данных третьих лиц обязаны подписать «Соглашение о неразглашении конфиденциальной информации».

8.3.11.2. «Внешняя защита» включает в себя создание целенаправленных неблагоприятных условий и труднопреодолимых препятствий для постороннего лица, пытающегося совершить несанкционированный доступ и овладение информацией. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Общества. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в структурных подразделениях Общества.

8.3.12. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных. Лица, виновные в нарушении норм, регулирующих обработку персональных данных, привлекаются к ответственности в соответствии с действующим законодательством Российской Федерации.

IX. ДЕЙСТВИЕ ЗАКОНА И НАСТОЯЩЕЙ ПОЛИТИКИ, ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ПОЛУЧЕНИЕ, ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Политика является обязательной для исполнения всеми Работниками Общества, имеющими доступ к персональным данным.

9.2. Настоящая Политика вступает в силу с момента её утверждения генеральным директором Общества и действует бессрочно, до замены её новой Политикой или замены ее отдельных условий или положений.

9.3. Все изменения в Политику вносятся приказом руководства Общества.

9.4. Все работники Общества должны быть ознакомлены с настоящей Политикой под роспись.

9.5. В случае отсутствия в настоящей Политике, или в ее отдельных Положениях условий для применения к правоотношениям по обработке персональных данных к субъектам или оператору, иным лицам, то на данные правоотношения распространяются требования закона, нормативных актов, регулирующих соответствующие правоотношения.

9.6. Каждый работник Общества, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

9.7. Лица, виновные в распространении конфиденциальной информации о персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации

X. ПРИЛОЖЕНИЯ (ФОРМЫ ДОКУМЕНТОВ)

Приложение № 1.
Форма приказа о назначении ответственного за организацию обработки персональных данных

ПРИКАЗ

г. _____ ___» _____202_ №_____

«О назначении ответственного работника Общества
за безопасность обработки персональных данных»

В целях обеспечения защиты персональных данных работников ООО «_____» (далее- Общество), в том числе при обработке в информационной системе персональных данных; в целях исполнения Федерального закона от 27 июля 2006 года № 152-ФЗ ч. 1 ст. 22 «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Назначить генерального директора _____ (ФИО) ответственным за безопасность обработки персональных данных.
2. Организовать _____(ФИО) мероприятия по сбору, хранению и обработке персональных данных в соответствии с требованиями законодательства РФ.
3. Доводить до сведения работников Общества нормативно-правовые акты по вопросам обработки персональных данных, требований к защите персональных данных.
4. В случае отсутствия ответственного за безопасность обработки персональных данных _____ (ФИО) по уважительным причинам (больничный, командировка, отпуск и проч.) замещающего его назначить _____ (должность) _____(ФИО).
5. Ознакомить _____(ФИО) и _____(ФИО) с должностной инструкцией ответственного за обработку персональных данных.
6. Контроль за исполнением настоящего приказа оставляю за собой.

Генеральный директор **ФИО**

Приложение № 2.
Форма приказа о хранении бумажных носителей персональных данных

ПРИКАЗ

г. _____ «___» _____202_№____

«Об утверждении мест хранения
материальных носителей персональных данных»

В соответствии с требованиями Федерального закона РФ от 27.07.2006 г. №152-ФЗ «О персональных данных» и Постановления Правительства РФ от 15.09.2008 N687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», в целях обеспечения режима конфиденциальности при работе с материальными носителями персональных данных в ООО «_____»,

ПРИКАЗЫВАЮ:

1. Утвердить места хранения материальных носителей персональных данных субъектов по адресу: _____ (Приложение 1).
2. Ответственным лицам за обеспечение сохранности материальных носителей персональных данных:
2.1. Соблюдать при хранении материальных носителей персональных данных условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.
2.2. Хранить материальные носители персональных данных только в установленных местах.
3. Ознакомить сотрудников, допущенных к обработке персональных данных с перечнем мест хранения.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Генеральный директор (ФИО)

Приложение № 3.
Форма приказа об утверждении
перечня персональных данных

ПРИКАЗ

г. _____ «___» _____202_ №_____

«Об утверждении перечня персональных данных,
информационных систем персональных данных
и допущенных работников»

Во исполнение требований Федерального закона №152-ФЗ от 27июля 2006 г. «О персональных данных» и прочих нормативных документов по защите информации,

ПРИКАЗЫВАЮ:

1. Утвердить Перечень персональных данных, обрабатываемых в ООО «_____» (Приложение 1 к настоящему приказу).
2. Утвердить Перечень информационных систем персональных данных ООО «_____» (Приложение 2 к настоящему Приказу).
3. Утвердить Перечень должностей работников ООО «_____», допущенных к обработке персональных данных (Приложение 3 к настоящему приказу).
4. Ответственному за организацию обработки персональных данных ознакомить работников, которым в связи со служебными обязанностями необходим доступ к персональным данным с прилагаемыми перечнями.
5. Контроль за исполнением настоящего приказа оставляю за собой.

Генеральный директор **ФИО**

Приложение 1
к приказу от _____ г. №_____

ПЕРЕЧЕНЬ персональных данных,
обрабатываемых в ООО «_____»

№ п/п	Категории субъектов персональных данных	Способы обработки персональных данных	Цели обработки персонльных данных	Перечень обрабатываемых персональных данных	Правовое основание обработки персональных данных	Срок хранения и обработки персональных
1.	Работники бывшие работники	Неавтоматизированный	-ведение кадрового, бухгалтерского и воинского учета; - содействие работникам в продвижении по службе; - обеспечение пропускного режима, сохранности имущества Оператора, обеспечение личной безопасности; - исполнение Оператором функции работодателя, оформления трудовых отношений и обеспечение установленных законодательством Российской Федерации условий труда; - осуществление видов деятельности, предусмотренных уставом.	Иные категории: - фамилия, имя, отчество; - сведения об изменении фамилии, имени, отчества (причина изменения, дата); - пол; - дата рождения (число, месяц, год); - место рождения (в соответствии с паспортными данными); - гражданство; - знание иностранных языков (наименование, степень владения); - сведения об образовании, в том числе и послевузовском профессиональном образовании (вид образования, наименование и год окончания образовательного учреждения, квалификация, специальность по документу об образовании); - профессия; - стаж работы; - состояние в браке; - состав семьи (степень родства, фамилия, имя, отчество, год рождения); - реквизиты документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ); - адрес места жительства (адрес регистрации, фактического проживания); - дата регистрации по месту жительства; - идентификационный номер налогоплательщика (ИНН); - номер страхового свидетельства государственного пенсионного страхования (СНИЛС); - контактные данные (номер телефона и адрес электронной почты); - сведения о воинском учете (категория запаса, воинское звание, состав (профиль), полное кодовое обозначение ВУС, категория годности к военной службе, наименование военного комиссариата по месту жительства, отметка о	- ст. ст. 65, 86-90 Трудового кодекса РФ; - Налоговый кодекс РФ; - Федеральный закон №167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»; - Федеральный закон №402-ФЗ «О бухгалтерском учете»; - Федеральный закон №255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнств	-

				постановке и снятии с воинского учета); - номер и дата трудового договора; - табельный номер; - сведения о приеме на работу и переводах на другую работу (дата, структурно подразделение, должность, тарифная ставка (оклад), основание); - сведения о предыдущем месте работы по трудовому договору (организация, адрес расположения, должность); - сведения о прохождении аттестации (дата, решение комиссии, номер и дата документа о прохождении аттестации, основание); - сведения о повышении квалификации (даты начала и окончания обучения, вид повышения квалификации, наименование образовательного учреждения, серия, номер, наименование документа о повышении квалификации); - сведения о профессиональной переподготовке (даты начала и окончания переподготовки, специальность, номер и дата документа о прохождении профессиональной переподготовки); - сведения о наградах (поощрениях), почетных званиях (наименование награды, наименование, номер и дата подтверждающего документа); - сведения об отпусках (вид отпуска, количество календарных дней отпуска, даты начала и окончания отпуска); - сведения о социальных льготах (наименование льготы, номер и дата выдачи документа); - основание прекращения трудового договора (увольнения); - дата увольнения; - банковские реквизиты для перечисления заработной платы и иных выплат; - фотография (не является биометрическими персональными данными, т.к. не используется для установления личности и не соответствует требованиям ГОСТ Р ИСО/МЭК 19794-5-2013); - сведения о деловых и иных личных качествах, носящих оценочный характер	ом»; - ст. 8 Федерального закона от 31.05.1996 №61-ФЗ «Об обороне»; - Федеральный закон № 326-Ф «Об обязательном медицинском страховании в Российской Федерации».	
2	Пользователи сайта	Автоматизированная в информационной системе «_____»	- продвижение товаров, работ, услуг; - установление с пользователем сайта обратной связи, включая направление уведомлений, запросов и их обработки, а также обработки запросов и заявок от пользователя в целях дальнейшего	Иные категории: - фамилия, имя, отчество; - дата рождения; - номер телефона; - адрес электронной почты; - адрес доставки/поставки; - информация, содежащиеся в резюме; - иная информация, которую пользователь решил предоставить.	- согласие на обработку персональных данных.	-

			заключения и исполнения договора; - получение и публикация отзывов; - подбор персонала.			
3	Пользователи; Обучающиеся; Дети; родители	Автоматизированная в информационной системе «____»	- ведение статистики и анализ работы Сайта.	Иные категории: - файлы cookie; - сведения о действиях пользователей Сайта; - сведения об оборудовании и браузере пользователя; - IP-адрес; - дата и время сессии; - реферер (адрес предыдущей страницы).	- согласие на обработку персональны данных.	-
		Неавтоматизированная; Автоматизированная в информационной системе «_____»	-	Иные категории: - фамилия, имя, отчество обучающегося/ребенка; - фамилия, имя, отчество родителей; - дата рождения; - СНИЛС; -Номер сертификата персонифицированного финансирования дополнительного образования обучающегося/ребенка; - Email; - телефон; -сведения о полученном образовании; - паспортные данные; -ИНН; - Адрес места жительства; - сведения медицинского характера для допуска управления транспортным средством	- согласие на обработку персональных данных.	-

Приложение 2
к приказу от _____ г. № _____

ПЕРЕЧЕНЬ
информационных систем персональных данных ООО «_____»

№ пп	Характеристики информационной системы	Значение характеристики информационной системы
1	Информационная система «_____» /ИС «_____»	
11.	Категории субъектов ПДн	Работники, контрагенты, третьи лица, обучающиеся (дети и родители)
1.2.	Категории ПДн	Иные категории ПДн
1.3.	Количество субъектов, ПДн которых обрабатываются в ИСПДн	Менее чем 100 000 субъектов
1.4.	Перечень действий (операций), совершаемых с ПДн	Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, передача, использование, доступ, удаление ПДн
1.5.	1.5 Месторасположение баз данных	Сервер в ЦОД «_____»

Приложение № 6.
Форма Согласия на обработку
персональных данных.
Форма письменного Согласия
на обработку персональных данных

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ ИСПОЛНИТЕЛЯ

Я, _____ даю согласие на обработку своих персональных данных, указанных в договоре, с использованием или без использования средств автоматизации, в целях заключения и исполнения настоящего договора.

_____/
(подпись) (расшифровка)

СОГЛАСИЕ
на обработку персональных данных

Я,
_____
(фамилия, имя, отчество - при наличии)
основной документ, удостоверяющий личность: _____
(вид документа, серия, номер, дата выдачи документа, наименование выдавшего органа)

зарегистрированный(ая) по адресу: _____

даю свое согласие на обработку моих персональных данных, относящихся исключительно к перечисленным ниже категориям персональных данных: фамилия, имя, отчество; пол; дата рождения; тип документа, удостоверяющего личность; данные документа, удостоверяющего личность; гражданство; и иные сведения.

Я даю согласие на использование персональных данных исключительно в целях рассмотрения моих документов, а также на хранение данных об этих результатах на электронных носителях.

Настоящее согласие предоставляется мной на осуществление действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу третьим лицам для осуществления действий по обмену информацией, обезличивание, блокирование персональных данных, а также осуществление любых иных действий, предусмотренных действующим законодательством Российской Федерации.

Я проинформирован, что получатель сведений гарантирует обработку моих персональных данных в соответствии с действующим законодательством Российской Федерации как неавтоматизированным, так и автоматизированным способами.

Данное согласие действует до достижения целей обработки персональных данных или в течение срока хранения информации.

Данное согласие может быть отозвано в любой момент по моему письменному заявлению.

Я подтверждаю, что, давая такое согласие, я действую по собственной воле и в своих интересах.

«___» _____2025 г. /_____/ _____/
(Подпись) *(Расшифровка подписи)*

Приложение №7.
Форма отзыва согласия
на обработку персональных
данных

Руководителю _____
(наименование оператора, обрабатывающего персональные данные)

_____
(фамилия, имя, отчество, номер основного документа,

_____
удостоверяющего личность субъекта персональных данных или его представителя,

_____
сведения о дате выдачи указанного документа и выдавшем его органе)

ЗАПРОС
на прекращение обработки персональных данных в связи с отзывом согласия на обработку персональных данных

В соответствии с ч. 5 ст. 21 Федерального закона «О персональных данных» и в связи с

прошу вас прекратить обработку моих персональных данных:
_____
_____
_____
Ответ на настоящий запрос прошу направить в письменной форме по адресу: _____ в установленные законом сроки.

_____ / _____/
(подпись) (расшифровка подписи)
(дата)

Приложение №8.
Форма согласия на обработку персональных данных соискателя

Я, _____
(фамилия, имя, отчество)
паспорт _____ № _____ выдан _____
(серия) *(номер)* *(дата выдачи)*

_____
(кем выдан паспорт)
проживающий(ая) по адресу_____

_____
(адрес места жительства по паспорту)

в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» своей волей и в своем интересе выражаю ООО «_____», ИНН _____ ОГРН _____ в целях рассмотрения вопроса о соответствии моей кандидатуры имеющимся вакансиям, согласие на обработку, предполагающую сбор (непосредственно от соискателя, из общедоступных информационных ресурсов, из архивов), запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление и уничтожение моих персональных данных, включающих фамилию, имя, отчество, год, месяц, дату и место рождения, гражданство, адрес регистрации, адрес места жительства, паспортные данные, сведения о составе семьи, сведения об образовании, в том числе о повышении квалификации, дополнительном образовании, владении иностранными языками и т.п., о занимаемой должности, данные о предыдущих местах работы и/или воинской службе, сведения о доходах и/или имуществе, идентификационный номер налогоплательщика, номер страхового свидетельства обязательного пенсионного страхования, сведения об инвалидности, сведения о воинском учете, данные о допуске к сведениям, составляющим государственную тайну, сведения о наградах, сведения о социальных льготах, которые предоставляются в соответствии с законодательством Российской Федерации, фотографию, контактная информация.

Обработка персональных данных осуществляется как с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, так и без использования таких средств.

Согласие вступает в силу со дня его подписания и действует в течение 30 суток с момента принятия ООО «_____» решения о несоответствии моей кандидатуры требованиям по вакантным должностям.

Согласие может быть отозвано в любое время на основании моего письменного заявления, направленного в адрес ООО «_____».

В случае отзыва настоящего Согласия ООО «_____» вправе обрабатывать мои персональные данные в случаях и в порядке, предусмотренных Федеральным законом «О персональных данных».

«___» _____ 20__г. _____ _____
(подпись) (расшифровка подписи)

Приложение № 9.
Форма согласия на передачу персональных данных работника третьим лицам

Я,	(фамилия, имя, отчество (последнее – при наличии),

проживающий(ая) по адресу:	(указать адрес места жительства)

в соответствии с требованиями статьи 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», в целях:

(указать цель обработки персональных данных),

действуя свободно, своей волей и в своем интересе, даю согласие

на передачу в (указать ФИО (адрес пребывания) или полное наименование организации (юридический адрес))
(указать наименование организации, которой передаются персональные данные, ИНН, ОГРН, адрес)

моих персональных данных: (указать перечень обрабатываемых персональных данных)
для обработки, совершаемой с использованием средств автоматизации или без использования таких средств, а именно (указать действия с персональными данными)

Подтверждаю, что ознакомлен (а) с основными положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

Настоящее согласие действует до истечения определяемых в соответствии с законодательством Российской Федерации сроков хранения персональных данных.

Оставляю за собой право отзыва данного согласия по моему письменному заявлению.

(Дата) (Подпись) (Расшифровка)

Приложение № 10.
Форма Согласия на обработку персональных данных, разрешенных субъектом для распространения

, _____ (фамилия, имя, отчество законного представителя субъекта персональных данных) основной документ, удостоверяющий личность _____выдан _____ (серия, номер, сведения о дате выдачи указанного документа и выдавшем его органе), проживающий по адресу _____ в дальнейшем «Представитель субъекта персональных данных», являющийся родителем (законным представителем) субъекта_____ (фамилия, имя, отчество несовершеннолетнего субъекта персональных данных) на основании _____ (реквизиты свидетельства о рождении ребенка или иного документа, подтверждающего полномочия родителя или иного законного представителя) проживающего по адресу_____,
далее именуемого «Субъект персональных данных», настоящим даю свое согласие учреждению ООО «_____» ИНН _____ ОГРН _____, далее «Оператор персональных данных», на обработку персональных данных на следующих условиях:
1. Настоящее согласие дается мною для осуществления и выполнения возложенных законодательством Российской Федерации и иными правовыми актами на Оператора персональных данных (далее- Оператор) функций, полномочий и обязанностей в рамках реализации образовательных программ.
2. Настоящее согласие дается мною на осуществление следующих необходимых действий или совокупности действий с использованием средств автоматизации и без использования таких средств с моими персональными данными и персональными данными моего ребенка, включающих: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу(распространение, предоставление, доступ),обезличивание, блокирование, удаление, уничтожение персональных данных.
3. Перечень персональных данных, передаваемых мною (Представителем субъекта персональных данных)
Оператору на обработку:
3.1. Обучающийся (Субъект персональных данных):
3.1.1. фамилия, имя, отчество (последнее – при наличии);
3.1.2.дата рождения;
3.1.3. реквизиты свидетельства о рождении или (для иностранных граждан и лиц без гражданства) документа, удостоверяющего личность;
3.1.4. адрес места жительства (места пребывания, места фактического проживания);
3.1.5. информация о результатах психолого-медико-педагогической комиссии (при наличии);
3.1.6. медицинское заключение;
3.1.7. информация о наличии братьев и(или) сестер, проживающих в одной с обучающимся семье и имеющих общее с ним место жительства;
3.2. Родитель или законный представитель обучающегося (Представитель субъекта персональных данных):
3.2.1. фамилия, имя, отчество (последнее – при наличии);
3.2.2. реквизиты документа, удостоверяющего личность, либо документа, удостоверяющего личность иностранного гражданина или лица без гражданства в РФ (в соответствии со статьей 10 Федерального закона от 25 июля 2002г. № 115-ФЗ «О правовом положении иностранных граждан в РФ»), подтверждающего право на пребывание в РФ, подтверждающего законность представления прав ребенка;
3.2.3. реквизиты документа, подтверждающего установление опеки (при наличии);
3.2.4. адрес электронной почты;
3.2.5. номер телефона;
3.2.6. информация о наличии права на специальные меры поддержки (гарантии) отдельных категорий граждан и их семей (при необходимости).
4. Оператор вправе передавать персональные данные Представителя субъекта персональных данных (далее – Представителя) и персональные данные Субъекта персональных данных(далее – Субъекта) третьим лицам на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта.
5. Представитель вправе требовать от Оператора уточнения своих персональных данных и персональных данных Субъекта, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
6. Представитель имеет право на получение информации, касающейся обработки его персональных данных и персональных данных Субъекта в соответствии сп.7 ст.14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»:
6.1. сведения должны быть предоставлены Представителю Оператором в доступной форме, в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных;
6.2. сведения предоставляются Представителю Оператором при обращении либо при получении запроса Представителя. Запрос должен быть оформлен в соответствии с п.3 ст.14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
7. Представитель вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, а также в целях ознакомления с обрабатываемыми персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса;
8. Представитель вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, а также в целях ознакомления с обрабатываемыми персональными данными ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями должен содержать обоснование направления повторного запроса.
9. Оператор вправе отказать Представителю в выполнении повторного запроса. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.
10. Право Представителя на доступ к его персональным данным может быть ограничено в соответствии с п.8 ст.14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».
11. Настоящее Согласие является действительным до истечения сроков хранения соответствующей информации или документов, содержащих вышеуказанную информацию, определяемых в соответствии с Федеральным законом от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации», после чего персональные данные уничтожаются или обезличиваются.
12.Согласие может быть отозвано Представителем путем направления соответствующего письменного уведомления в адрес Оператора по почте заказным письмом, с уведомлением о вручении, либо вручением лично под расписку представителю Оператора, после чего Оператор обязуется в течение 30 (тридцати) дней прекратить обработку и уничтожить персональные данные Представителя и Субъекта.
Подпись Представителя субъекта персональных данных
_____/_____
подпись расшифровка подписи

«____»_____20___г. дата заполнения

Приложение № 11.
Форма информированного согласия
пользователя сайта

Во исполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» даю своё согласие Обществу с ограниченной ответственностью «_____», ИНН _____ ОГРН _____ (далее – Общество), сайт Общества: _____на обработку своих персональных данных со следующими условиями:

1. Данное Согласие даётся на обработку персональных данных с использованием средств автоматизации. Согласие даётся на обработку следующих персональных данных:
   - Фамилия
   - Имя
   - Отчество (при наличии)
   - год рождения
   - месяц рождения
   - дата рождения
   - место рождения
   - номер телефона
   - электронная почта.
2. Целью обработки персональных данных является надлежащее выполнение оператором своих обязательств в рамках деятельности по сертификации продукции.
3. Основанием для обработки персональных данных являются статья 6 Федерального закона № 152-ФЗ «О персональных данных»; настоящее информированное согласие пользователя сайта на обработку персональных данных.
4. В ходе обработки с персональными данными будут совершены следующие действия: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), блокирование, удаление, уничтожение данных.
5. Согласие действует с момента предоставления его Обществу в течение неопределенного срока (или до достижения целей обработки персональных данных) и может быть отозвано путем направления Обществу заявления в свободной письменной форме об отзыве согласия, при этом Общество прекращает обработку персональных данных и уничтожает их, за исключением персональных данных, включенных в документы, обязанность по хранению которых прямо предусмотрена законодательством и внутренними документами оператора. Хранение таких персональных данных осуществляется Обществом в течение срока, установленного законодательством и внутренними документами оператора.
6. Настоящим Согласием я подтверждаю, что являюсь субъектом предоставляемых персональных данных, подтверждаю достоверность предоставляемых данных.

Приложение № 12.
Форма Обязательства (соглашения)
о неразглашении информации,
содержащей персональные данные

Я, _____,
паспорт серии _____, номер _____, выданный « _____ »_____ 20____ г.,
_____, являясь штатным работником «_____», в соответствии с трудовым договором, должностной инструкцией понимаю, что получаю доступ к персональным данным физических лиц, а именно: _____

_____

Я также понимаю, что во время исполнения своих обязанностей мне приходится заниматься сбором, обработкой, накоплением, хранением и т.д. персональных данных физических лиц.
Я обязуюсь хранить в тайне известные мне конфиденциальные сведения, информировать руководителя образовательного учреждения о фактах нарушения порядка обращения с конфиденциальными сведениями, о ставших мне известным попытках несанкционированного доступа к информации.
Я обязуюсь соблюдать правила пользования документами, порядок их учета и хранения, обеспечивать в процессе работы сохранность информации, содержащейся в них, от посторонних лиц, знакомиться только с теми служебными документами, к которым получаю доступ в силу исполнения своих служебных обязанностей.
Я понимаю, что разглашение такого рода информации может нанести ущерб физическим лицам, как прямой, так и косвенный.
В связи с этим даю обязательство при работе (сборе, обработке, накоплении, хранении и т.д.) с персональными данными физических лиц соблюдать все описанные в Федеральном законе от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлении Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и других нормативных актах, требования.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных физических лиц, или их утраты я несу ответственность в соответствии с действующим законодательством РФ.
Я подтверждаю, что не имею права разглашать сведения:

- анкетные и биографические данные;
- сведения об образовании;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке, их аттестации;
- копии отчетов, направляемые в органы статистики.

« _____ » _____ 20____ г.

_____ _____

Подпись Расшифровка подписи

Приложение № 13.
Перечень форм, содержащих персональные данные

Наименование формы	Хранить	Основание
Т-1 «Приказ (распоряжение) о приеме работника на работу»	75 лет	Постановление Госкомстата РФ от 5 января 2004 г. № 1
Т-2 «Личная карточка работника»	75 лет	Постановление Госкомстата РФ от 5 Января 2004 г. № 1
Т-5 «Приказ (распоряжение) о переводе работника на другую работу»	5 лет	Постановление Госкомстата РФ от 5 Января 2004 г. № 1
Т-6 «Приказ (распоряжение) о предоставлении отпуска работнику»	75 лет	Постановление Госкомстата РФ от 5 Января 2004 г. № 1
Т-8 «Приказ (распоряжение) о прекращении (расторжении) трудового договора с работником (увольнении)»	10 лет	Постановление Госкомстата РФ от 5 Января 2004 г. № 1
Т-9 «Приказ (распоряжение) о направлении работника в командировку»	10 лет	Постановление Госкомстата РФ от 5 Января 2004 г. № 1
Т-54 «Лицевой счет»	5 лет	Постановление Госкомстата РФ от 5 Января 2004 г. № 1
Т-60 «Записка-расчет о предоставлении отпуска работнику»	5 лет	Постановление 5 лет Госкомстата РФ от 5 Января 2004 г. № 1
Т-61 «Записка-расчет при прекращении (расторжении) трудового договора с работником (увольнении)»		
Трудовой договор с работником	75 лет	Трудовой кодекс РФ
Т-73 «Акт о приеме работ, выполненных по срочному трудовому договору, заключенному на время выполнения определенной работы»	5 лет	Постановление Госкомстата РФ от 5 Января 2004 г. № 1

Приложение № 14.
Договор поручения на обработку персональных данных третьим лицом

[место заключения договора] [число, месяц, год]

[**Наименование организации-оператора**], именуемое в дальнейшем "Доверитель", в лице [**должность, Ф. И. О.**], действующего на основании [**устава, положения, доверенности**], с одной стороны, и

[**наименование организации**], именуемое в дальнейшем "Поверенный", в лице [**должность, Ф. И. О.**], действующего на основании [**устава, положения, доверенности**], с другой стороны, а вместе именуемые "Стороны", заключили договор о нижеследующем:

1. Предмет договора

1.1. Поверенный обязуется по поручению, от имени и за счет Доверителя совершить действия по обработке персональных данных, которые включают следующее: [**указать перечень действий (операций) с персональными данными; такими действиями могут быть, например: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных**] (далее Поручение).

1.2. Состав персональных данных, подлежащих обработке, включает [**вписать нужное**].

1.3. Обработка персональных данных осуществляется в целях [**вписать нужное**].

1.4. Обработка персональных данных должна быть осуществлена в срок [**вписать нужное**].

1.5. Передача Доверителем персональных данных для обработки Поверенному осуществляется с согласия субъекта персональных данных по акту приема-передачи.

2. Обязанности сторон договора

2.1. Доверитель обязан:

2.1.1. В течение [**значение**] дней с даты подписания настоящего договора передать Поверенному персональные данные для обработки.

2.1.2. Возмещать Поверенному понесенные в связи с исполнением поручения издержки, подтвержденные документами, оформленными надлежащим образом.

2.1.3. Принять отчет Поверенного, все предоставленные им документы и все исполненное им в соответствии с настоящим договором.

2.1.4. Уплатить Поверенному вознаграждение в порядке, установленном разделом 3 настоящего договора.

2.2. Поверенный обязан:

2.2.1. Лично исполнять данное ему поручение.

2.2.2. Соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 г. № 152-ФЗ "О персональных данных".

2.2.3. Осуществлять обработку персональных данных в соответствии с целями, определенными Сторонами в настоящем договоре.

2.2.4. Обеспечить при обработке персональных данных их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

2.2.5. Осуществлять хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных.

2.2.6. Соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также соблюдать требования к защите обрабатываемых персональных данных.

2.2.7. В случае выявления неправомерной обработки персональных данных прекратить неправомерную обработку персональных данных в срок, не превышающий трех рабочих дней с даты этого выявления.

2.2.8. В случае достижения цели обработки персональных данных прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.

2.2.9. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва.

2.2.10. Представлять Доверителю по его требованию информацию о ходе исполнения поручения.

2.2.11. По исполнении поручения или при прекращении настоящего договора до его исполнения без промедления возвратить Доверителю персональные данные и представить отчет о выполненном поручении с приложением документов, подтверждающих издержки Поверенного, связанные с обработкой персональных данных.

3. Цена договора и порядок оплаты

3.1. Размер вознаграждения Поверенного составляет [**цифрами и прописью**] рублей.

3.2. Вознаграждение по настоящему договору выплачивается Доверителем Поверенному следующим образом: [**единовременно, не позднее (значение) дней с даты предоставления отчета о выполненном поручении /(значение) % суммы, указанной в** п. 3.1**. настоящего договора, оплачиваются авансом в течение (значение) дней с даты подписания настоящего договора; оставшиеся (значение) % суммы - в течение (значение) дней с даты принятия отчета о выполненном поручении**].

3.3. Издержки Поверенного, понесенные в ходе исполнения настоящего договора, подлежат возмещению Доверителем в полном объеме на основании представленных Поверенным документов, подтверждающих обоснованность расходов.

Возмещение указанных расходов осуществляется Доверителем не позднее [**значение**] дней с даты предоставления отчета о выполненном поручении.

3.4. Расчеты по настоящему договору осуществляются в безналичной форме путем перечисления денежных средств на расчетный счет Поверенного, указанный в настоящем договоре.

3.5. В случае прекращения настоящего договора до того, как поручение будет исполнено, Доверитель обязан возместить Поверенному понесенные при исполнении поручения издержки и уплатить ему вознаграждение соразмерно выполненной им работе.

4. Ответственность сторон

4.1. В случае неисполнения или ненадлежащего исполнения своих обязательств по настоящему договору Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.

4.2. В случае неисполнения или ненадлежащего исполнения поручения Поверенным в сроки, предусмотренные настоящим договором, он лишается права на получение вознаграждения, предусмотренного разделом 3 настоящего договора.

4.3. В случае просрочки в уплате вознаграждения Поверенному Доверитель выплачивает последнему пени в размере [**значение**] процентов от просроченной суммы за каждый день просрочки, но не более [**значение**] процентов от суммы вознаграждения Поверенного по настоящему договору.

4.4. В случае просрочки Доверителем в возмещении расходов Поверенного в соответствии с п. 3.3. настоящего договора Доверитель выплачивает последнему пени в размере [**значение**] процентов от просроченной суммы за каждый день просрочки, но не более [**значение**] процентов от просроченной суммы.

4.5. Ответственность перед субъектом персональных данных за действия Поверенного несет Доверитель. Поверенный, осуществляющий обработку персональных данных по поручению Доверителя, несет ответственность перед Доверителем.

4.6. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных, установленных Федеральным законом от 27.07.2006 г. № 152-ФЗ "О персональных данных", подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

5. Конфиденциальность персональных данных и требования к защите обрабатываемых персональных данных

5.1. Стороны, получившие доступ к персональным данным по настоящему договору, обязуются не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных.

5.2. Стороны при обработке персональных данных обязаны принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

5.3. Обеспечение безопасности персональных данных достигается:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

5.4. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы.

5.5. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

5.6. Поверенный обеспечивает безопасность персональных данных при их обработке в информационной системе.

5.7. Поверенный осуществляет выбор средств защиты информации для системы защиты персональных данных в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона от 27.07.2006 г. № 152-ФЗ "О персональных данных".

5.8. Поверенный производит определение типа угроз безопасности персональных данных, актуальных для информационной системы, с учетом оценки возможного вреда и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона от 27.07.2006 г. № 152-ФЗ "О персональных данных".

5.9. При обработке персональных данных в информационных системах устанавливается [значение] уровень защищенности персональных данных.

6. Основания и порядок прекращения договора

6.1. Настоящий договор подлежит прекращению вследствие:

6.1.1. Отмены поручения Доверителем.

6.1.2. Отказа Поверенного от исполнения поручения.

6.1.3. Вступления в действие решения суда о признании Доверителя несостоятельным (банкротом).

6.1.4. Вступления в действие решения суда о признании Поверенного несостоятельным (банкротом).

6.2. Доверитель вправе отменить поручение, а Поверенный отказаться от него во всякое время. Соглашение об отказе от этого права ничтожно.

6.3. В случае, если настоящий договор поручения прекращается до того, как поручение исполнено Поверенным полностью, Доверитель обязан возместить Поверенному понесенные им при исполнении поручения издержки и уплатить вознаграждение соразмерно выполненной им работе.

6.4. В случае одностороннего отказа Поверенного от исполнения поручения он обязан возместить Доверителю все причиненные этим убытки в случае, если Доверитель будет лишен возможности иначе обеспечить свои интересы.

7. Порядок разрешения споров

7.1. Споры и разногласия, которые могут возникнуть при исполнении настоящего договора, будут по возможности разрешаться путем переговоров между Сторонами.

7.2. В случае, если Стороны не придут к соглашению, споры разрешаются в судебном порядке в соответствии с действующим законодательством Российской Федерации.

8. Заключительные положения

8.1. Настоящий договор составлен в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

8.2. Договор вступает в силу с момента подписания и действует до полного выполнения обязательств по данному договору.

8.3. Все изменения и дополнения оформляются дополнительными соглашениями Сторон в письменной форме, которые являются неотъемлемой частью настоящего договора.

9. Реквизиты и подписи сторон

Доверитель
[вписать нужное]
М. П.

Поверенный
[вписать нужное]
М. П.

Приложение № 15.
Форма запроса на уточнение персональных данных

Кому: Руководителю ООО «_____» ИНН _____
От _____
ФИО субъекта
_____
вид документа
_____
номер документа
_____
дата выдачи и кем выдан документ
_____
контактная информация

Запрос

В соответствии с ч. 1 ст. 14 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» прошу уточнить, обрабатываемые вами, мои персональные данные в соответствии со сведениями:
_____
(указать уточненные персональные данные)
в связи с тем, что
_____
_____.
(указать причину уточнения персональных данных)

____.____.20___г. _____ _____
дата подпись расшифровка

Приложение № 16.
Форма запроса о наличии
и об ознакомлении
с персональными данными

Кому: ООО «_____» ИНН_____
От _____
ФИО субъекта
_____
вид документа
_____
номер документа
_____
дата выдачи и кем выдан документ
_____
контактная информация

Запрос

В соответствии со ст. 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» я имею право получить от вас информацию, касающуюся обработки моих персональных данных.
Прошу вас предоставить мне следующие сведения (нужное отметить «X» или «V»):

□ подтверждение факта обработки моих персональных данных;
□ правовые основания и цели обработки персональных данных;
□ применяемые способы обработки персональных данных;
□ какие лица имеют доступ или могут получить доступ к персональным данным;
□ перечень обрабатываемых персональных данных и источник их получения;
□ срок хранения персональных данных;
□ осуществлялась ли трансграничная передача персональных данных, а, если нет, то предполагается ли такая передача.

Ответ на настоящий запрос прошу направить в письменной форме по адресу:
_____
в установленные законом сроки.

____.____.20___г. _____ _____
дата подпись расшифровка

Приложение № 17.
Форма запроса на уничтожение персональных данных

Кому: ООО «_____» ИНН _____
От _____
ФИО субъекта
_____
вид документа
_____
номер документа
_____
дата выдачи и кем выдан документ
_____
контактная информация

Запрос

В соответствии с ч. 1 ст. 14 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» прошу уничтожить следующие мои персональные данные:
_____
(указать уничтожаемые персональные данные)
в связи с тем, что
_____
_____.
(указать причину уничтожения персональных данных)

Ответ на настоящий запрос прошу направить в письменной форме по адресу:
_____
в установленные законом сроки.

____.____.20___г. _____ _____
дата подпись расшифровка

Приложение № 18.
Форма запроса на блокирование персональных данных

Кому: ООО «_____» ИНН _____

От _____
ФИО субъекта

_____
вид документа

_____
номер документа

_____
дата выдачи и кем выдан документ

_____
контактная информация

Запрос

В соответствии с ч. 1 ст. 14 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» прошу заблокировать следующие мои персональные данные:

_____
(указать блокируемые персональные данные)

на срок:

_____
(указать срок блокирования)

в связи с тем, что

_____
_____.
(указать причину блокирования персональных данных)

Ответ на настоящий запрос прошу направить в письменной форме по адресу:

_____

в установленные законом сроки.

____.____.20___г. _____ _____
дата подпись расшифровка

Приложение № 19.
Форма уведомления об отказе внесения изменений
в персональные данные субъекта

Субъекту персональных данных: _____ ФИО

От ООО «_____» ИНН _____ОГРН _____

Уведомление

Сообщаем Вам о том, что ООО «_____» не может внести изменения в Ваши персональные данные, так как Вами не было предоставлено необходимых документов, подтверждающих запрашиваемые Вами изменения.

Генеральный директор _____ _____

(подпись) (ФИО)

Приложение № 20.
Форма Требования о прекращении передачи (распространения, предоставления, доступа) персональных данных, разрешенных субъектом персональных данных для распространения

Настоящим я, _____, руководствуясь статьей 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», требую прекратить ООО «_____» ИНН _____ обработку моих персональных данных, включающую их распространение через размещение информации обо мне *(указать ресурсы)* в информационной системе

Домен «_____» (https:_____.ru).

Прекращение согласия на вышеуказанное распространение касается следующих моих персональных данных: Фамилия, Имя, Отчество, дата рождения, СНИЛС, ИНН, пол, гражданство, должность.

«___» _____ 20___ года _____

Подпись

Приложение № 21.
Форма уведомления органа
по защите прав субъектов
персональных данных

Г-ну/г-ке _____

В связи с выявлением недостоверности Ваших персональных данных (персональных данных г-на/г-ки_____) могу сообщить следующее.

ООО «_____» ИНН _____ (далее – Общество) были внесены изменения в Ваши персональные данные (персональные данные г-на/г-ки _____): _____Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных (персональных данных г-на/г-ки _____), пожалуйста, обратитесь в Общество.

_____ (должность) _____ (ФИО)

_____ (дата, подпись, печать)

Приложение № 22.
Форма Акта определения уровня защищённости персональных данных

Акт определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных

Комиссия в составе:

Председатель комиссии	Ф.И.О.	Должность
Члены комисии	Ф.И.О.	Должность
	Ф.И.О.	Должность
	Ф.И.О.	Должность

рассмотрев исходные данные об информационной системе персональных данных (ИСПДн) «_____»,

ОПРЕДЕЛИЛА:

Вариант №1 (если в ИСПДн обрабатываются специальные категории ПДн)

Тип ИСПДн	Категориисубъектов	Количество субъектов	Тип актуальных угроз		
			1 тип	2 тип	3 тип
Специальные категории персональных данных	Не сотрудников	Более 100 000	УЗ 1	УЗ 1	УЗ 2
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 00	УЗ 1	УЗ 2	УЗ 3

Вариант №2 (если в ИСПДн обрабатываются биометрические категории ПДн)

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1 тип	2 тип	3 тип
Биометрические категории персональных данных	Не сотрудников	Более100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3

Вариант 3 (если в ИСПДн обрабатываются иные категории ПДн)

Тип ИСПДн	Категории субъектов	Количество субъектов	Типактуальных угроз		
			1 тип	2 тип	3 тип
Иные категории персональных данных	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4
	Сотрудников	Более 100 000	УЗ 1	УЗ 3	УЗ 4
		Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4

Вариант 4 (если в ИСПДн обрабатываются общедоступные категории ПДн)

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1 тип	2 тип	3 тип
Иные категории персональных	Не сотрудников	Более 100 000	УЗ 2	УЗ 2	УЗ 4
		Менее чем 100 000	УЗ 2	УЗ 3	У 4
	Сотрудников	Более 100 000	УЗ 2	УЗ 3	УЗ 4

данных		Менее чем 100 000	УЗ 2	УЗ 3	УЗ 4

Структура ИСПДн: **ЛОКАЛЬНАЯ** (автономная ИСПДн, распределенная ИСПДн);
Наличие подключения информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена (выход в сеть Интернет): **ИМЕЕТСЯ** (отсутствует);
Режим обработки персональных данных: **МНОГОПОЛЬЗОВАТЕЛЬСКИЙ** (однопользовательский);
Режим разграничения прав доступа пользователей ИСПДн:

С РАЗГРАНИЧЕНИЕМ ПРАВ ДОСТУПА (без разграничения прав доступа);
Местонахождение технических средств обработки ПДн в ИСПДн: **В ПРЕДЕЛАХ РФ** (за пределами РФ);
Местонахождение баз данных граждан РФ: **В ПРЕДЕЛАХ РФ** (за пределами РФ).

В соответствии с Постановлением Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных",

РЕШИЛА:
ИСПДн «_____» установить уровень защищенности: **_**.

Председатель комиссии	Личная подпись	Ф.И.О.
Члены комиссии	Личная подпись	Ф.И.О.
	Личная подпись	Ф.И.О.
	Личная подпись	Ф.И.О.

«__» _____ 20__г.

Комментарии:

Специальные категории персональных данных - обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.
Биометрические категории персональных данных - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных.
Иные категории персональных данных – Ф.И.О., место жительства, телефон, паспортные данные, СНИЛС и т.д.
Общедоступные персональные данные - общеизвестные сведения и иная информация, доступ к которой не ограничен (справочники, телефонные книги).

Приложение № 23.
Форма Акта оценки потенциального вреда субъектам персональных данных

Акт оценки потенциального вреда субъектам персональных данных

Дата_____ место проведение _____

Комиссия в составе:

Председатель: (должность) (ФИО)

Члены комиссии:

1. Педагог (ФИО)

2. Делопроизводитель (ФИО)

3. Офис- менеджер (ФИО

в соответствии с п.5 ч.1 ст.18.1 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» (далее - ФЗ «О персональных данных»), произвела экспертную оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения ООО «_____» ИНН _____ ОГРН _____ (далее, - Общество) обязанностей, предусмотренных ФЗ «О персональных данных».

Размер вреда, который может быть причинен субъектам персональных данных в случае нарушения ФЗ «О персональных данных», определяется в соответствии со статьями 15, 151, 152, 1101 Гражданского кодекса Российской Федерации.

Комиссия, проанализировав перечень персональных данных, обрабатываемых в Обществе и состав реализованных организационных и технических мер по защите персональных данных, пришла к выводу, что в результате нарушения одного из свойств безопасности персональных данных (конфиденциальности, целостности, доступности), возможны незначительные негативные последствия в социальной, финансовой или иных областях деятельности субъекта персональных данных, а Общество как оператор персональных данных, может выполнять возложенные на него функции с незначительным снижением эффективности.

Исходя из полученных данных, комиссия установила, что уровень потенциального вреда, который может быть причинен субъекту персональных данных в случае нарушения одного из свойств безопасности персональных данных, оценивается как - низкий.

Подписи членов комиссии:

Приложение № 24.
Форма Акта об уничтожении
персональных данных

АКТ
об уничтожении персональных данных
в информационных системах персональных данных

Комиссия, созданная приказом по ООО «_____» от _____ № _____, в составе
(дата приказа) (номер приказа)
председателя комиссии
_____
(должность и фамилия, имя, отчество)
членов комиссии
_____
(должность и фамилия, имя, отчество)
_____
(должность и фамилия, имя, отчество)
_____
(должность и фамилия, имя, отчество)
в соответствии со ст. 21 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" составила настоящий акт об уничтожении персональных данных субъектов персональных данных, обрабатываемых ООО «_____» ИНН _____ ОГРН _____.
Фамилия, имя, отчество (при наличии) субъекта (субъектов) или иная информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены:
_____
Перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных:
_____
Наименование информационной (информационных) системы (систем) персональных данных, из которой (которых) были уничтожены персональные данные субъекта (субъектов) персональных данных (в случае обработки персональных данных с использованием средств автоматизации):_____
Способ уничтожения персональных данных:
_____
Причина уничтожения персональных данных:
_____
Дата уничтожения персональных данных субъекта (субъектов) персональных данных:
_____

Акт подлежит хранению до _____
(дата, прибавить три года с даты акта)

Председатель комиссии _____ _____
(подпись) (фамилия, имя, отчество)
Члены комиссии __ _____ _____
(подпись) (фамилия, имя, отчество)
_____ _____
(подпись) (фамилия, имя, отчество)

Приложение №2 к приказу от _____ № _____

АКТ
об уничтожении персональных данных
в случае обработки персональных данных без использования средств автоматизации

Комиссия, созданная приказом по ООО «_____» от _____ № _____, в составе
(дата приказа) (номер приказа)
председателя комиссии _____
(должность и фамилия, имя, отчество)
членов комиссии _____
(должность и фамилия, имя, отчество)
_____
(должность и фамилия, имя, отчество)
_____
(должность и фамилия, имя, отчество)
в соответствии со ст. 21 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" составила настоящий акт об уничтожении персональных данных субъектов персональных данных, обрабатываемых ООО «_____» ИНН _____ ОГРН _____.
Фамилия, имя, отчество (при наличии) субъекта (субъектов) или иная информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены: _____
Перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных: _____
Наименование уничтоженного материального (материальных) носителя (носителей), содержащего (содержащих) персональные данные субъекта (субъектов) персональных данных, с указанием количества листов в отношении каждого материального носителя (в случае обработки персональных данных без использования средств автоматизации): _____
_____
Способ уничтожения персональных данных: _____
Причина уничтожения персональных данных: _____
Дата уничтожения персональных данных субъекта (субъектов) персональных данных: _____

Акт подлежит хранению до _____
(дата, прибавить три года с даты акта)

Председатель комиссии _____ _____
(подпись) (фамилия, имя, отчество)
Члены комиссии _____ _____
(подпись) (фамилия, имя, отчество)
_____ _____
(подпись) (фамилия, имя, отчество)
_____ _____
(подпись) (фамилия, имя, отчество)

Приложение № 25.
Форма уведомления об устранении неправомерных действий с персональными данными

Субъекту персональных данных
_____
ФИО субъекта, адрес
_____

Уведомление

Сообщаем Вам о том, что допущенные нарушения при обработке персональных данных, а именно:

_____
_____.

(указать допущенные нарушения)

_____ _____ _____

Должность руководителя организации Подпись И.О. Фамилия

Приложение № 26.
Форма Журнала учёта прав доступа
к информации с персональными данными

№№	Сведения о лице предоставляемому доступ к персональным данным	Состав предоставляемых персональных данных	Цель получения персональных данных	Отметка в предоставлении персональных данных	Дата предоставления персональных данных	Подпись лица которому предоставляются данные	Подпись ответственного сотрудника
1	2	3	4	5	6	7	8

Приложение № 27.
Журнал учета обращений субъектов
персональных данных о выполнении их законных
прав в области защиты персональных данных

№ №	Сведения о запрашивающем лице	Краткое содержание обращения	Цель получения информации	Отметка о предоставлении или отказе в предоставлении информации	Дата передачи/отказа в предоставлении информации	Подпись запрашивающего лица	Подпись ответственного сотрудника
1	2	3	4	5	6	7	8

Приложение № 28.
Форма Журнала учета запросов
субъектов персональных данных

№ №	Сведения о запрашивающем лице	Состав запрашиваемых персональных данных	Цель получения персональных данных	Отметка о передаче или отказе в передаче персональных данных	Дата передачи/отказа в передаче персональных данных	Подпись запрашивающего лица	Подпись ответственного сотрудника
1	2	3	4	5	6	7	8

Приложение № 29.
Форма Журнала учета съемных носителей, содержащих персональные данные

№ п/п	Уч. № носителя	Тип носителя	Номер (серийный/ инвентарный)	Место хранения	Расписка в получении		Дата уничтожения носителя	№ и дата акта уничтожения носителя	ФИО, подпись администратора безопасности
					ФИО, дата получения, подпись	ФИО, дата сдачи, подпись			
1	2	3	4	5	6	7	8	9	10

Приложение № 30.
Форма Журнала учета прохождения первичного инструктажа работниками, имеющими доступ к обработке персональных данных

№ п/п	ФИО работника	Дата прохождения инструктажа	Подпись работника	ФИО должностного лица, проводившего инструктаж	Подпись должностного лица
1	2	3	4	5	6

Приложение № 31.
Инструкция ответственного
а организацию обработки персональных данных

Содержание

Перечень терминов и сокращений

Обозначение Описание

Безопасность информации состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Обработка ПДн любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

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

1. Общие положения

Настоящая Инструкция о лице, ответственном за обработку персональных данных, в наименование организации (далее — Инструкция) определяет основные задачи, функции, права Ответственного за организацию обработки персональных данных (далее — ПДн) в наименование организации. Настоящая Инструкция разработана во исполнение требований Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Ответственный за организацию обработки ПДн является работником наименование организации и назначается приказом директора наименование организации. В своей деятельности Ответственный за организацию обработки ПДн руководствуется законодательством Российской Федерации, настоящей Инструкцией и другими внутренними нормативными документами наименование организации.

2. Функции ответственного за организацию обработки ПДн

Основными функциями Ответственного за организацию обработки ПДн являются:

- обеспечение соблюдения требований законодательства Российской Федерации в части обработки ПДн, нормативных правовых актов, регулирующих обработку ПДн, а также внутренних организационно-распорядительных документов;
- обеспечение правомерности обработки персональных данных, а также соответствия процессов обработки ПДн заявленным целям;
- обеспечение соответствия договоров и соглашений, заключаемых с третьими лицами и связанных с передачей, совместной обработкой или поручением обработки персональных данных, требованиям законодательства Российской Федерации;
- мониторинг изменений законодательства Российской Федерации по вопросам обработки ПДн;
- разработка внутренних нормативных документов по организации обработки ПДн и контроль за их исполнением;
- организация мероприятий по повышению осведомленности работников Учреждения по вопросам обработки ПДн;
- изучение и анализ вновь выходящих нормативно-правовых и методических документов в области обработки ПДн;

 организация и ведение учета лиц, допущенных к обработке ПДн в наименование организации.

3. Права и обязанности Ответственного за организацию обработки ПДн

Ответственный за организацию обработки ПДн имеет право:

 по согласованию с директором наименование организации давать структурным подразделениям наименование организации и отдельным работникам обязательные для исполнения указания по вопросам, входящим

в компетенцию Ответственного за организацию обработки ПДн;

 запрашивать и получать от структурных подразделений наименование организации сведения, справочные и другие материалы, необходимые

для исполнения своих обязанностей в соответствии с настоящим Положением;

 инициировать проведение служебных расследований по фактам нарушения установленных правил обработки ПДн и обеспечения безопасности ПДн и предоставлять директору наименование организации отчет

о проведенных служебных расследованиях с представлением информации

о субъектах доступа, нарушивших режим доступа;

 готовить предложения о привлечении к проведению работ

по обеспечению безопасности ПДн на договорной основе юридических лиц, имеющих лицензии на право проведения работ в области защиты информации;

 совместно с Ответственным за обеспечение безопасности ПДн вносить предложения по совершенствованию деятельности наименование организации в области обеспечения безопасности ПДн при их обработке.

Ответственный за организацию обработки ПДн обязан:

 осуществлять внутренний контроль за соблюдением работниками Учреждения законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;

 доводить до сведения работников Учреждения положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;

 организовывать прием и обработку обращений запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;

 добросовестно выполнять функции, возложенные на него;

 не разглашать ПДн, полученные в рамках выполнения обязанностей.

Ответственный за организацию обработки ПДн должен знать:

 законодательные и нормативно-правовые акты, методические

и нормативные материалы по вопросам, связанным с обеспечением информационной безопасности и безопасности ПДн;

 процессы обработки ПДн, действующие в наименование организации;

 используемые информационные технологии Обработки ПДн;

 систему организации защиты ПДн;

 основы работы и функционирования;

 категории обрабатываемых ПДн, категории субъектов ПДн, работников, допущенных к обработке ПДн.

4. Обязанности ответственного за организацию обработки ПДн

в случае обнаружения нарушений

Ответственный за организацию обработки ПДн для проведения расследования привлекает комиссию Учреждения, назначенную приказом директора наименование организации. Комиссия обязана установить, имела

ли место утечка ПДн и обстоятельства, ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по обработке ПДн, установить причины и условия,

способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования председатель экспертной комиссии принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

Все структурные подразделения и работники, работающие с ПДн, обязаны содействовать проведению служебной проверки.

Работа с ПДн может возобновляться только после устранения всех выявленных нарушений и нейтрализации их последствий.

5. Ответственность

Ответственный за организацию обработки ПДн несет ответственность (гражданскую, уголовную, административную, дисциплинарную) за неисполнение либо ненадлежащее исполнение должностных обязанностей.

Приложение № 32.
Инструкция ответственного за обеспечение безопасности персональных данных

Инструкция
ответственного по обеспечению безопасности персональных данных

1. Общие положения

1.1. Инструкция ответственного по обеспечению безопасности персональных данных в ООО «_____» (далее – Инструкция) разработана в целях обеспечения безопасности персональных данных (далее - ПДн) при их обработке в ООО «_____» (далее Общество).

1.2. Ответственный по обеспечению безопасности ПДн в Обществе назначается приказом генерального директора.

1.3. Ответственный по обеспечению безопасности ПДн в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными нормативными правовыми актами, настоящей Инструкцией, а также иными нормативными правовыми актами Общества, регламентирующими вопросы обработки ПДн и несет персональную ответственность за свои действия.

2. Обязанности ответственного по обеспечению безопасности ПДн

2.1. Осуществлять внутренний контроль за соблюдением сотрудникамиОбщества законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн.

2.2. Доводить до сведения сотрудников Общества положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн.

3. Основные функции ответственного по обеспечению безопасности ПДн

3.1. Проведение единой политики Общества и координация работ по обеспечению безопасности ПДн.

3.2. Планирование мероприятий по организации обеспечения безопасности ПДн.

3.3. Организация мероприятий по техническому обеспечению безопасности ПДн.

3.4. Организация мероприятий, направленных на предотвращение несанкционированного доступа к ПДн или передачи их лицам, не имеющим права доступа к такой информации.

3.5. Организация постоянного контроля за обеспечением уровня защищенности ПДн.

3.6. Координация действий по подготовке информационных систем к аттестации по выполнению требований по обеспечению безопасности ПДн.

3.7. Контроль за исполнением организационных и распорядительных документов по обеспечению безопасности Общества.

3.8. Рассмотрение предложений по устранению недостатков и предупреждению нарушений в части обеспечения безопасности ПДн, осуществление контроля за устранением нарушений.

3.9. Организация повышения информированности сотрудников по вопросам обеспечения безопасности ПДн.

3.10. Изучение отчетов о состоянии работ по обеспечению безопасности Общества.

4. Права ответственного по обеспечению безопасности ПДн

Ответственный по обеспечению безопасности ПДн имеет право:

4.1. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам обеспечения безопасности ПДн.

4.2. Осуществлять контроль за реализацией требований организационных и распорядительных документов по обеспечению безопасности ПДн, а также предписаний государственных органов контроля.

4.3. Контролировать деятельность сотрудников Общества в части выполнения ими требований по обеспечению безопасности ПДн.

4.4. Принимать решение о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) ПДн.

4.5. Привлекать в установленном порядке необходимых специалистов из числа сотрудников Общества для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения безопасности ПДн.

5. Ответственность ответственного по обеспечению безопасности ПДн

Ответственный по обеспечению безопасности ПДн несет персональную ответственность за:

– правильность и объективность принимаемых решений по вопросам защиты ПДн;

– правильное и своевременное выполнение требований организационных и распорядительных документов, принятых в Обществе по вопросам защиты ПДн;

– выполнение возложенных на него обязанностей, предусмотренных настоящей Инструкцией;

– качество проводимых работ по обеспечению безопасности ПДн в соответствии с функциональными обязанностями;

соблюдение трудовой дисциплины, охраны труда.

Приложение № 33.
Инструкция по учету лиц,
допущенных к работе
с персональными данными

Инструкция по учету лиц, допущенных к работе с персональными данными в информационных системах ООО «_____» (далее – Общество).

1. Настоящая Инструкция определяет порядок учета лиц, допущенных к работе с персональными данными в информационных системах.

2. В журнале указываются сведения о проведении инструктажа пользователей информационных систем персональных данных правилам работы с системой защиты персональных данных.

3. Основанием для допуска работника к персональным данным является «Список лиц, доступ которых к персональным данным необходим для выполнения трудовых обязанностей» на основании приказа вынесенного руководством Общества.

4. Основанием для прекращения допуска работника к персональным данным является исключение работника из перечня работников, допущенных к персональным данным.

5. Журнал ведется администратором безопасности.

6. Форма ведения журнала определена в приложении к Инструкции.

Форма Журнала учета лиц, допущенных к работе с персональными данными в информационных системах ООО «_____» ИНН _____

Сведения о допуске к персональным данным					Сведения о прекращении допуска к персональным данным				
№ п/п	Должность и ФИО работника	Наименование информационной системы	Дата утверждения «Перечня лиц…»	Дата и подпись допускаемого	Работник, проводивший инструктаж	Подпись инструктируемого лица	Дата утверждения «Перечня лиц…» или дата приказа об увольнении	Номер приказа об увольнении	Дата и подпись лица об ознакомлении с документом, прекращающим допуск к ПДн
1	2	3	4	5	6	7	8	9	10

Приложение № 34.
Инструкция по проведению инструктажа,
допущенных к работе с персональными данными

Инструкция по проведению инструктажа лиц,
допущенных к работе с персональными данными

1. Настоящая инструкция разработана с целью обеспечения безопасности персональных данных, обрабатываемых в ООО «_____» ИНН _____ ОГРН _____ (далее – Общество).

2. При поступлении на работу сотрудника, которому для выполнения своих трудовых обязанностей необходим доступ к персональным данным (далее – новый сотрудник), ответственный сотрудник за проведение инструктажа лиц, допущенных к работе с персональными данными в Обществе на основании имеющихся локальных актов в соответствии с пунктом 6 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»:

2.1. проводит ознакомление нового сотрудника с положениями законодательства Российской Федерации о персональных данных;

2.2. проводит ознакомление нового сотрудника с Политикой в отношении обработки персональных данных Общества;

2.3. знакомит нового сотрудника с ответственностью за неисполнение требований по обеспечению безопасности персональных данных в информационных системах персональных данных, предусмотренной действующим законодательством Российской Федерации;

2.4. делает отметку в Журнале учета прохождения первичного инструктажа сотрудниками, допущенными к работе с персональными данными о проведении инструктажа новому сотруднику.

Новый сотрудник может приступить к исполнению своих непосредственных трудовых обязанностей, связанных с обработкой персональных данных, только после успешного прохождения первичного инструктажа.

Приложение № 35.
Инструкция по учёту и хранению
съёмных носителей персональными данными

ИНСТРУКЦИЯ
по учёту и хранению съёмных носителей персональных данных

1.Общие положения

1.1. Настоящая «Инструкция по учёту и хранению съёмных носителей персональных данных» (далее — Инструкция) определяет порядок работы со съёмными носителями персональных данных в ООО «_____» ИНН _____ ОГРН _____ (далее — Оператор) в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иными нормативными правовыми актами РФ в области защиты персональных данных.

1.2. С Инструкцией знакомятся под подпись и выполняют её все лица, допущенные к обработке персональных данных распоряжением о допуске к обработке персональных данных.

2.Определения

Съёмный носитель персональных данных — носитель информации, используемый для хранения и передачи персональных данных в электронной форме.

Пользователь — работник Оператора или сотрудник по договору гражданско-правового характера, допущенный к обработке персональных данных распоряжением о допуске к обработке персональных данных.

3. Порядок работы со съёмными носителями

3.1. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, выдаёт съёмные носители пользователям только в случаях производственной необходимости.

3.2. Все съёмные носители персональных данных учитываются и выдаются пользователям под подпись.

3.3 Пользователям, получившим съёмные носители персональных данных под подпись, запрещается передавать их третьим лицам.

3.4. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, изымает съёмные носители персональных данных при увольнении пользователя.

3.5. Все съёмные носители персональных данных хранятся в запираемых шкафах или сейфах (металлических шкафах) с кодовыми или внутренними замками (с не менее чем двумя дубликатами ключей).

3.6. Допускается хранение съёмных носителей персональных данных вне запираемых шкафов или сейфов (металлических шкафов) при условиях уничтожения персональных данных в соответствии с Инструкцией по порядку уничтожения и обезличивания персональных данных, либо если на съёмном носителе персональных данных хранятся только персональные данные в зашифрованном или обезличенном виде.

3.7. Право на перемещение съёмных носителей информации за пределы территории, на которой осуществляется обработка, имеют только те лица, которым это необходимо для выполнения своих должностных обязанностей.

3.8. Использование неучтённых съёмных носителей для обработки персональных данных фиксируется как несанкционированное, а ответственный за обеспечение безопасности персональных данных инициирует служебную проверку. По факту выясненных обстоятельств составляется Акт проведения расследования инцидента.

3.9. Пользователи, в случаях утраты или кражи съёмных носителей персональных данных, сообщают об этом ответственному за обеспечение безопасности персональных данных.

3.10. Съёмные носители персональных данных, пришедшие в негодность, или отслужившие в установленный срок, подлежат уничтожению в соответствии с Инструкцией по порядку уничтожения и обезличивания персональных данных. По результатам уничтожения составляется Акт уничтожения персональных данных.

4. Порядок организации учёта съёмных носителей

4.1. На каждом съёмном носителе персональных данных размещается этикетка с уникальным учётным номером.

4.2. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, при выдаче, приёме, уничтожении съёмных носителей персональных данных вносит в Журнал учета съёмных носителей персональных данных (Приложение 1): учётный номер, размещённый на этикетке на съёмном носителе персональных данных; тип съёмного носителя (ШВ-накопитель, внешний жёсткий диск, СБ/БУБ диск); серийный или инвентарный номер съёмного носителя; место хранения (номер запираемого шкафа или сейфа, номер помещения); дату и номер Акта уничтожения персональных данных в случае уничтожения съёмного носителя; подпись.

4.3. Пользователи при получении либо сдаче съёмных носителей персональных данных заносят в Журнал учёта съёмных носителей персональных данных свои фамилию, имя, отчество, ставят дату и подпись.

5.Ответственность

5.1. Все работники Оператора, допущенные в установленном порядке к работе с персональными данными, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством за обеспечение сохранности и соблюдению правил работы с персональными данными.

5.2. Ответственность за доведение требований настоящей Инструкции до работников Оператора несёт ответственный за организацию обработки персональных данных.

5.3. Ответственность за обеспечение мероприятий по реализации требований настоящей Инструкции, в том числе учёт, выдачу, уничтожение съёмных носителей персональных данных несёт ответственный за обеспечение безопасности персональных данных.

ЖУРНАЛ УЧЁТА съёмных носителей персональных данных

№ п/п	Учётный номер	Тип носителя	Номер (серийный/ инвентарный)	Место хранения	Расписка в получении		Дата и номер акта уничтожения	Подпись ответственного лица	Примечание
					ФИО, дата получения, подпись	ФИО, дата сдачи, подпись			
1.	2.	3.	4.	5.	6.	7.	8.	9.	10.

Приложение № 36.
Политика конфиденциальности
по персональным данным

Политика конфиденциальности персональных данных

Настоящая Политика конфиденциальности персональных данных (далее – Политика) разработана в соответствии с требованиями Федерального закона РФ от 27.07.2006 года № 152-ФЗ «О персональных данных», Общим регламентом Европейского союза по защите данных 2016/679 (General Data Protection Regulation), Конвенцией Совета Европы от 28.01.1981 СЕД №108 «О защите физических лиц в отношении автоматизированной обработки данных личного характера» и действует в отношении Персональных данных, которые сайт https:// _____ (далее – Сайт) может получить от Пользователя.

1. Определение терминов

1.1.В настоящей Политике используются следующие термины:

1.1.1.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;

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

1.1.3.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;

1.1.4.Конфиденциальность персональных данных – обязательное для соблюдения Оператором и иными лицами, получившими доступ к Персональным данным, требование не передавать третьим лицам и не распространять Персональные данные без согласия Субъекта персональных данных, если иное не предусмотрено федеральным законом;

1.1.5.Сайт – совокупность связанных между собой веб-страниц, размещенных в сети Интернет по уникальному адресу (URL) - _____;

1.1.6.Пользователь сайта (Пользователь) – лицо, осуществляющее регистрацию на Сайте и/или имеющее реквизиты доступа к Сайту (логин и пароль);

1.1.7. Файл Cookie – небольшой фрагмент данных, который Сайт отправляет и запрашивает у браузера, используемого на компьютерах или мобильных устройствах Пользователя. Cookies позволяют Сайту «узнавать» Пользователя и «запоминать» его действия. Файлы Cookies хранятся локально на компьютерах и/или мобильных устройствах Пользователя. Пользователь может удалять сохраненные файлы Cookies по своему желанию, а также отключать возможность их использования. Другие аналогичные технологии для сбора и хранения данных в целях настоящей Политики приравниваются к файлам Cookies;

1.1.8. IP-адрес – уникальный сетевой адрес узла в компьютерной сети, через который Пользователь получает доступ к Сайту.

2. Общие положения

2.1. Задачей настоящей Политики конфиденциальности является определение способов и целей, для которых осуществляется сбор и использование Персональных данных, чтобы Пользователь мог сделать осознанный выбор в отношении использования Сайта;

2.2.Использование Сайта Пользователем означает согласие с настоящей Политикой и условиями обработки Персональных данных Пользователя;

2.3.В случае несогласия с условиями Политики Пользователь должен прекратить использование Сайта;

2.4.Настоящая Политика применяется к конкретному Сайту;

2.5.Пользователь гарантирует достоверность предоставляемых им Персональных данных. Оператор не осуществляет проверку достоверности предоставляемых пользователями сайта персональных данных, полагая, что они действуют добросовестно и поддерживают информацию о своих персональных данных в актуальном состоянии.

3. Предмет политики

3.1.Настоящая Политика устанавливает обязательства Оператора по неразглашению и защите Персональных данных, которые Пользователь предоставляет при регистрации на мероприятии, при использовании Сайта, а также при подписке на информационную рассылку;

3.2.Категории обрабатываемых Персональных данных: фамилия; имя; отчество; телефон; e-mail; название компании или образовательного учреждения.

3.3. Использование файлов Cookies:

3.3.1.Файлы Cookies, сведения о действиях Пользователей на Сайте, сведения об оборудовании Пользователя, дата и время сессии обрабатываются Оператором в целях поддержки и улучшения работы Сайта. Оператор также использует данные сервисов вебаналитики «Яндекс.Метрика», «Google Analytics» для анализа поведения Пользователя на Сайте и улучшения работы Сайта.

3.3.2.Пользователь может выключить (отключить) Cookies, при этом Пользователь может обнаружить, что некоторые разделы Сайта не работают должным образом. Инструкцию по управлению файлами Cookies в браузере можно найти в документации браузера.

4. Цели и способы обработки персональных данных

4.1.Обработка Персональных данных Пользователей осуществляется в следующих целях:

4.1.1.Организации участия Пользователя в Мероприятии;

4.1.2.Улучшения работы Сайта;

4.1.3. Создания учетной записи, предоставления доступа к контенту Сайта;

4.1.4.Рассылки уведомлений, новостей о данном Мероприятии и других будущих мероприятиях, проводимых Организатором Мероприятия;

4.1.5.Проведение опросов, анкетирований Пользователя по вопросам, связанным с проведением Мероприятия;

4.1.6.Печати бейджа участника Мероприятия;

4.1.7.Контроля доступа на Мероприятие;

4.1.8. Учета посетителей Мероприятия.

4.2.Обработка Оператором Персональных данных Пользователей осуществляется только в случае предоставления Пользователем согласия на обработку своих Персональных данных. Согласие уполномочивает Оператора передавать данные Организатору мероприятия, который берет на себя ответственность за обработку и использование Персональных данных, гарантируя их безопасность в соответствии с действующим законодательством.

4.3.Безопасность Персональных данных в соответствии с требованиями законодательства Российской Федерации в области защиты Персональных данных обеспечивается реализацией организационных, технических и правовых мер.

4.4.Оператор обязуется не осуществлять продажу, обмен, опубликование, либо разглашение иными возможными способами переданных Персональных данных.

4.5.Обработка Персональных данных осуществляется с использованием средств автоматизации или без использования таких средств с осуществлением следующих действий: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, блокирование, удаление и передача Персональных данных: ООО «_____» ИНН _____ ОГРН _____ – оператор персональных данных.

5. Сроки обработки персональных данных

5.1.Обработка Персональных данных Пользователей осуществляется 30 дней после даты проведения мероприятия.

5.2.Обработка Персональных данных с целью рассылки уведомлений, новостей о предстоящих мероприятиях (включая информирование посредством телефонной связи) осуществляется в течение одного года после даты проведения мероприятия.

5.3.Обработка Персональных данных Пользователей может осуществляться после удаления аккаунта в случаях, предусмотренных законодательством Российской Федерации.

6. Правила взаимодействия Оператора и Субъекта данных

6.1.Оператор персональных данных, вправе:

6.1.1.предоставлять Персональные данные Субъектов государственным и надзорным органам (являющимся в данном случае третьими лицами), если это предусмотрено законодательством (налоговые, правоохранительные органы и др.);

6.1.2.отказывать в предоставлении Персональных данных в случаях, предусмотренных законодательством;

6.1.3.использовать Персональные данные субъекта без его согласия, в случаях, предусмотренных законодательством;

6.1.4.отстаивать свои интересы в суде.

6.2.Оператор персональных данных обязан:

6.2.1.использовать Персональные данные Пользователей исключительно для целей, указанных в настоящей Политике конфиденциальности;

6.2.2.обеспечить хранение Персональных данных Пользователей в тайне, не разглашать их без согласия Пользователя, а также не осуществлять продажу, обмен, публикацию, либо разглашение иными возможными способами переданных Персональных данных Пользователя.

6.3.Субъект, персональных данных имеет право:

6.3.1.требовать уточнения своих Персональных данных, их блокирования или уничтожения в случае, если Персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

6.3.2.требовать перечень Персональных данных Субъекта и источник их получения;

6.3.3.получать информацию о сроках обработки своих Персональных данных, в том числе о сроках их хранения;

6.3.4.требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его Персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

6.3.5.обжаловать в уполномоченный орган по защите прав субъектов Персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его Персональных данных;

6.3.6.на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

7. Дополнительные условия

7.1.Политика вступает в силу с момента ее размещения на Сайте;

7.2.Оператор вправе вносить изменения в настоящую Политику без согласия и/или уведомления Пользователя. Изменения вступают в силу с момента публикации обновленной Политики на Сайте;

7.3.В случае возникновения вопросов относительно настоящей Политики конфиденциальности или подозрений, что конфиденциальность Персональных данных была нарушена, необходимо связаться с Оператором персональных данных по электронной почте: _____.

Приложение № 37.
Инструкция пользователя информационной системы персональных данных

ИНСТРУКЦИЯ
пользователя информационной системы персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция пользователя информационных систем персональных данных ООО «_____» (далее- Общество) определяет общие правила работы работников в информационных системах персональных данных Общества.

1.2. В настоящей Инструкции применяются следующие термины и определения:

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

1.2.2. 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.

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

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

1.2.5. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

1.2.6. Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.2.7. Несанкционированный доступ (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

1.2.8. Посторонние лица – лица, которые не имеют права самостоятельного доступа в помещение и (или) не имеют права самостоятельного доступа в информационные системы и (или) не имеют допуска к защищаемой информации.

1.2.9. Средство защиты информации от несанкционированного доступа (СЗИ НСД) – программное, техническое или программнотехническое средство, направленное на предотвращение или существенное затруднение несанкционированного доступа к информации.

1.2.10. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных Общества.

1.2.11. Администратор ИСПДн - лицо, выполняющее функции по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники ИСПДн в пределах своей зоны ответственности.

1.3. Пользователем является каждый работник Общества, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.4. Для каждого пользователя создается уникальная учетная запись для авторизации в сети и в информационных системах. Учетная запись пользователя – это его реквизиты в сети, основными параметрами которой являются имя пользователя и его пароль.

1.5. Пользователь в своей работе руководствуется настоящей Инструкцией, Положением об обработке персональных данных Общества, руководящими и нормативными актами ФСТЭК

России и ФСБ России и локальными нормативными актами Общества, регламентирующими обработку персональных данных.

1.6. Методическое руководство работой Пользователя осуществляет Администратор ИСПДн.

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

2.1. Знать и выполнять требования законодательных актов Российской Федерации, настоящей Инструкции и других внутренних документов Общества, регламентирующих порядок обработки персональных данных.

2.2. Выполнять на автоматизированном рабочем месте только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных.

2.4. Использовать для хранения персональных данных только определенные места хранения и учтенные носители персональных данных Общества.

2.5. Не разглашать персональные данные, которые будут доверены или станут известны в ходе рабочего процесса во время выполнения должностных (договорных) обязанностей.

2.6. Не сообщать устно или письменно, не передавать в каком-либо виде третьим лицам и не раскрывать публично персональные данные без соответствующего разрешения непосредственного руководителя.

2.7. Незамедлительно, в кратчайшие сроки, сообщать непосредственному руководителю об утрате или недостаче носителей информации, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению персональных данных.

2.8. Незамедлительно сообщать в отдел разработки, сопровождения и обслуживания информационных систем о замеченных случаях нарушения компьютерной безопасности (несанкционированный доступ к оборудованию и информации, несанкционированное искажение или уничтожение информации).

2.9. При прекращении работ (трудовых отношений) все материальные носители, содержащие персональные данные (флэш-накопители, дискеты, компакт-диски, документы, черновики, распечатки на принтерах, кино- и фотоматериалы, модели, промышленные образцы и пр.), передать непосредственному руководителю.

2.10. Использовать информационные ресурсы Общества и переданные в распоряжение технические средства хранения, обработки и передачи информации исключительно для выполнения порученных работ, должностных (договорных) обязанностей.

2.11. Соблюдать требования парольной политики (раздел 3 настоящей Инструкции).

2.12. Соблюдать требования антивирусной защиты (раздел 4 настоящей Инструкции).

2.13. Пользователи, имеющие выход в Интернет, обязаны соблюдать правила при работе в сетях связи общего пользования и (или) сетях международного информационного обмена – Интернет (раздел 5 настоящей Инструкции).

2.14. Пользователи, работающие с персональными данными контрагентов организации, все наработанные файлы должны хранить на определенном Администратором сетевом диске/папке.

2.15. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.16. Обо всех выявленных нарушениях, связанных с порядком обработки персональных данных, а также для получений консультаций по вопросам обработки персональных данных необходимо обращаться к Администратору ИСПДн или ответственному за организацию обработки персональных данных.

2.17. Пользователям запрещается:

2.17.1. Нарушать установленные в Общества правила обработки персональных данных.

2.17.2. Использовать компоненты программного и аппаратного обеспечения Общества в неслужебных целях.

2.17.3. Оставлять свое рабочее место без присмотра, предварительно не заблокировав (штатными средствами операционной системы Windows или Linux – комбинацией клавиш [WIN] + [L] или [CTRL] + [ALT] + [DEL] с дальнейшим нажатием кнопки «Блокировка» появившегося меню, либо при помощи штатных средств защиты информации от несанкционированного доступа при их наличии).

2.17.4. Оставлять без присмотра или неубранными в хранилища (шкаф, сейф) носители или документы, содержащие персональные данные.

2.17.5. Записывать и хранить конфиденциальную информацию (в том числе персональные данные) на неучтенных носителях информации (оптических (CD) дисках, гибких магнитных дисках, флеш-накопителях и т.п.).

2.17.6. Самовольно изменять состав и конфигурацию используемых программных, аппаратных, программно-аппаратных средств, самовольно устанавливать программное обеспечение, отключать/подключать оборудование или изменять режимы его работы.

2.17.7. Самовольно подключать компьютер к ЛВС Общества, изменять IP-адрес, MAC-адрес и иные настройки сети компьютера.

2.17.8. Производить действия, направленные на получение несанкционированного доступа к АРМ и серверам, равно как и любым другим узлам сети Интернет, в том числе:

– действия, направленные на нарушение нормального функционирования элементов сети (компьютеров, другого сетевого оборудования или программного обеспечения);

– установка программного обеспечения, осуществляющего перехват информации (информационных пакетов), адресованной другим пользователям;

– действия, направленные на получение несанкционированного доступа к информационным ресурсам, в последующем использовании такого доступа;

– уничтожение, модификация программного обеспечения или данных без согласования с непосредственным руководителем или владельцами этого ресурса;

– попытки подбора паролей к любым информационным ресурсам методом перебора всех возможных вариантов паролей, либо атак по словарю;

– умышленные действия по созданию, использованию и распространению вредоносных программ, в том числе направленных на получение несанкционированного доступа к любым информационным и служебным ресурсам (как внутри Общества, так и вне), либо на нарушение целостности и работоспособности этих систем;

– действия по сканированию локальной сети с целью определения ее внутренней структуры, списков открытых портов, наличия существующих сервисов и уязвимостей.

2.17.9. Самовольно изменять параметры средств защиты информации (в том числе и средств антивирусной защиты), а также завершать их работу и (или) самостоятельно их устанавливать.

2.17.10. Самостоятельно разрабатывать или использовать нерегламентированные (без разрешения непосредственного руководителя, не относящиеся к производственному процессу) программы (например, игры; IM-клиенты, такие как Google Messenger, Microsoft Messenger, ICQ и т.п.; P2Pклиенты: Kazaa, eMule, Skype и т.п.). 2.17.11. Разрешать посторонним лицам работать под своей учетной записью на АРМ.

2.17.12. Пересылать конфиденциальную информацию, в том числе персональные данные, по каналам связи в открытом виде, в том числе Интернет, по телефону, факсу, электронной почте и т.п. (без использования средств шифрования или шифрования и электронной подписи).

2.17.13. Получать доступ к сети Интернет любыми способами, кроме как установленными настоящей Инструкцией, например, при помощи несанкционированно установленных на АРМ модемов и т. п.

2.17.14. Самовольно создавать совместно используемые сетевые ресурсы (папки общего доступа) на своих компьютерах и файловых серверах, несанкционированно удалять или изменять права доступа к ним.

2.17.15. В случае возникновения любых механических неисправностей в оборудовании осуществлять самостоятельные попытки их устранения.

2.17.16. Препятствовать должностным лицам при проведении проверок и служебных расследований, связанных с обеспечением безопасности информации.

2.17.17. Удалять или искажать программы и файлы с конфиденциальной информацией, в том числе персональных данных, и иной важной информацией (например, системной, необходимой для функционирования информационных систем).

2.17.18. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению внештатной ситуации. Об обнаружении такого рода ошибок – ставить в известность руководителя своего подразделения и сотрудников, ответственных за установку и (или) сопровождение программного обеспечения.

2.17.19. Подключать к ЛВС Общества личные средства вычислительной техники: ноутбуки, карманные компьютеры, смартфоны и т.п., а также личные носители и накопители информации. В случае необходимости переноса информации с личных носителей информации обращаться к системному администратору.

3. ПАРОЛЬНАЯ ПОЛИТИКА

3.1. Общие требования к паролям:

3.1.1. Минимальное требование: буквенно-цифровой пароль. Желательно использовать буквы в верхнем или нижнем регистрах, цифры или специальные символы (например, ~ ! @ # $ % ^ & * ( ) _ - + = | \ ? / . , : ; ’] [{ } < > . и т.п.).

3.1.2. Минимальная длина пароля: не менее 8-ми (восьми) символов.

3.1.3. Максимальный срок действия пароля: 180 суток.

3.1.4. Запрет использования трех ранее использовавшихся паролей.

3.1.5. Пароль пользователя не должен включать в себя легко вычисляемые сочетания символов, общепринятые сокращения, имена, фамилии, должности, год рождения, номер паспорта, табельный номер, иную информацию о Пользователе, доступную другим лицам. 3.1.6. Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

3.1.7. Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567, qwerty и т.п.).

3.2. Правила использования паролей:

3.2.1. Хранить в тайне свой пароль, не сообщать его другим лицам.

3.2.2. Не давать доступ в информационные системы другим лицам под своей учетной записью и паролем.

3.2.3. Изменять свой пароль при первом требовании политики паролей операционной системы (информационной системы).

3.2.4. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.2.5. Немедленно сообщить ответственному по парольной защите об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

3.2.6. Запрещается записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.

3.2.7. Запрещается хранить пароли в записанном виде на отдельных листах бумаги.

3.2.8. Смена, удаление личного пароля любого Пользователя производится в следующих случаях: – в случае подозрения на компрометацию пароля; – по окончании срока действия; – в случае прекращения полномочий (увольнение, переход на другую работу внутри Общества)

Пользователя после окончания последнего сеанса работы в информационных системах; – по указанию Администратора ИСПДн.

3.2.9. При увольнении, переходе на новую должность работника, имеющего доступ помимо своей учетной записи к другим ресурсам (межсетевые экраны, маршрутизаторы, серверы, другие учетные записи и т.п.) также производится внеплановая смена паролей к таким ресурсам.

3.2.10. Для создания значений паролей могут применяться специальные программные средства (генераторы паролей).

4. АНТИВИРУСНАЯ ЗАЩИТА

4.1. В случае отсутствия штатных функций антивирусной программы, предусматривающих автоматическую проверку файлов, Пользователь обязан осуществлять проверку файлов, получаемых:

– по электронной почте;

– через сеть Интернет;

– на магнитном, оптическом диске, флэш–накопителе;

– ином съемном носителе информации;

– полученные иным способом.

4.2. Пользователю запрещается:

4.2.1. Осуществлять действия, направленные на выключение антивирусной программы;

4.2.2. Самостоятельно устанавливать на АРМ программное обеспечение;

4.2.3. Запускать файлы, полученные по сетям связи (электронной почте, Интернет), со съемных носителей, даже если они получены проверенного адресата, без предварительной их проверки антивирусной программой.

4.3. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) Пользователь самостоятельно или вместе с ответственным за антивирусную защиту должен провести внеочередной антивирусный контроль своего рабочего места.

4.4. В случае обнаружения при проведении антивирусной проверки вирусного заражения Пользователи обязаны: – приостановить работу; – немедленно поставить в известность о факте обнаружения вирусного заражения ответственного за антивирусную защиту; – совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования; – провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь ответственного за антивирусную защиту)

5. ПОРЯДОК РАБОТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И СЕТИ ИНТЕРНЕТ

5.1. Подключение к информационным системам и сервисам сети Интернет:

5.1.1. Целью работы Пользователя в информационных системах и сети Интернет является сбор, обработка, хранение общедоступной и служебной информации, обмен электронными сообщениями в служебных целях.

5.1.2. Доступ к ресурсам информационных систем и сервисам сети Интернет предоставляется Пользователям только в том случае, если это не противоречит требованиям по защите информации (требованиям настоящей Инструкции и иных нормативных документов в области защиты информации).

5.1.3. Возможность получить доступ к ресурсам информационных систем и сервисам сети Интернет не является гарантией того, что запрошенный ресурс или сервис является разрешенным политиками Общества.

5.1.4. Основанием для подключения работника Общества к ресурсам информационных систем и сервисам сети Интернет является мотивированная заявка Администратору от непосредственного руководителя Пользователя с указанием полномочий доступа к таким ресурсам и сервисам.

5.1.5. Администратор, либо работник, выполняющий его функции, организует подключение к сервисам сети Интернет Пользователей в установленном порядке, осуществляет контроль над использованием ресурсов сети Интернет.

5.1.6. После выполнения задания Администратор сообщает Пользователю о выполнении заявки.

5.1.7. Основанием для отключения АРМ Пользователя от информационных систем и сервисов сети Интернет являются следующие события:

– нарушение инструкций и иных локальных нормативных актов в области защиты информации Общества;

– в случае нарушения Пользователем действующего законодательства в сфере компьютерной информации;

– увольнение Пользователя, либо перевод его в другое подразделение.

5.2. Порядок работы в сети Интернет:

5.2.1. Использование сотрудниками Общества сети Интернет должно осуществляться исключительно для выполнения должностных обязанностей.

5.2.2. Информация, образованная (образующаяся) в процессе трудовой деятельности работника, является собственностью Общества и не подлежит использованию, в том числе использованию в сети Интернет или с помощью сети Интернет в личных целях и (или) в корыстных интересах других лиц (организаций).

5.2.3. При проведении технических работ, связанных с настройкой оборудования (коммуникационное оборудование, прокси-сервера, маршрутизаторы и т.п.); в случае обнаружения попыток несанкционированного доступа к Интернет-шлюзу, АРМ Пользователей может проводиться временное отключение Пользователей от сервисов сети Интернет (в случае планового отключения Пользователи уведомляются об этом заблаговременно).

5.2.4. Вся информация о ресурсах, посещаемых работниками Общества, протоколируется и, при необходимости, может быть предоставлена руководителям подразделений, а также руководству Общества для детального изучения и принятия решения о мерах дисциплинарной ответственности.

5.2.5. При работе в сети Интернет Пользователям запрещается: – умышленное распространение и получение материалов в/из сети Интернет, противоречащих законодательству Российской Федерации, в том числе материалов, пропагандирующих насилие или экстремизм; разжигающих расовую, национальную или религиозную вражду; разъясняющих порядок изготовления и/или применения наркотиков, взрывчатых веществ, оружия и т. п.; материалов порнографического характера; компьютерных вирусов и других вредоносных программ; – передавать в сеть Интернет информацию, к которой в соответствии с законодательством ограничен доступ (персональные данные, коммерческая тайна) без соответствующего разрешения; – фальсифицировать IP-адрес, MAC-адрес, иные адреса, используемые в сетевых протоколах, а также прочую служебную информацию при передаче данных через сеть Интернет. – предоставлять доступ в сеть Интернет со своей рабочей станции кому-либо, в том числе программно-техническими способами через локальную вычислительную сеть Управления (например, путем несанкционированной установки локального Интернет-шлюза на рабочую станцию);

– получать доступ к сети Интернет любыми способами, не предусмотренными действующими локальными нормативными актами Общества (инструкциями, положениями, регламентами);

– осуществлять несанкционированный доступ к ресурсам и сервисам сети Интернет.

– выполнять действия (взлом, DoS (отказ в обслуживании), ARPspoofing атаки, сканирование локальной вычислительной сети) направленные на нарушение функционирования элементов сети Интернет (коммуникационного оборудования, серверов, рабочих станций, программного обеспечения).

5.3. Правила работы Пользователей с электронной почтой:

5.3.1. Пользователи обязаны использовать электронную почту только для выполнения служебных обязанностей. 5.3.2. Запрещается отправлять файлы, содержащие персональные данные в открытом виде (незашифрованные). 5.3.3. Запрещается массовая рассылка почтовых сообщений (более 10) внешним адресатам без согласования с руководством (спама). 5.3.4. Запрещается использовать не свой обратный адрес при отправке электронной почты.

5.3.5. Запрещается отправлять по электронной почте исполняемые файлы (обычно имеют расширения exe, com, bat). В случае необходимости отправки таких файлов, помещать их в архив.

5.3.6. Присоединяемые файлы рекомендуется упаковывать в архив при помощи программ-архиваторов.

5.3.7. Корпоративные рекомендации использования электронной почты:

– Вы должны оказывать то же уважение, что и при устном общении;

– Вы должны проверять правописание, грамматику и дважды перечитывать свое сообщение перед отправлением;

– Вы не должны участвовать в рассылке посланий, пересылаемых по цепочке (чаще всего это письма религиозно-мистического, развлекательного содержания, спам);

– Вы не должны по собственной инициативе пересылать по произвольным адресам незатребованную информацию;

– Вы не должны рассылать сообщения, которые являются зловредными, раздражающими или содержащими угрозы другим пользователям;

– Вы не должны отправлять никаких сообщений противозаконного или неэтичного содержания;

– Вы должны помнить, что электронное послание является эквивалентом почтовой открытки и не должно использоваться для пересылки конфиденциальной информации без использования средств защиты (шифрование);

– Вы не должны использовать широковещательные возможности электронной почты за исключением выпуска уместных объявлений; – Вы должны свести к минимуму количество электронных посланий личного характера;

– Вы должны неукоснительно соблюдать правила и инструкции и помогать администраторам бороться с нарушителями правил.

6. ПОРЯДОК РАБОТЫ С НОСИТЕЛЯМИ ИНФОРМАЦИИ

6.1. Под использованием носителей информации в информационных системах Общества понимается их подключение к инфраструктуре информационных систем с целью обработки, приема/передачи информации между информационными системами и носителями информации.

6.2. Допускается использование только учтенных носителей информации, которые являются собственностью Общества и подвергаются регулярной ревизии и контролю.

6.3. Учет и выдачу съемных носителей информации осуществляет администратор. Факт выдачи носителя фиксируется в журнале учета съемных носителей информации, форма которого утверждается приказом ректора.

6.4. Возможность подключения носителей информации, а также получение учтенных носителей информации предоставляются Пользователям по инициативе руководителей структурных подразделений в случаях:

– необходимости выполнения вновь принятым работником своих должностных обязанностей;

– возникновения у Пользователя производственной необходимости.

6.5. При использовании носителей информации необходимо:

– использовать носители информации исключительно для выполнения своих служебных обязанностей;

– бережно относится к носителям конфиденциальной информации;

– обеспечивать физическую безопасность носителей информации всеми разумными способами;

– извещать администраторов о фактах утраты (кражи) носителей информации.

6.6. При использовании носителей конфиденциальной информации запрещено:

– использовать носители конфиденциальной информации в личных целях;

– передавать носители конфиденциальной информации другим лицам (за исключением администраторов);

– хранить съемные носители с конфиденциальной информацией (персональными данными) на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

– выносить съемные носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому и т. д.

6.7. Любое взаимодействие (обработка, прием/передача информации), инициированное Пользователем между информационной системой и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с администраторами заранее). Администратор оставляет за собой право блокировать или ограничивать использование носителей информации.

6.8. Информация об использовании Пользователями носителей информации в информационных системах протоколируется и, при необходимости, может быть предоставлена руководителям структурных подразделений, а также руководителям Общества.

6.9. В случае выявления фактов несанкционированного и/или нецелевого использовании носителей информации инициируется служебная проверка, проводимая комиссией, состав которой определяется ответственным за организацию обработки персональных данных и утверждается приказом Общества. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Общества и действующему законодательству Российской Федерации.

6.10. При отправке или передаче конфиденциальной информации (персональных данных) адресатам на съемные носители записываются только предназначенные адресатам данные.

6.11. Вынос съемных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

6.12. Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется комиссией, состав которой определяется ответственным за организацию обработки персональных данных. По результатам уничтожения носителей составляется акт.

6.13. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители конфиденциальной информации изымаются и делаются соответствующие пометки в журнале учета носителей.

7. ПРАВА ПОЛЬЗОВАТЕЛЯ

7.1. Использовать информационные системы Общества для выполнения служебных обязанностей.

7.2. Обращаться к системному администратору, Администратору ИСПДн, ответственному за организацию обработки персональных данных для консультаций по поводу использования программного обеспечения и АРМ, вопросам обработки персональных данных. 7.3. Направлять предложения по установке новых версий существующего программного обеспечения (с обоснованием необходимости замены старых версий на новые).

7.4. Направлять предложения по модернизации программного обеспечения, разрабатываемого в Обществе или по заказу Общества.

7.5. Направлять предложения по установке нового (а также дополнительного) программного обеспечения (с указанием цели использования, преимуществ перед существующими аналогами).

7.6. Направлять предложения по модернизации АРМ (замены на новые аналоги), входящих в ИСПДн (с обязательным обоснованием замены и указанием преимуществ перед существующими аналогами).

7.7. Требовать от руководства прекращения работ в рамках информационной системы при обнаружении обстоятельств, создающих предпосылки утечки информации ограниченного доступа, обрабатываемой в рамках данной информационной системы.

7.8. Получать консультации и разъяснения по работе с компьютерным оборудованием и программным обеспечением, по вопросам компьютерной безопасности.

8. ОТВЕТСТВЕННОСТЬ

8.1. Пользователь несет персональную ответственность за свои действия или бездействие, которые повлекут за собой разглашение персональных данных, а также за нарушение нормального функционирования информационных систем или ее отдельных компонентов, несанкционированный доступ к информации в соответствие с законодательством Российской Федерации и локальными нормативными актами Общества.

Приложение № 38.
Инструкция резервного копирования
в информационных системах персональных данных

ИНСТРУКЦИЯ
по организации резервного копирования в информационных системах персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция устанавливает основные требования к организации резервного копирования (восстановления) программ и данных, хранящихся в базах данных на серверах, а также к резервированию аппаратных средств.

1.2. Настоящая Инструкция разработана с целью:

- определения категории информации, подлежащей обязательному резервному копированию;

определения процедуры резервирования данных для последующего восстановления работоспособности информационных систем при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

- определения порядка восстановления информации в случае возникновения такой необходимости;
- упорядочения работы и определения ответственности должностных лиц, связанной с резервным копированием и восстановлением информации.

1.3. Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности информационных систем персональных данных (ИСПДн) в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

1.4. Резервному копированию подлежит информация следующих основных категорий:

- персональная информация пользователей (личные каталоги) и групповая информация (общие каталоги подразделений) на файловых серверах;
- информация, обрабатываемая пользователями в ИСПДн, а также информация, необходимая для восстановления работоспособности ИСПДн, в т.ч. систем управления базами данных (СУБД) общего пользования и справочно- информационные системы общего использования;
- рабочие копии установочных компонент программного обеспечения общего назначения и специализированного программного обеспечения ИСПДн, СУБД, серверов и рабочих станций;
- информация, необходимая для восстановления серверов и систем управления базами данных ИСПДн, локальной вычислительной сети, системы электронного документооборота;
- регистрационная информация системы информационной безопасности ИСПДн;
- другая информация ИСПДн, по мнению пользователей и администратора безопасности, являющаяся критичной для работоспособности ИСПДн.

1.5. Для каждой ИСПДн разрабатывается отдельный Регламент резервного копирования в зависимости от следующих требований:

- состав и объем копируемых данных, необходимая периодичность проведения резервного копирования (по форме, приведенной в Приложении N 1);
- максимальный срок хранения резервных копий;
- требований к надежности и защищенности хранения резервных копий;
- требований к резервируемым аппаратным средствам ИСПДн (при необходимости, в случае предъявления высоких требований к обеспечению доступности данных, обрабатываемых в ИСПДн, и значительного ущерба при нарушении заданных характеристик безопасности ПДн).

Допускается составление одного Регламента для нескольких ИСПДн в случае идентичности требований к их резервированию.

1.6. Машинным носителям информации, содержащим резервную копию, присваивается гриф конфиденциальности по наивысшему грифу содержащихся на них сведений.

1.7. Резервные копии хранятся вне пределов серверного помещения, доступ к резервным копиям ограничен. К носителям информации, содержащим резервные копии, а также к резервируемым программным и аппаратным средствам допускаются только работники, указанные в Списке лиц, имеющих доступ к резервируемым программным и аппаратным средствам ИСПДн (форма Списка лиц приведена в Приложении N 2). Список лиц формируется на основании письменной Заявки руководителя подразделения информационных технологий (ИТ), согласованной с руководителем подразделения информационной безопасности (ИБ). Изменение прав доступа к резервируемым техническим средствам, массивам и носителям информации производится на основании Заявки руководителя подразделения ИТ, согласованной с руководителем подразделения ИБ. О выявленных попытках несанкционированного доступа к резервируемой информации и аппаратным средствам, а также иных нарушениях ИБ, произошедших в процессе резервного копирования, сообщается в подразделение ИБ служебной запиской в течение рабочего дня после обнаружения указанного события.

2. ОБЩИЕ ТРЕБОВАНИЯ К РЕЗЕРВНОМУ КОПИРОВАНИЮ

2.1. В Регламенте резервного копирования описываются действия при выполнении следующих мероприятий:

- резервное копирование с указанием конкретных резервируемых данных и аппаратных средств (в случае необходимости);
- контроль резервного копирования:
- хранение резервных копий;
- полное или частичное восстановление данных.

2.2. Архивное копирование резервируемой информации производится при помощи специализированных программно-аппаратных систем резервного копирования, программный и аппаратный состав которых обеспечивает выполнение требования к резервному копированию, приведенные в п. 1.5. Система резервного копирования обеспечивает производительность, достаточную для сохранения информации, указанной в п. 1.4, в установленные сроки и с заданной периодичностью.

2.3. Требования к техническому обеспечению систем резервного копирования:

- это комплекс взаимосвязанных технических средств, обеспечивающих процессы сбора, передачи, обработки и хранения информации, основывающийся на единой технологической платформе;
- имеет возможность расширения (замены) состава технических средств, входящих в комплекс, для улучшения их эксплуатационно-технических характеристик по мере возрастания объемов обрабатываемой информации:
- обеспечивает выполнение функций, перечисленных в п. 2.1;
- средства вычислительной техники отвечают действующим на момент сертификации российским и международным стандартам и рекомендациям.

2.4. Требования к программному обеспечению систем резервного копирования:

- лицензионное системное программное обеспечение и программное обеспечение резервного копирования;
- программное обеспечение резервного копирования обеспечивает простоту процесса инсталляции, конфигурирования и сопровождения.

2.5. Сопровождение системы резервного копирования возлагается на уполномоченных работников подразделения ИТ, которые обязаны следить за работоспособностью программных и аппаратных средств, осуществляющих архивное копирование, в соответствии с их инструкциями по эксплуатации.

2.6. Предварительный учет магнитных носителей архивных копий производится в отдельном журнале учета магнитных носителей для архивного копирования, который находится

в подразделении ИТ (форма журнала приведена в Приложении N 3). Все магнитные носители с архивными копиями маркируются, на них указывается предназначение носителя.

В случае неотделимости носителей архивной информации от системы резервного копирования допускается их не маркировать и учитывать всю систему как одно целое.

2.7. Хранение отдельных магнитных носителей архивных копий организуется в отдельном от используемых данных помещении. Физический доступ к архивным копиям строго ограничен. Контроль за физическим доступом возлагается на администратора безопасности.

2.8. Доступ к носителям архивных копий имеют только уполномоченные работники подразделений ИТ и ИБ, которые несут персональную ответственность за сохранность архивных копий и невозможность ознакомления с ними лиц, не имеющих на то права.

2.9. Магнитные носители для архивных копий изымаются для работы только работником, непосредственно осуществляющим резервное копирование, под роспись в журнале учета магнитных носителей архивных копий. Передача магнитных носителей с архивными копиями кому бы то ни было без документального оформления не допускается.

2.10. Уничтожение отделяемых магнитных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательной записью в журнале их учета.

3. ОТВЕТСТВЕННОСТЬ ЗА СОСТОЯНИЕ РЕЗЕРВНОГО КОПИРОВАНИЯ

3.1. Ответственность за периодичность и полноту резервного копирования, а также состояние системы резервного копирования возлагается на уполномоченных работников подразделения ИТ, осуществляющих резервное копирование.

3.2. Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением соответствующего Регламента, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на администратора безопасности.

3.3. В случае обнаружения попыток несанкционированного доступа к носителям архивной информации, а также иных нарушениях ИБ, произошедших в процессе резервного копирования, сообщается в подразделение ИБ служебной запиской в течение рабочего дня после обнаружения указанного события.

4. ПЕРИОДИЧНОСТЬ РЕЗЕРВНОГО КОПИРОВАНИЯ

4.1. Резервное копирование специализированного программного обеспечения производится при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.

4.2. Резервное копирование открытой информации делается не позднее чем через сутки после ее изменения, но не реже одного раза в месяц.

4.3. Информация (ПДн), содержащаяся в постоянно изменяемых базах данных, сохраняется в соответствии со следующим графиком:

- ежедневно проводится копирование измененной и дополненной информации. Носители с ежедневной информацией должны храниться в течение недели;
- еженедельно проводится резервное копирование всей базы данных. Носители с еженедельными копиями хранятся влечение месяца;
- ежемесячно производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится постоянно.

4.4. Не реже одного раза в год на носители длительного хранения записывается информация, не относящаяся к постоянно изменяемым базам данных (приказы, распоряжения, открытые издания и т.д.).

5. КОНТРОЛЬ РЕЗУЛЬТАТОВ РЕЗЕРВНОГО КОПИРОВАНИЯ

5.1. Контроль результатов всех процедур резервного копирования осуществляется ответственными должностными лицами, в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур. В случае обнаружения

ошибки лицо, ответственное за контроль результатов, сообщает руководителю подразделения ИТ до 18 часов текущего рабочего дня.

5.2. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, осуществляется ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для ее хранения.

6. РОТАЦИЯ НОСИТЕЛЕЙ РЕЗЕРВНОЙ КОПИИ

6.1. Система резервного копирования обеспечивает возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивает восстановление текущей информации ИСПДн в случае отказа любого из устройств резервного копирования.

6.2. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются ответственным работником подразделения ИТ. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек. Информация ограниченного доступа с носителей, которые перестают использоваться в системе резервного копирования, уничтожается.

7. ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ ИЗ РЕЗЕРВНЫХ КОПИЙ

7.1. В случае необходимости восстановление данных из резервных копий производится ответственным работником подразделения ИТ.

7.2. Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

7.3. Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

7.4. Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

7.5. Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.

7.6. При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

Приложение № 39.
Инструкция по организации антивирусной защиты в информационной системы персональных данных

Инструкция по организации антивирусной защиты в ИСПДн

1. Общие положения

Целью создания системы антивирусной защиты является обеспечение защищенности информационно-коммуникационной системы (далее ИКС) от воздействия различного рода вредоносных программ и несанкционированных массовых почтовых рассылок, предотвращения их внедрения в информационные системы, выявления и безопасного удаления из систем в случае попадания, а также фильтрации доступа пользователей Учреждения к непродуктивным Интернет- ресурсам и контроля их электронной переписки.

Основополагающими требованиями к системе антивирусной защиты УСЗН являются:

- решение задачи антивирусной защиты должно осуществляться в общем виде. Средство защиты не должно оказывать противодействие конкретному вирусу или группе вирусов, противодействие должно оказываться в предположениях, что вирус может быть занесен на компьютер и о вирусе (о его структуре (в частности, сигнатуре) и возможных действиях) ничего не известно;
- решение задачи антивирусной защиты должно осуществляться в реальном времени.
- Мероприятия, направленные на решение задач по антивирусной защите: установка только лицензированного программного обеспечения либо бесплатное антивирусное программное обеспечение, идущее в комплекте с подлинной операционной системой (типа Microsoft Security Essentials (сеть до 10 рабочих станций) или Microsoft Forefront Endpoint Protection (сеть более 10 рабочих станций)), поддерживающее работу с пользовательскими профилями.
- регулярное обновление и ежедневные профилактические проверки (желательно в нерабочее ночное время);
- непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах ИКС;
- ежедневный анализ, ранжирование и предотвращение угроз распространения и воздействия вредоносных программ путем выявления уязвимостей используемого в ИКС операционного программного обеспечения и сетевых устройств и устранения обнаруженных дефектов в соответствии с данными поставщика программного обеспечения и других специализированных экспертных антивирусных служб.
- проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур.
- проведение регулярных проверок целостности критически важных программ и данных. Наличие лишних файлов и следов несанкционированного внесения изменений должно быть зарегистрировано в журнале и расследовано;
- внешние носители информации неизвестного происхождения следует проверять

на наличие вирусов до их использования;

- необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения;
- следует иметь планы обеспечения бесперебойной работы УСЗН для случаев вирусного заражения, в том числе планы резервного копирования всех необходимых данных и программ и их восстановления. Эти меры особенно важны для сетевых файловых серверов, поддерживающих большое количество рабочих

станций.

1. Технологические инструкции

1.1. В УСЗН руководителем должно быть назначено лицо, ответственное за антивирусную защиту, в должностные инструкции для которого должны быть прописаны порядок действия в период вирусных эпидемий, порядок действий при возникновении внештатных ситуаций, связанных с работоспособностью средств антивирусной защиты, порядок действий для устранения последствий заражений . В противном случае вся ответственность за обеспечение антивирусной защиты ложится на руководителя УСЗН.

1.2. В УСЗН может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.

1.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, почтовые сообщения), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация, находящаяся на съемных носителях (магнитных дисках, лентах, CD-ROM, DVD,flash-накопителях и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

1.4. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

2. Требования к проведению мероприятий по антивирусной защите

2.1. В начале работы при загрузке компьютера в автоматическом режиме должно выполняться обновление антивирусных баз и серверов.

2.2. Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю, данные, расположенные на рабочих станциях пользователей - ежедневно, в ночное время по расписанию.

2.3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

2.3.1. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка на серверах и персональных компьютерах УСЗН.

2.3.2. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

2.3.3. При отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

2.4. В случае обнаружения зараженных вирусами файлов или электронных писем пользователи обязаны:

2.4.1. Приостановить работу.

2.4.2. Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты (в случае его отсутствия - руководителя УСЗН).

2.4.3. Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.

2.4.4. Провести лечение или уничтожение зараженных файлов.

3. Ответственность

3.1. Ответственность за организацию антивирусной защиты возлагается на руководителя УСЗН или лицо, им назначенное.

3.2. Ответственность за проведение мероприятий антивирусного контроля в УСЗН возлагается на ответственного за обеспечение антивирусной защиты.

3.3. Соблюдение требований настоящей Инструкции при работе на персональных рабочих местах возлагается на специалистов – пользователей.

3.4. Периодический контроль за состоянием антивирусной защиты в Учреждении осуществляется руководителем и фиксируется Актом проверки (не реже 1 раз в квартал).

Приложение № 40.
Инструкция пользователя информационной системы персональных данных при возникновении нештатной ситуации

Инструкция пользователя информационной системы персональных данных при возникновении нештатных ситуаций

1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием информационных систем персональных данных (далее – ИСПДн) ООО «_____» (далее - Общество) меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания работоспособности в случае реализации рассматриваемых угроз.

3. Задачами данной Инструкции являются: — определение мер защиты от прерывания работоспособности; — определение действий по восстановлению в случае прерывания работоспособности.

4. Действие настоящей Инструкции распространяется на всех пользователей ИСПДн, имеющих доступ к ресурсам ИСПДн, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

— системы жизнеобеспечения;

— системы обеспечения отказоустойчивости;

— системы резервного копирования и хранения данных; — системы контроля физического доступа.

5. Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении № 1.

6. При реагировании на инцидент важно, чтобы пользователь правильно классифицировал критичность инцидента.

Критичность оценивается на основе следующей классификации:

— Уровень 1. Незначительный инцидент – локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты;

— Уровень 2. Авария – любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты;

— Уровень 3. Катастрофа – любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, к уничтожению, блокированию, неправомерной модификации или компрометации защищаемых персональных данных, а также к угрозе жизни пользователей ИСПДн.

7. При возникновении нештатной ситуации любого уровня пользователь обязан оповестить ответственного за организацию обработки персональных данных, сообщив характер аварийной ситуации, масштаб ситуации по предварительной субъективной оценке.

8. Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за организацию обработки персональных данных в Журнале регистрации фактов нарушения и восстановления работоспособности оборудования или ИСПДн. В кратчайшие сроки, не превышающие одного рабочего дня, должны быть предприняты меры по восстановлению работоспособности ИСПДн.

9. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные (программно-аппаратные) и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как: — системы жизнеобеспечения;

— системы обеспечения отказоустойчивости;

— системы резервного копирования и хранения данных;

— системы контроля физического доступа. Системы жизнеобеспечения ИСПДн включают:
— пожарные сигнализации и системы пожаротушения;
— системы вентиляции и кондиционирования;
— системы резервного питания.

Все критичные помещения, в которых размещаются элементы ИСПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации восстановления ИСПДн описан в Инструкции по организации резервирования и восстановления программного обеспечения, баз персональных данных ИСПДн.

10. Ответственный за организацию обработки персональных данных:

— ознакомляет всех сотрудников, находящихся в его зоне ответственности, с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу;

— обучает пользователей, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Пользователи ИСПДн должны получить базовые знания в следующих областях:

— оказание первой медицинской помощи;
— пожаротушение; — эвакуация людей;
— защита материальных и информационных ресурсов;
— методы оперативной связи со службами спасения и руководителями структурных подразделений; — выключение оборудования, электричества, водоснабжения, газоснабжения;

— по окончанию ознакомления сотрудников получает их роспись в Журнале учета прохождения первичного инструктажа.

11. Навыки и знания пользователей ИСПДн по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение пользователей ИСПДн порядку действий при возникновении аварийной ситуации.

Ответственность за организацию обучения пользователей ИСПДн несет ответственный за организацию обработки персональных данных генеральный директор Общества, который согласует сроки и порядок их обучения.

Приложение 1
к Инструкции пользователя ИСПДн
при возникновении нештатной ситуации

Источники угроз безопасности персональных данных

Технологические угрозы: пожар в здании; повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения); взрыв (бытового газа, взрывчатых веществ или приборов, работающих под давлением); химический выброс в атмосферу.

Внешние угрозы: массовые беспорядки; сбои общественного транспорта; эпидемия; массовое отравление персонала; теракт.

Стихийные бедствия: удар молнии; сильный снегопад; сильные морозы; просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания; затопление водой в период паводка; наводнение, вызванное проливным дождем; торнадо; подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод).

ИТ-угрозы: сбой системы кондиционирования в серверном помещении; выход из строя файлового сервера ; частичная потеря информации на сервере без потери его работоспособности; выход из строя локальной сети; выход из строя рабочей станции; частичная потеря информации на рабочей станции без потери её работоспособности.

Угроза, связанная с человеческим фактором: ошибка персонала, имеющего доступ к элементам ИСПДн; нарушение конфиденциальности, целостности и доступности конфиденциальной информации, а также несанкционированные действия, заблокированные средствами защиты и зафиксированные средствами регистрации.

Угрозы, связанные с внешними поставщиками: отключение электроэнергии; сбой в работе интернет-провайдера; физический разрыв внешних каналов связи.

Приложение № 41.
Журнал регистрации нарушения и восстановления работоспособности

№ п/п	Наименование ИСПДн описание нарушения работоспособности оборудования или ИСПДн	Дата и время обнаружения начала нарушения работоспособности	Выявленная причина нарушения работоспособности	Дата и время восстановления работоспособности	Сотрудник, проводивший восстановление работоспособности оборудования или ИСПДн	
					Фамилия	Подпись
1	**2**	**3**	**4**	**5**	**6**	**7**

Приложение № 42.
Журнал учета средств защиты информации

№ п/п	Наименование СЗИ	Дата ввода в эксплуатацию	№ лицензии на СЗИ	срок действия	Название и местонахождение организации ФИО сотрудника, установившей СЗИ	
					Фамилия подпись	Примечание
1	**2**	**3**	**4**	**5**	**6**	**7**

Приложение № 43.
Журнал учета проверок
контролирующими органами

Журнал
учета проверок юридического лица, индивидуального предпринимателя, проводимых органами государственного контроля (надзора), органами муниципального контроля

(дата начала ведения Журнала)

(наименование юридического лица/фамилия, имя, отчество (в случае, если имеется)

(адрес (место нахождения) постоянно действующего исполнительного органа юридического лица/место жительства (место осуществления деятельности (если не совпадает с местом жительства)

(государственный регистрационный номер записи о государственной регистрации юридического лица/индивидуального предпринимателя, идентификационный номер налогоплательщика (для индивидуального предпринимателя); номер реестровой записи и дата включения сведений в реестр субъектов малого или среднего предпринимательства (для субъектов малого и среднего предпринимательства))

Ответственное лицо:

(фамилия, имя, отчество (в случае, если имеется), должность лица (лиц), ответственного за ведение журнала учета проверок)

(фамилия, имя, отчество (в случае, если имеется) руководителя юридического лица, индивидуального предпринимателя)

Подпись:

М.П.

Сведения о проводимых проверках

1	Дата начала и окончания проверки	
2	Общее время проведения проверки (в отношении субъектов малого предпринимательства и микропредприятий указывается в часах)	
3	Наименование органа государственного контроля (надзора), наименование органа муниципального контроля	
4	Дата и номер распоряжения или приказа о проведении проверки	
5	Цель, задачи и предмет проверки	
6	Вид проверки (плановая или внеплановая): в отношении плановой проверки: – со ссылкой на ежегодный план проведения проверок; в отношении внеплановой выездной проверки: – с указанием на дату и номер решения прокурора	

	о согласовании проведения проверки (в случае, если такое согласование необходимо)	
7	Дата и номер акта, составленного по результатам проверки, дата его вручения представителю юридического лица, индивидуальному предпринимателю	
8	Выявленные нарушения обязательных требований (указываются содержание выявленного нарушения со ссылкой на положение нормативного правового акта, которым установлено нарушенное требование, допустившее его лицо)	
9	Дата, номер и содержание выданного предписания об устранении выявленных нарушений	
10	Фамилия, имя, отчество (в случае, если имеется), должность должностного лица (должностных лиц), проводящего(их) проверку	
11	Фамилия, имя, отчество (в случае, если имеется), должности экспертов, представителей экспертных организаций, привлеченных к проведению проверки	
12	Подпись должностного лица (лиц), проводившего проверку	

Приложение № 44.
Форма запроса о наличии
и ознакомлении
с персональными данными

Генеральному директору ООО «_____»
От:_____

ФИО Субъекта
_____
Вид документа
_____
Номер документа
_____
Дата выдачи и кем выдан документ

ЗАПРОС

В соответствии со ст. 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» я имею право получить от вашей организации информацию, касающуюся обработки моих персональных данных.

Прошу вас предоставить мне следующие сведения:
1. Подтверждение факта обработки моих персональных данных;
2. Правовые основания и цели обработки персональных данных;
3. Применяемые способы обработки персональных данных;
4. Какие лица имеют доступ или могут получить доступ к персональным данным;
5. Перечень обрабатываемых персональных данных и источник их получения;
6. Срок хранения персональных данных;
7. Осуществлялась ли трансграничная передача персональных данных, а, если нет, то предполагается ли такая передача.

Ответ на настоящий запрос прощу направить в письменной форме по адресу:_____
в установленные законом сроки.

«_____» _____ 202___ г. _____ _____

Приложение № 45.
Правила рассмотрения
запросов субъектов
персональных данных

ПРАВИЛА
рассмотрения [наименование организации, учреждения] запросов субъектов персональных данных
или их представителей

1. Общие положения
1.1. Настоящие правила рассмотрения запросов субъектов персональных данных или их представителей (далее – Правила) определяют порядок рассмотрения запросов субъектов персональных данных или их представителей [наименование организации, учреждения].
1.2. Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области защиты персональных данных.
1.3. Правила обязательны для исполнения всеми работниками [наименование организации, учреждения], организующими или непосредственно участвующими в процессе обработки запросов субъектов персональных данных и их представителей.

2. Запросы на предоставление информации о порядке обработки персональных данных
2.1. В случае поступления от субъекта персональных данных (представителя субъекта персональных данных) запроса о предоставлении сведений, касающихся обработки персональных данных, [наименование организации, учреждения] подготавливает согласно запросу необходимый ответ.
2.2. Перечень сведений, которые может запрашивать субъект персональных данных (представитель субъекта персональных данных), представляет следующие сведения:
- подтверждение факта обработки персональных данных оператором.
- правовые основания и цели обработки персональных данных.
- цели и применяемые оператором способы обработки персональных данных.
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона.
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом.
- сроки обработки персональных данных, в том числе сроки их хранения. - порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее - Закон о персональных данных).
- информацию об осуществленной или о предполагаемой трансграничной передаче данных.
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу.
- бланк запроса субъекта персональных данных (представителя субъекта персональных данных) на получение информации, касающейся обработки его персональных данных приведен в приложении к настоящим Правилам (Приложение 1).
- бланк предоставления сведений по запросу субъекта персональных данных (представителя субъекта персональных данных) приведен в приложении к настоящим Правилам

2.3. В случае требования предоставления иных, не предусмотренных правовыми актами сведений, [наименование организации, учреждения] подготавливает письменный отказ в предоставлении сведений со ссылкой на действующее законодательство Российской Федерации.
2.4. Бланк отказа в предоставлении сведений по запросу субъекта персональных данных (представителя субъекта персональных данных) приведен в приложении к настоящим Правилам
2.5. В случае если сведения, указанные в п. 2.1 настоящего документа, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных (представителю субъекта персональных данных) по его запросу, субъект персональных данных (представитель субъекта персональных данных) вправе обратиться повторно в [наименование организации, учреждения] или направить ему повторный запрос в целях получения сведений, указанных в п. 2.1 настоящего документа, и ознакомления с такими персональными данными не ранее чем через 30 (тридцать) дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен Законом о персональных данных, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.
2.6. Субъект персональных данных (представитель субъекта персональных данных) вправе обратиться повторно в [наименование организации, учреждения] или направить ему повторный запрос в целях получения сведений, указанных в п. 2.1 настоящего документа, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п. 2.6 настоящего документа, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п. 2.1 Правил, должен содержать обоснование направления повторного запроса.
2.7. Выдача работникам [наименование организации, учреждения] документов, связанных с их трудовой деятельностью (копий приказов о приеме на работу, переводах на другую работу, увольнении с работы; выписок из трудовой книжки, справок о месте работы, заработной плате, периоде работы в организации и др.) регулируется трудовым законодательством Российской Федерации и внутренними организационно-распорядительными документами [наименование организации, учреждения]. Взаимодействие с работниками [наименование организации, учреждения] осуществляют соответствующие работники отдела кадров.
2.8. В случае отзыва субъектом персональных данных (представителем субъекта персональных данных) согласия на обработку его персональных данных, [наименование организации, учреждения] прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий 30 (тридцати) дней с даты поступления указанного отзыва, если иное не предусмотрено договором, иным соглашением между [наименование организации, учреждения] и субъектом персональных данных.

3. Запросы на уточнение, блокирование, уничтожение персональных данных
3.1. В случае поступления от субъекта персональных данных (представителя субъекта персональных данных) запроса об уточнении, блокировании или уничтожении персональных данных [Наименование организации, учреждения] проверяет подтверждающие документы, вносит необходимые исправления, и оповещает субъект персональных данных (представителя субъекта персональных данных), а также всех работников, связанных с обработкой персональных данных в [Наименование организации, учреждения] о внесенных изменениях. Копии документов, являющихся основанием для исключения или исправления неверных или неполных персональных данных, хранятся в личных делах субъектов.

3.2. Бланк запроса субъекта персональных данных (представителя субъекта персональных данных) на уточнение, блокирование или уничтожение своих персональных данных приведен в приложении к настоящим Правилам
3.3. Бланк уведомления субъекта персональных данных (представителя субъекта персональных данных) об уточнении, блокировании или уничтожении его персональных данных приведен в приложении к настоящим Правилам
3.4. В случае отсутствия основания для уточнения, блокирования или уничтожения [Наименование организации, учреждения] подготавливает письменный отказ об уточнении, блокировании или уничтожении персональных данных со ссылкой на действующее законодательство Российской Федерации.
3.5. Бланк уведомления субъекта персональных данных (представителя субъекта персональных данных) об отказе в уточнении, блокировании или уничтожении его персональных данных приведен в приложении к настоящим Правилам

4. Порядок рассмотрения запросов
4.1. Запрос субъекта персональных данных (представителя субъекта персональных данных) может быть направлен в [наименование организации, учреждения]: - в письменной форме;
- в форме электронного документа, подписанного электронной подписью в соответствии с законодательством Российской Федерации с использованием Интернет-ресурса «Электронная приемная» [наименование организации, учреждения].
4.2. Все поступившие запросы субъектов персональных данных (представителей субъекта персональных данных) по вопросам обработки персональных данных регистрируются в Журнале учета обращений субъектов персональных данных и представителей субъектов персональных данных [наименование организации, учреждения]
4.3. Ответственным лицом за ведение Журнала учета обращений субъектов персональных данных и представителей субъектов персональных данных [наименование организации, учреждения] является ответственный за организацию обработки персональных данных.
4.4. После регистрации запроса ответственный за организацию обработки персональных данных подготавливает мотивированный ответ на запрос и в случае необходимости направляет подготовленный ответ на рассмотрение всем задействованным лицам. Перечень лиц, привлекаемых для подготовки ответа, определяется ответственным за организацию обработки персональных данных в зависимости от предмета обращения.
4.5. Лица, задействованные в подготовке ответа, должны соблюдать порядок и сроки обработки запросов, установленные законодательством Российской Федерации в зависимости от их типов (настоящих Правил).
4.6. Ответственный за организацию обработки персональных данных контролирует соблюдение указанных сроков в соответствии с законодательством Российской Федерации.
4.7. После подготовки и отправки ответа на запрос, ответственный за организацию обработки персональных данных делает соответствующую отметку в Журнале учета обращений субъектов персональных данных и представителей субъектов персональных данных [наименование организации, учреждения] с указанием даты отправки.

5. Права и обязанности субъектов персональных данных
5.1. Субъект, персональные данные которого обрабатываются в [наименование организации, учреждения], имеет право:
- получать доступ к своим персональным данным и знакомиться с ними.
- требовать от [наименование организации, учреждения] уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

- требовать извещения всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- получать информацию, касающуюся обработки его персональных данных;
- обжаловать в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия [наименование организации, учреждения] при обработке и защите его персональных данных.

5.2. Субъект, персональные данные которого обрабатываются в [наименование организации, учреждения], обязан предоставлять [наименование организации, учреждения] достоверные сведения о себе и своевременно информировать об изменении своих персональных данных [наименование организации, учреждения] оставляет за собой право проверять достоверность предоставленных субъектом сведений.

6. Обязанности [наименование организации, учреждения] как оператора персональных данных

6.1. [Наименование организации, учреждения] обязано:
- предоставить субъекту персональных данных (представителю субъекта персональных данных) по его просьбе информацию, касающуюся обработки его персональных данных;
- разъяснить субъекту персональных данных (представителю субъекта персональных данных) юридические последствия отказа предоставить его персональные данные. Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные приведена в приложении к настоящим Правилам (0).

6.2. В случае если персональные данные получены не от субъекта персональных данных, [наименование организации, учреждения], до начала обработки таких персональных данных, обязан предоставить субъекту персональных данных следующую информацию о начале обработки его персональных данных:
- наименование либо фамилию, имя, отчество и адрес оператора или его представителя; - цель обработки персональных данных и ее правовое основание;
- предполагаемых пользователей персональных данных;
- права субъекта персональных данных, установленные Законом о защите персональных данных; - источник получения персональных данных.

6.3. [Наименование организации, учреждения] обязано сообщить субъекту персональных данных (представителю субъекта персональных данных) о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных (представителя субъекта персональных данных) в течение 30 (тридцати) дней.

6.4. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных субъекту персональных данных (представителю субъекта персональных данных) при обращении, либо при получении запроса субъекта персональных данных (представителя субъекта персональных данных), [Наименование организации, учреждения] обязано дать в письменной форме мотивированный ответ, содержащий ссылку, являющуюся основанием для такого отказа.

6.5. [Наименование организации, учреждения] обязано предоставить безвозмездно субъекту персональных данных (представителю субъекта персональных данных) возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. [Наименование организации, учреждения] обязан уведомить субъекта персональных данных (представителя субъекта персональных данных) о внесенных изменениях и предпринятых мерах.

Приложение 1
к Правилам рассмотрения [наименование организации, учреждения]
запросов субъектов персональных данных или их представителей

ЗАПРОС субъекта персональных данных (представителя субъекта персональных данных) на получение информации,
касающейся обработки его персональных данных (На бланке организации)
В соответствии с положениями статьи 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» прошу [Наименование организации, учреждения] (далее – оператор) предоставить информацию, касающуюся обработки персональных данных относящихся к следующему субъекту персональных данных: (фамилия, имя, отчество субъекта персональных данных) (фамилия, имя, отчество представителя субъекта персональных данных, реквизиты доверенности или иного документа, подтверждающего полномочия представителя) (номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе) (сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором) Перечень запрашиваемой информации (отметить требуемое):
 подтверждение факта обработки персональных данных оператором;
 правовые основания и цели обработки персональных данных;
 цели и применяемые оператором способы обработки персональных данных;
 наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
 обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
 сроки обработки персональных данных, в том числе сроки их хранения;
 порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»; информацию об осуществленной или о предполагаемой трансграничной передаче данных;
 наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
 иные сведения, предусмотренные Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» или другими федеральными законами: _____
_____ (приводятся, с указанием основания) / (подпись) (фамилия, имя, отчество)

Приложение 2
к Правилам рассмотрения [наименование организации, учреждения]
запросов субъектов персональных данных или их представителей

ПРЕДОСТАВЛЕНИЕ СВЕДЕНИЙ ПО ЗАПРОСУ субъекта персональных данных (представителя субъекта персональных данных) на получение информации, касающейся обработки его персональных данных (На бланке организации)

В ответ на Ваш запрос от «____» _____ 20___ года, на получение информации, касающейся обработки персональных данных следующего субъекта персональных данных: (фамилия, имя, отчество субъекта персональных данных) [наименование организации, учреждения] во исполнение положений статьи 14 и статьи 20 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» предоставляет следующую информацию:

_____
_____
_____ _____
_____ (должность) (подпись) (фамилия, имя, отчество)
«____» _____ 20___ года

Приложение 3
к Правилам рассмотрения [наименование организации, учреждения]
запросов субъектов персональных данных или их представителей

ОТКАЗ в предоставлении сведений по запросу субъекта персональных данных (представителя субъекта персональных данных) на получение информации, касающейся обработки его персональных данных (На бланке организации)

В ответ на Ваш запрос от «____» _____ 20___ года, на получение информации, касающейся обработки персональных данных, относящихся к следующему субъекту персональных данных: (фамилия, имя, отчество субъекта персональных данных) [наименование организации, учреждения] во исполнение положений статьи 14 и статьи 20 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» отказывает в предоставлении информации по следующей причине:

_____
_____
_____ _____ _____
(должность) (подпись) (фамилия, имя, отчество)

«____» _____ 20___ года

Приложение 4
к Правилам рассмотрения [наименование организации, учреждения]
запросов субъектов персональных данных или их представителей

ЗАПРОС субъекта персональных данных (представителя субъекта персональных данных) на уточнение, блокирование или уничтожение своих персональных данных (На бланке организации)

В соответствии с положениями статьи 21 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», прошу [наименование организации, учреждения] (далее – оператор) осуществить уточнение / блокирование / уничтожение (ненужное зачеркнуть) обрабатываемых персональных данных, относящихся к следующему субъекту персональных данных:
(фамилия, имя, отчество субъекта персональных данных) (фамилия, имя, отчество представителя субъекта персональных данных, реквизиты доверенности или иного документа, подтверждающего полномочия представителя) (номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе) (сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором) в связи с тем, что персональные данные являются неполными / устаревшими / неточными / незаконно полученными / не являются необходимыми для заявленной цели обработки. (ненужное зачеркнуть)

Основания для запроса:
_____
_____
_____
_____
(основания для запроса, сведения, подтверждающие, что персональные данные являются неполными, неточными или неактуальными, актуальные персональные данные)

_____ _____
_____ (должность) (подпись) (фамилия, имя, отчество)
«____» _____ 20___ года

Приложение 5
к Правилам рассмотрения [наименование организации, учреждения]
запросов субъектов персональных данных или их представителей

УВЕДОМЛЕНИЕ субъекта персональных данных (представителя субъекта персональных данных) об уточнении, блокировании или уничтожении его персональных данных (На бланке организации)

На основании Вашего обращения от «____» _____ 20___ года, об уточнении, блокировании или уничтожении персональных данных, относящихся к следующему субъекту персональных данных (фамилия, имя, отчество субъекта персональных данных) сообщаем, что [наименование организации, учреждения] в соответствии с требованиями статьи 21 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», «___» _____ 20__ года осуществил уточнение / блокирование / уничтожение (ненужное зачеркнуть) персональных данных, относящихся к вышеуказанному субъекту персональных данных. Дополнительная информация (указывается при необходимости): (перечень персональных данных, относящийся к соответствующему субъекту персональных данных, в случае их уточнения)

_____ _____
_____ (должность) (подпись) (фамилия, имя, отчество)
«____» _____ 20___ года

Приложение 6
к Правилам рассмотрения [наименование организации, учреждения]
запросов субъектов персональных данных или их представителей

УВЕДОМЛЕНИЕ субъекта персональных данных (представителя субъекта персональных данных) об отказе в уточнении, блокировании или уничтожении его персональных данных (На бланке организации)

В ответ на Ваш запрос от «____» _____ 20___ года, на уточнение, блокирование или уничтожение персональных данных, относящихся к следующему субъекта персональных данных_____ (фамилия, имя, отчество субъекта персональных данных) [наименование организации, учреждения], отказывает в уточнении / блокировании / уничтожении (ненужное зачеркнуть) обрабатываемых персональных данных по следующей причине: (указывается причина отказа)

_____ _____
_____ (должность) (подпись) (фамилия, имя, отчество)
«____» _____ 20___ года

Приложение 7
к Правилам рассмотрения [наименование организации, учреждения]
запросов субъектов персональных данных или их представителей

УТВЕРЖДАЮ _____ / _____ «____» _____ 20__ г.

ЖУРНАЛ учета обращений субъектов персональных данных и представителей субъектов персональных данных [наименование организации, учреждения]

Начат: «___» _____ 20___ г. На ____ листах Окончен: «___» _____ 20___ г. _____ (ФИО ответственного лица за ведение журнала) _____ подпись

№№	Фамилия И.О. обратившегося лица	Документы, подтверждающие полномочия обратившегося лица	Сведения о запросе			Сведения о принятом решении		Подпись исполнителя	Примечания
			Дата поступления запроса	Предмет	Действие по обращению	Дата отправления ответа	Основание		
1	2	3	4	5	6	7	8	9	10
1	Иванов А.А.	Паспорт РФ	дата	Уничтожение ПДн	Осуществлено уничтожение ПДн	дата	ч. 3 ст. 20 ФЗ «О персональных данных»		

Приложение 8
к Правилам рассмотрения [наименование организации, учреждения]
запросов субъектов персональных данных или их представителей

Порядок и сроки обработки запросов и обращений субъектов персональных данных на получение информации, касающейся обработки персональных данных

В таблицах 8.1 – 8.6 рассматриваются возможные случаи, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», когда субъект персональных данных (представитель субъекта персональных данных) может обратиться или направить запрос оператору.

В каждой таблице описан порядок действий при реагировании на запросы и обращения субъектов персональных данных (представителей персональных данных), а также сроки выполнения указанных действий.

Таблица 8.1 – Сроки выполнения запроса и обращения субъекта персональных данных (представителя субъекта персональных данных) на получение информации, касающейся обработки персональных данных

№	Действие	Срок выполнения действия	Примечание
1	Предоставить субъекту ПДн или его представителю запрашиваемую информацию, касающуюся обработки его ПДн, и предоставить	В течение 30 дней со дня получения запроса субъекта ПДн или его представителя	Запрашиваемая информация не может быть предоставлена субъекту ПДн или его представителю в случаях, предусмотренных в п.8 ст.14 Федерального закона от 27.07.2006 № 152- ФЗ «О персональных

	возможность ознакомления с этими ПДн (согласно п.7 ст.14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»		данных»
2	Если запрашиваемая информация не может быть предоставлена субъекту ПДн или его представителю в соответствии с п.8 ст.14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», дать в письменной форме мотивированный ответ	В срок, не превышающий 30 дней со дня со дня получения запроса или обращения субъекта ПДн или его представителя	Мотивированный ответ должен содержать ссылку на п.8 ст.14 Федерального закона от 27.07.2006 № 152- ФЗ «О персональных данных» или на иной федеральный закон, являющийся основанием для отказа

Таблица 8.2 – Возможные сроки направления субъектом персональных данных (представителем субъекта персональных данных) повторного запроса или обращения на получение информации, касающейся обработки персональных данных

№	Действие	Срок выполнения действия	Примечание
1	Если запрашиваемая информация и/или обрабатываемые ПДн были предоставлены в полном объеме, субъект ПДн вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения информации, касающейся обработки его ПДн, и ознакомления с такими ПДн	Не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса	Если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн
2	Если запрашиваемая информация и/или обрабатываемые ПДн не были предоставлены в полном объеме, субъект ПДн вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения информации, касающейся обработки его ПДн, и ознакомления с такими ПДн	В любое время	Повторный запрос должен содержать обоснование направления такого запроса

Таблица 8.3 – Сроки выполнения запроса и обращения субъекта персональных данных (представителя субъекта персональных данных) на уточнение его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными

№	Действие	Срок выполнения действия	Примечание
1	Блокировать на период проверки ПДн, относящиеся к субъекту ПДн, или обеспечить их блокирование лицом, действующим по поручению оператора	Сразу после получения запроса или обращения от субъекта ПДн или его представителя	Если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц
2	Если подтвержден факт обработки неполных, устаревших, неточных ПДн, уточнить ПДн или обеспечить их уточнение лицом, действующим по поручению оператора на основании предоставленных сведений, подтверждающих, что ПДн субъекта являются неполными, неточными или неактуальными, и снять блокирование ПДн	В срок, не превышающий 7 рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными	-
3	Уведомить субъекта ПДн или его	Сразу после внесения изменений в	-

	представителя о внесенных изменениях, а также уведомить третьих лиц, которым ПДн этого субъекта были переданы	ПДн	

аблица 8.4 – Сроки выполнения запроса и обращения субъекта персональных данных (представителя субъекта персональных данных) на уточнение его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки

№	Действие	Срок выполнения действия	Примечание
1	Уничтожить ПДн, которые являются незаконно полученными или не являются необходимыми для заявленной цели обработки	В срок, не превышающий 7 рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки	-
2	Уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах, а также уведомить третьих лиц, которым ПДн этого субъекта были переданы	Сразу после уничтожения ПДн	-

Таблица 8.5 – Сроки выполнения запроса и обращения субъекта персональных данных (представителя субъекта персональных данных) в случае выявления неправомерной обработки персональных данных

№	Действие	Срок выполнения действия	Примечание
1	Блокировать на период проверки неправомерно обрабатываемые ПДн, относящиеся к субъекту ПДн, или обеспечить их блокирование лицом, действующим по поручению оператора	Сразу после получения запроса или обращения от субъекта ПДн или его представителя	-
2	Если подтвержден факт неправомерной обработки ПДн, прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению оператора	В срок, не превышающий 3 рабочих дня со дня выявления неправомерной обработки ПДн	-
3	Если обеспечение правомерности обработки ПДн невозможно, уничтожить неправомерно обрабатываемые ПДн или обеспечить их уничтожение лицом, действующим по поручению оператора	В срок, не превышающий 10 рабочих дней со дня выявления неправомерной обработки ПДн	-
4	Если отсутствует возможность уничтожения ПДн в течение срока, указанного в п.3 данной таблицы, блокировать ПДн или обеспечить их блокирование лицом, действующим по поручению оператора и обеспечить уничтожение ПДн	В срок не более чем 6 месяцев	
5	Уведомить субъекта ПДн или его представителя об устранении допущенных нарушений или об уничтожении ПДн	После устранения допущенных нарушений/ после уничтожения ПДн	Если иной срок не установлен федеральными законами

Таблица 8.6 – Сроки выполнения запроса и обращения субъекта персональных данных (представителя субъекта персональных данных) в случае отзыва согласия на обработку персональных данных

№	Действие	Срок выполнения действия	Примечание
1	Прекратить обработку ПДн или обеспечить прекращение такой обработки лицом,	Сразу после поступления отзыва согласия на обработку ПДн	-

	действующим по поручению оператора		
2	Если сохранение ПДн более не требуется для целей обработки ПДн или если оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн, уничтожить ПДн или обеспечить их уничтожение лицом, действующим по поручению оператора	В срок, не превышающий 30 дней со дня поступления указанного отзыва	Если иные сроки не предусмотрены договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между оператором и субъектом ПДн
3	Если отсутствует возможность уничтожения ПДн в течение срока, указанного в п.2 данной таблицы, блокировать ПДн или обеспечить их блокирование лицом, действующим по поручению оператора и обеспечить уничтожение ПДн	В срок не более чем 6 месяцев	Если иной срок не установлен федеральными законами

Приложение 9
к Правилам рассмотрения [наименование ОИВ, организации, учреждения]
запросов субъектов персональных данных или их представителей

РАЗЪЯСНЕНИЕ субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (На бланке организации)

Уважаемый_____ (фамилия, имя, отчество субъекта персональных данных) (фамилия, имя, отчество представителя субъекта персональных данных, реквизиты доверенности или иного документа, подтверждающего полномочия представителя) (номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе)

уведомляем Вас, что обязанность предоставления Вами персональных данных установлена:_____
_____
_____
(основания предоставления персональных данных, установленные законодательством Российской Федерации)

В случае отказа Вами предоставить свои персональные данные [наименование организации, учреждения]: (юридические последствия отказа предоставления персональных данных)

_____ _____
_____ (должность) (подпись) (фамилия, имя, отчество)
«____» _____ 20___ года

Приложение № 46.
Правила осуществления
внутреннего контроля

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом № 152-ФЗ, иными нормативными правовыми актами и локальными актами ООО «Центр детских и юношеских программ «Мир»» (далее - Учреждение), в Учреждении организуется проведение плановых и внеплановых проверок (далее - проверки).

2. Плановые проверки проводятся в соответствии с планом, утвержденным генеральным директором Учреждения (далее – Генеральный директор).

Плановая проверка организуется ответственным за организацию обработки персональных данных в Учреждении не реже 1 раза в год.

В план проверки включаются объекты внутреннего контроля, срок проведения плановой проверки, ответственные исполнители.

Срок проведения плановой проверки не должен превышать одного месяца.

3. Внеплановые проверки проводятся по поручению Генеральный директор или ответственного за организацию обработки персональных данных в случаях:

1) поступления в Учреждение в письменной форме или форме электронного документа заявления субъекта персональных данных или его представителя о фактах нарушений требований законодательства Российской Федерации при обработке персональных данных;

2) выявления инцидента информационной безопасности (событие или комбинация событий), указывающего на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности, результатом которой являются:

нарушение или возможное нарушение работы средств защиты информации в составе информационных систем;

нарушение или возможное нарушение требований законодательства Российской Федерации, локальных актов Учреждения, регулирующих порядок обработки персональных данных;

нарушение или возможное нарушение выполнения технологических процессов обработки персональных данных в информационных системах.

4. Проведение внеплановой проверки организуется в течение пяти рабочих дней с момента возникновения соответствующих оснований. Срок проведения внеплановой проверки не должен превышать пятнадцати рабочих дней со дня принятия решения о ее проведении.

5. Проверки проводятся комиссией в составе не менее трех человек, утверждаемой приказом Учреждения. В состав комиссии в обязательном порядке включается работник, в должностные обязанности которого входит защита информации. Комиссию возглавляет ответственный за организацию обработки персональных данных.

6. Проверки проводятся непосредственно на месте обработки персональных данных, при этом производится проверка документов, опрос и осмотр рабочих мест работников Учреждения, участвующих в процессе обработки персональных данных.

7. При проведении проверок должны быть полностью, всесторонне и объективно установлены:

1) соблюдение правил обработки персональных данных в Учреждении (отделении (структурном подразделении) Учреждения);

2) соблюдение правил работы с обезличенными персональными данными в Учреждении (отделении (структурном подразделении) Учреждения);

3) соблюдение порядка доступа работников Учреждения в помещения, в которых ведется обработка персональных данных;

4) наличие (отсутствие) фактов несанкционированного доступа к персональным данным;

5) наличие (отсутствие) фактов неправомерной обработки персональных данных;

6) соблюдение требований к защите персональных данных, установленных Федеральным законом № 152-ФЗ.

8. При проведении проверок комиссия имеет право:

1) запрашивать у работников Учреждения информацию, необходимую для осуществления внутреннего контроля;

2) вносить ответственному за организацию обработки персональных данных в Учреждении предложения о совершенствовании правового и организационного регулирования обеспечения безопасности персональных данных при их обработке.

9. По результатам проверки оформляется письменное заключение с указанием мер, необходимых для устранения выявленных нарушений.

Приложение № 47.
Модель угроз безопасности

Модель угроз безопасности персональных данных ООО «_____»
(далее – Общество)

I. Перечень обозначений и сокращений

1. АРМ - автоматизированное рабочее место;
2. ИР - информационный ресурс;
3. ИСПДн - информационная система персональных данных;
4. КЗ - контролируемая зона;
5. ПДн - персональные данные;
6. ПО - программное обеспечение;
7. ПТС - программно-технические средства;
8. ПЭМИН - побочные электромагнитные излучения и наводки;
9. СЗИ - средства защиты информации;
10. СКЗИ - средства криптографической защиты информации;
11. ФСБ - Федеральная служба безопасности;
12. ФСО - Федеральная служба охраны;
13. ФСТЭК - Федеральная служба по техническому и экспертному контролю.

II. Общие положения

1.Настоящая модель угроз безопасности персональных данных (далее - Модель) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в Обществе. Указанные угрозы могут исходить от источников, имеющих антропогенный, техногенный и стихийный характер и воздействующих на уязвимости ИСПДн, характерные для данной ИСПДн, реализуя тем самым угрозы информационной безопасности.

2.В Модели дается обобщенное описание ИСПДн, состав, категории и предполагаемый объем обрабатываемых ПДн с последующей классификацией ИСПДн.

3.Модель описывает потенциального нарушителя безопасности ПДн и подходы по определению актуальности угроз с учетом возможностей нарушителя и особенностей конкретной ИСПДн.

4.Настоящая Модель разработана в соответствии с требованиями Федерального законодательства и федеральных органов по защите персональных данных.

III. Характеристика объекта информатизации

1. В качестве объекта информатизации школы выступают автономные автоматизированные рабочие места (АРМ).

2. Ввод персональных данных осуществляется как с бумажных носителей (например, документов, удостоверяющих личность субъекта ПДн), так и с электронных носителей информации. Категории персональных данных: фамилия, имя, отчество, год рождения, месяц рождения, дата рождения, место рождения, адрес, семейное положение, образование, профессия, состояние здоровья;

3. ИСПДн предполагают распределенную (на АРМ) обработку и хранение ПДн.

4. Персональные данные субъектов ПДн могут выводиться из ИСПДн с целью передачи персональных данных субъектов Учреждения, как в электронном, так и в бумажном виде.

5. Контролируемой зоной (КЗ) ИСПДн являются здания и отдельные помещения. В пределах контролируемой зоны находятся рабочие места пользователей и места хранения архивных копий данных, сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование,

используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

IV. Состав, категории и объем персональных данных, определение уровня защищенности персональных данных

1. На основе характеристик и особенностей используемых ИСПДн и обрабатываемых в них персональных данных, можно констатировать, что персональные данные субъектов ПДн, обрабатываются в Учреждении информационной системой, обрабатывающей общедоступные персональные данные, а также системой, обрабатывающей иные категории персональных данных, специальные категории персональных данных. Биометрические персональные данные в ИСПДн Учреждения не обрабатываются.

2. Для ИСПДн Общества актуальны угрозы 3 типа - угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе. Согласно подпункту «б» пункта И «Требований к защите персональных данных при их обработке в информационных системах персональных данных» для ИСПДн Общества требуется обеспечить 2-ий уровень защищенности персональных данных при их обработке в информационной системе.

V. Способы нарушения характеристик безопасности персональных данных

Исходя из перечня персональных данных, обрабатываемых в ИСПДн, существуют следующие способы нарушения характеристик безопасности ПДн:

- хищение персональных данных сотрудниками Учреждения для использования в корыстных целях; - передача финансовой, адресной, юридической и прочей информации о субъекте ПДн третьим лицам;
- несанкционированное публичное разглашение персональных данных, ставших известными сотрудникам Общества;
- несанкционированное получение персональных данных третьими лицами; - уничтожение финансовой, адресной и прочей информации о субъекте ПДн,
- блокирование финансовой, адресной и прочей информации о субъекте ПДн; - ввод некорректной финансовой, адресной и прочей информации о субъекте ПДн;
- передача некорректной финансовой, адресной и прочей информации о субъекте ПДн;
- искажение архивной информации по субъекту ПДн;
- уничтожение архивной информации по субъекту ПДн.

VI. Угрозы безопасности персональных данных, при их обработке в информационных системах персональных данных

1. Под угрозами безопасности персональных данных при их обработке в ИСПДн понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее. Таким образом, угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн, так и со специально осуществляемыми неправомерными действиями отдельных организаций и граждан, а также иными источниками угроз. Неправомерные действия могут исходить также и от сотрудников Учреждения в случае, когда они рассматриваются в качестве потенциального нарушителя безопасности ПДн.

2. В целях формирования систематизированного перечня угроз безопасности ПДн при их обработке в ИСПДн и разработке на их основе частных (детализированных) моделей применительно к конкретному виду ИСПДн, угрозы безопасности персональным данным в ИСПДн можно классифицировать в соответствии со следующими признаками:

- по видам возможных источников угроз;
- по типу ИСПДн, на которые направлена реализация угроз;
- по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);

- по способам реализации угроз;
- по используемой уязвимости;
- по объекту воздействия.

3. Для ИСПДн существуют следующие классы угроз безопасности ПДн:

- По видам возможных источников угроз безопасности персональных данных:

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющими доступ к ИР ИСПДн, включая пользователей, реализующие угрозы непосредственно в ИСПДн;

- угрозы, возникновение которых напрямую зависит от свойств техники, используемой в ИСПДн;

- угрозы, связанные со стихийными природными явлениями. Кроме этого, угрозы могут возникать в результате внедрения аппаратных закладок и вредоносных программ.

- По типу ИСПДн, на которые направлена угроза: По структуре ИСПДн, на которые направлена угроза, необходимо рассматривать следующие классы угроз:

- угрозы безопасности данных, обрабатываемых в ИСПДН на базе автоматизированных рабочих мест; - По способам реализации угроз.

По способам реализации угроз выделяют следующие классы угроз:

- угрозы, связанные с несанкционированным доступом к ПДн (в том числе угрозы внедрения вредоносных программ); - угрозы специальных воздействий на ИСПДн.

- По виду нарушаемого свойства информации (несанкционированных действий, осуществляемых с персональными данными)

По виду несанкционированных действий, осуществляемых с персональными данными, можно выделить следующий класс угроз: угрозы, приводящие к нарушению конфиденциальности ПДн (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;

- угрозы, приводящие к несанкционированному воздействию на содержание информации, в результате которого происходит изменение данных или их уничтожение;

- угрозы, приводящие к несанкционированному воздействию на программные или программноаппаратные элементы ИСПДн, в результате которого осуществляется блокирование данных. –

По используемой уязвимости выделяются следующие классы угроз:

- угрозы, реализуемые с использованием уязвимости системного программного обеспечения (ПО);

- угрозы, реализуемые с использованием уязвимости прикладного ПО; - угрозы, возникающие в результате использования уязвимости, вызванной наличием в ИСПДн аппаратной закладки;

- угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;

- угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации технической защиты информации от несанкционированного доступа;

- угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации; - угрозы, реализуемые с использованием уязвимостей средств защиты информации. - По объекту воздействия выделяются следующие классы угроз:

- угрозы безопасности ПДн, обрабатываемых на АРМ;
- угрозы безопасности ПДн, передаваемых по сетям связи;
- угрозы прикладным программам, с помощью которых обрабатываются ПДн;
- угрозы системному ПО обеспечивающему функционирование ИСПДн.

VII. Характеристика источников угроз безопасности персональных данных в ИСПДн

В отношении ИСПДн могут существовать три типа источников угроз безопасности ПДн:

1. Антропогенные источники угроз безопасности ПДн.
2. Техногенные источники угроз безопасности ПДн.
3. Стихийные источники угроз безопасности ПДн.

- Антропогенные источники угроз безопасности ПДн В качестве антропогенного источника угроз для ИСПДн необходимо рассматривать субъекта (личность), имеющего санкционированный или несанкционированный доступ к работе со штатными средствами ИСПДн, действия которого могут привести к нарушению безопасности персональных данных. Антропогенные источники угроз по отношению к ИСПДн могут быть как внешними, так и внутренними

Среди внешних антропогенных источников можно выделить случайные и преднамеренные источники.

Случайные (непреднамеренные) источники могут использовать такие уязвимости, как ошибки, совершенные при проектировании ИСПДн и ее элементов, ошибки в программном обеспечении; различного рода сбои и отказы, повреждения, проявляемые в ИСПДн. К таким источникам можно отнести персонал поставщиков различного рода услуг, персонал надзорных организаций и аварийных служб и т.п. Действия (угрозы), исходящие от данных источников, совершаются по незнанию, невнимательности или халатности, из любопытства, но без злого умысла. Преднамеренные источники проявляются в корыстных устремлениях нарушителей.

Основная цель таких источников - умышленная дезорганизация работы, вывод систем Организации из строя, искажение информации за счет проникновения в ИСПДн путем несанкционированного доступа.

Внутренними источниками, как правило, являются специалисты в области программного обеспечения и технических средств, в том числе средств защиты информации, имеющие возможность использования штатного оборудования и программно-технических средств ИСПДн.

К таким источникам можно отнести основной персонал, представителей служб безопасности, вспомогательный и технический персонал.

Для внутренних источников угроз особое место занимают угрозы в виде ошибочных действия и (или) нарушений требований эксплуатационной и иной документации сотрудниками Учреждения, имеющих доступ к ИР ИСПДн.

К подобным угрозам, в частности, относятся:

- непредумышленное искажение или удаление программных компонентов;
- игнорирование организационных ограничений (установленных правил) при работе с ресурсами ИСПДн, включая средства защиты информации. В частности:
- нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (ключевой, парольной и аутентифицирующей информации);
- предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований;
- настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов;
- несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа. Наибольшую опасность представляют преднамеренные угрозы, исходящие как от внешних, так и от внутренних антропогенных источников. Необходимо рассматривать следующие классы таких угроз:
- угрозы, связанные с преднамеренными действиями лиц, имеющими доступ к ИСПДн, включая пользователей ИСПДн и иных сотрудников Учреждения, реализующими угрозы непосредственно в ИСПДн (внутренний нарушитель);
- угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к ИСПДн и реализующими угрозы из внешних сетей связи общего пользования или сетей международного

информационного обмена (внешний нарушитель); - угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к ИСПДн и реализующими угрозы по ТКУ И.

- Техногенные источники угроз безопасности ПДн Техногенные источники угроз напрямую зависят от свойств техники. Данные источники также могут быть как внешними, так и внутренними. К внешним источникам относятся инфраструктурные элементы ИСПДн: средства связи (телефонные линии, линии передачи данных и т.п.), сети инженерных коммуникаций (водоснабжение, канализация, отопление и пр.). К внутренним источникам относятся некачественные технические и программные средства обработки информации, вспомогательные средства (охраны, сигнализации, телефонии), другие технические средства, применяемые в ИСПДн, а также вредоносное программное обеспечение и аппаратные закладки. Аппаратная закладка Аппаратные закладки могут быть конструктивно встроенными и автономными. Аппаратные закладки могут реализовать угрозы: - сбора и накопления ПДн, обрабатываемых и хранимых в ИСПДн;

- формирования ТКУИ. В силу отмеченных свойств аппаратных закладок эффективная защита от них может быть обеспечена только за счет тщательного учета их специфики и соответствующей организации технической защиты информации на всех стадиях жизненного цикла ИСПДн. Носитель вредоносной программы В качестве носителя вредоносной программы в ИСПДн может выступать аппаратный элемент средств вычислительной техники из состава ИСПДн или ПО, выполняющее роль программного контейнера. Если вредоносная программа не ассоциируется с какой-либо прикладной программой из состава системного или общего ПО ИСПДн, в качестве ее носителя выступают:

- внешний машинный (отчуждаемый) носитель, т.е. дискета, оптический диск, лазерный диск, флэшпамять, внешний жесткий диск и т.п.; -

встроенные носители информации (жесткие диски, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок устройства

- видеоадаптера, сетевой платы, устройств ввода/вывода и т. д.)

- микросхемы внешних устройств (монитора, клавиатуры, принтера, плоттера, сканера и т.п.).

В том случае, если вредоносная программа может быть проассоциирована с системным или общим ПО, с файлами различной структуры или с сообщениями, передаваемыми по сети, то ее носителем являются:

- пакеты передаваемых по сети ИСПДн сообщений;

- файлы (исполняемые, текстовые, графические и т.д.).

При возникновении угроз из данной группы появляется потенциальная возможность нарушения конфиденциальности, целостности, доступности и других характеристик безопасности ПДн. Стихийные источники угроз безопасности ПДн Стихийные источники угроз отличается большим разнообразием и непредсказуемостью и являются, как правило, внешними по отношению к Учреждению. Под ними, прежде всего, рассматриваются различные природные катаклизмы: пожары, землетрясения, ураганы, наводнения. Возникновение этих источников трудно спрогнозировать и им тяжело противодействовать, но при наступлении подобных событий нарушается штатное функционирование самой ИСПДн и ее средств защиты, что потенциально может привести к нарушению конфиденциальности, целостности, доступности и других характеристик безопасности ПДн. Защита от угроз, исходящих от техногенных и стихийных источников угроз безопасности ПДн, регламентируется инструкциями, разработанными и утвержденными оператором с учетом особенностей эксплуатации ИСПДн. VIII.

VIII. Модель нарушителя безопасности персональных данных

1. Анализ возможностей, которыми может обладать нарушитель, проводится в рамках модели нарушителя. При разработке модели нарушителя зафиксированы следующие положения:

- Безопасность ПДн в ИСПДн обеспечивается средствами защиты информации ИСПДн, а также используемыми в них информационными технологиями, техническими и программными средствами, удовлетворяющими требованиям по защите информации, устанавливаемым в соответствии с законодательством Российской Федерации; - Средства защиты информации (СЗИ) штатно функционируют совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к СЗИ требований;

- СЗИ не могут обеспечить защиту ПДн от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СЗИ не может обеспечить защиту ПДн от раскрытия лицами, которым предоставлено право на доступ к этим данным).

2 .Описание нарушителей. С точки зрения наличия права постоянного или разового доступа в контролируемую зону (КЗ) объектов размещения ИСПДн все физические лица могут быть отнесены к следующим двум категориям: - категория I - лица, не имеющие права доступа в контролируемую зону ИСПДн;

- категория II - лица, имеющие право доступа в контролируемую зону ИСПДн. Все потенциальные нарушители подразделяются на:

- внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны ИСПДн;

- внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны ИСПДн. В качестве внешнего нарушителя кроме лиц категории I должны рассматриваться также лица категории II, находящиеся за пределами КЗ. В отношении ИСПДн в качестве внешнего нарушителями из числа лиц категории I могут выступать:

- бывшие сотрудники Учреждения;

- посторонние лица, пытающиеся получить доступ к ПДн в инициативном порядке; - представители преступных организаций. Внешний нарушитель может осуществлять:

- перехват обрабатываемых техническими средствами ИСПДн ПДн за счет их утечки по ТКУИ с использованием портативных, возимых, носимых, а также автономных автоматических средств разведки серийной разработки;

- деструктивные воздействия через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами КЗ; - несанкционированный доступ к информации с использованием специальных программных воздействий посредством программы вирусов, вредоносных программ, алгоритмических или программных закладок;

- перехват информации, передаваемой по сетям связи общего пользования или каналам связи, не защищенным от несанкционированного доступа (НСД) к информации организационнотехническими мерами;

- атаки на ИСПДн путем реализации угроз удаленного доступа. Внутренний нарушитель (лица категории II) подразделяется на восемь групп в зависимости от способа и полномочий доступа к информационным ресурсам (ИР) ИСПДн.

-К первой группе относятся сотрудники Учреждения, не являющиеся зарегистрированными пользователями и не допущенные к ИР ИСПДн, но имеющие санкционированный доступ в КЗ. Лицо данной группы может:

- располагать именами и вести выявление паролей зарегистрированных пользователей ИСПДн;

- изменять конфигурацию технических средств обработки ПДн, вносить программно-аппаратные закладки в ПТС ИСПДн и обеспечивать съем информации, используя непосредственное подключение к техническим средствам обработки информации.

- Ко второй группе относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ИР ИСПДн с рабочего места. К этой категории относятся сотрудники Учреждения, имеющие право доступа к локальным ИР ИСПДн для выполнения своих должностных обязанностей.

Лицо данной группы:

- обладает всеми возможностями лиц первой категории;

- знает, по меньшей мере, одно легальное имя доступа; - обладает всеми необходимыми атрибутами (например, паролем), обеспечивающим доступ к ИР ИСПДн; - располагает ПДн, к которым имеет доступ.

- К третьей группе относятся зарегистрированные пользователи подсистем ИСПДн, осуществляющие удаленный доступ к ПДн по локальной сети Учреждения. Лицо данной группы:

- обладает всеми возможностями лиц второй категории;

- располагает информацией о топологии сети ИСПДн и составе технических средств ИСПДн; - имеет возможность прямого (физического) доступа к отдельным техническим средствам (ТС) ИСПДн.

- К четвертой группе относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности ИСПДн. Лицо данной группы:

- обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте ИСПДн; - обладает полной информацией о технических средствах и конфигурации сегмента ИСПДн;

- имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте ИСПДн;

- имеет доступ ко всем техническим средствам сегмента ИСПДн;

- обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента ИСПДн.

- К пятой группе относятся зарегистрированные пользователи с полномочиями системного администратора, выполняющего конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства мониторинга, резервного копирования, антивирусного контроля, защиты от несанкционированного доступа. Лицо данной группы:

- обладает полной информацией о системном, специальном и прикладном ПО, используемом в ИСПДн;

- обладает полной информацией о ТС и конфигурации ИСПДн - имеет доступ ко всем ТС ИСПДн и данным; - обладает правами конфигурирования и административной настройки ТС ИСПДн.

- К шестой группе относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности Учреждения, отвечающего за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей, криптографическую защиту информации. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор. Лицо данной группы:

- обладает полной информацией об ИСПДн;

- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;

- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

- К седьмой группе относятся лица из числа программистов - разработчиков сторонней организации, являющихся поставщиками ПО и лица, обеспечивающие его сопровождение на объекте размещения ИСПДн. Лицо данной группы:

- обладает информацией об алгоритмах и программах обработки информации в ИСПДн;

- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в ПО ИСПДн на стадии его разработки, внедрения и сопровождения; - может располагать любыми фрагментами информации о ТС обработки и защиты информации в ИСПДн.

-К восьмой группе относятся персонал, обслуживающий ТС ИСПДн, а также лица, обеспечивающие поставку, сопровождение и ремонт ТС ИСПДн. Лицо данной группы:

- обладает возможностями внесения закладок в ТС ИСПДн на стадии их разработки, внедрения и сопровождения;

- может располагать фрагментами информации о топологии ИСПДн, автоматизированных рабочих местах, серверах и коммуникационном оборудовании, а также о ТС защиты информации в ИСПДн.

3. Предположения о возможностях нарушителя. Для получения исходных данных о ИСПДн нарушитель (как I категории, так и II категории) может осуществлять перехват зашифрованной информации и иных данных, передаваемых по каналам связи сетям общего пользования и (или) сетям международного информационного обмена, а также по локальным сетям ИСПДн. Любой внутренний нарушитель может иметь физический доступ к линиям связи, системам электропитания и заземления. Предполагается, что возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны объектов размещения ИСПДн ограничительных факторов, из которых основными являются режимные мероприятия и организационно-технические меры, направленные на:

- предотвращение и пресечение несанкционированных действий;

- подбор и расстановку кадров;

- допуск физических лиц в контролируемую зону и к средствам вычислительной техники; - контроль над порядком проведения работ.

В силу этого внутренний нарушитель не имеет возможности получения специальных знаний о ИСПДн в объеме, необходимом для решения вопросов создания и преодоления средств защиты ПДн, и исключается его возможность по созданию и применению специальных программно-технических средств реализации целенаправленных воздействий данного нарушителя на подлежащие защите объекты и он может осуществлять попытки несанкционированного доступа к ИР с использованием только штатных программно-технических средств ИСПДн без нарушения их целостности. Возможность сговора внутренних нарушителей между собой, сговора внутреннего нарушителя с персоналом организаций-разработчиков подсистем ИСПДн, а также сговора внутреннего и внешнего нарушителей должна быть исключена применением организационнотехнических и кадрово-режимных мер, действующих на объектах размещения ИСПДн.

4. Предположения об имеющихся у нарушителя средствах атак Предполагается, что нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства. Внешний нарушитель (лица категории I, а также лица категории II при нахождении за пределами КЗ) может использовать следующие средства доступа к защищаемой информации: - доступные в свободной продаже аппаратные средства и программное обеспечение, в том числе программные и аппаратные компоненты криптосредств; - специально разработанные технические средства и программное обеспечение;

- средства перехвата и анализа информационных потоков в каналах связи;

- специальные технические средства перехвата информации по ТКУИ; - штатные средства ИСПДн (только в случае их расположения за пределами КЗ). Внутренний нарушитель для доступа к защищаемой информации, содержащей ПДн, может использовать только штатные средства ИСПДн. При этом его возможности по использованию штатных средств зависят от реализованных в ИСПДн организационно-технических и режимных мер.

5. Описание каналов атак. Возможными каналами атак, которые может использовать нарушитель для доступа к защищаемой информации в ИСПДн, являются:

- каналы непосредственного доступа к объекту (визуально-оптический, акустический, физический); - электронные носители информации, в том числе съемные, сданные в ремонт и вышедшие из употребления;

- бумажные носители информации;

- штатные программно-аппаратные средства ИСПДн;

- кабельные системы и коммутационное оборудование, расположенные в пределах контролируемой зоны и не защищенные от НСД к информации организационно-техническими мерами;

- незащищенные каналы связи; ТКУИ. 6. Тип нарушителя при использовании в ИСПДн криптографических средств защиты информации При обмене информацией между ИСПДн и внешними по отношению к предприятию информационными системами необходимо использование средств криптографической защиты информации (СКЗИ).

Уровень криптографической защиты персональных данных, обеспечиваемой СКЗИ, определяется путем отнесения нарушителя, действиям которого должно противостоять СКЗИ, к конкретному типу, и базируется на подходах, описанных в «Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации».

Тип нарушителя и класс СКЗИ должен определяться в соответствии с таблицей

Таблица - Соответствие типов нарушителя и класса СКЗИ

Группа внутреннего нарушителя	Тип нарушителя	Класс СКЗИ
Группа 1	Н 2	КС2
Группа 2	ИЗ	КС3
Группа 3	ИЗ	КС3
Группа 4	ИЗ	КС3
Группа 5	ИЗ	КС3
Группа 6	ИЗ	КС3
Группа 7	Н5	КВ 2
Группа 8	Н4	КВ 1

Внешний нарушитель относится к типу Н1. При этом, если он обладает возможностями по созданию способов и подготовки атак, аналогичными соответствующим возможностям внутреннего нарушителя типа Нi (за исключением возможностей, предоставляемых пребыванием в момент атаки в контролируемой зоне), то этот нарушитель также будет обозначаться как нарушитель типа Нi.

IX. Актуальные угрозы безопасности персональных данных в информационных системах персональных данных

1. Для выявления из всего перечня угроз безопасности ПДн актуальных для ИСПДн оцениваются два показателя: - уровень исходной защищенности ИСПДн; - частота (вероятность) реализации рассматриваемой угрозы.

2. Уровень исходной защищенности информационной системы персональных данных Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн.

1. Принимается, что ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий», а остальные уровню «средний». В случае если не менее 70% характеристик ИСПДн относится к уровню «не ниже среднего», а остальные к уровню «низкий», то исходная защищенность ИСПДн будет среднего уровня. Во всех остальных случаях ИСПДн будет иметь низкий уровень защищенности. Исходя из критериев оценки, делаем вывод, что ИСПДн Учреждения имеет средний уровень защищенности.

2. Определение актуальных угроз безопасности персональных данных. Для оценки уровня исходной защищенности вводится коэффициент исходной защищенности Y1, который может принимать значения:

0 - для высокой степени исходной защищенности;

5 - для средней степени исходной защищенности;

10 - для низкой степени исходной защищенности. Следующим параметром, необходимым для определения актуальности угроз безопасности ПДн, является частота (или вероятность) реализации угрозы, под которой понимается определенный экспертным путем показатель, характеризующий вероятность реализации конкретной угрозы безопасности ПДн для ИСПДн в реальных условиях ее функционирования.

Вводится четыре значения этого показателя, обозначаемого как Y2:

маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты. Данный показатель принимает следующие значения:

0 - для маловероятной угрозы;

2 - для низкой вероятности угрозы;

5 - для средней вероятности угрозы;

10 - для высокой вероятности угрозы. Используя значения приведенных выше показателей Y1 и Y2, вычисляется коэффициент реализуемости угрозы Y, определяемый соотношением Y = (Y1+Y2)/20. В зависимости от своего значения этот коэффициент принимает значения: 0 < 0,3 - реализуемость угрозы признается низкой; 0,3 < 0,6 - реализуемость угрозы признается средней;

0,6 < 0,8 - реализуемость угрозы признается высокой; Y > 0,8 - реализуемость угрозы признается очень высокой. Далее дается оценка опасности каждой угрозы ПДн для ИСПДн. Данная оценка носит экспертный характер и получается путем опроса экспертов в области безопасности информации. Данная оценка имеет три значения: низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов ПДн;

средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов ПДн;

высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов ПДн.

После просчета всех показателей производится оценка актуальности каждой угрозы безопасности ПДн при их обработке в ИСПДн исходя из матрицы, приведенная в таблице 9.2:

Таблица 9.2 - Матрица расчета актуальности угроз безопасности ПДн

Реализуемость угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	актуальная	неактуальная	актуальная
Средняя	актуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

На основании положений модели угроз, модели нарушителя, данных об исходной защищенности ИСПДн (Y1), коэффициенте реализуемости угрозы (Y), вероятности ее реализации (Y2), а также экспертной оценки опасности угрозы, определяется актуальность каждой угрозы

безопасности ПДн, обрабатываемых в ИСПДн. (Таблица 9.3) Таблица 9.3 - Актуальность угроз безопасности ПДн

№ п/п	Угроза безопасности ПДн	Вероятность реализации угрозы	Коэффициент реализуемости угрозы	Оценка опасности угрозы	Оценка актуальности угрозы
1	Разглашение, передача или утрата атрибутов разграничения доступа к ИСПДн	5	0,75	средняя	актуальная
2	Нарушение правил хранения атрибутов разграничения доступа к ИСПДн	5	0,75	низкая	актуальная
3	Несообщение о фактах утраты, компрометации атрибутов разграничения доступа к ИСПДн	10	1,0	высокая	актуальная
4	Внедрение агентов в число персонала системы	0	0,5	высокая	актуальная
5	Несанкционированный запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.)	2	0,6	высокая	актуальная
6	Ввод ошибочных данных	10	1,0	низкая	актуальная
7	Действия сотрудников, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств	5	0,75	высокая	актуальная
8	Игнорирование организационных ограничений (установленных правил) при работе с ПД	10	1		актуальная
9	Физическое разрушение или вывод из строя всех или отдельных наиболее важных компонентов ИСПДн	0	0,5	высокая	актуальная
10	Закупки несовершенных, устаревших или неперспективных средств информатизации и информационных технологий;	0	0,5	низкая	неактуальная
11	Хищение носителей информации, содержащих ПД	2	0,6	высокая	актуальная
12	То же, внешний нарушитель	2	0,6	высокая	актуальная
13	Незаконное получение паролей и других реквизитов разграничения доступа к ИСПДн	5	0,75	средняя	актуальная
14	То же, внешний нарушитель	2	0,6	низкая	актуальная
15	Несанкционированная модификация программного обеспечения	5	0,75	высокая	актуальная
16	То же, внешний нарушитель	2	0,6	высокая	актуальная
17	Перехват ПД, передаваемых по каналам связи	0	0,5	низкая	неактуальная
18	То же, внешний нарушитель	0	0,5	низкая	неактуальная
19	Несанкционированное копирование носителей информации с ПД	5	0,75	средняя	актуальная
20	То же, внешний нарушитель	2	0,6	средняя	неактуальная
21	Чтение остаточной информации из оперативной памяти и с внеш	0	0,5	низкая	неактуальная
22	То же, внешний нарушитель	0	0,5	низкая	актуальная
23	Непреднамеренное заражение компьютера вирусами	5	0,75	низкая	актуальная
24	Преднамеренное заражение компьютера вирусами	10	1,0	низкая	актуальная
25	Вмешательство в процесс функционирования ИСПДн, сетей общего пользования с целью несанкционированной модификации данных	5	0,75	высокая	актуальная

26	То же, внешний нарушитель	2	0,6	высокая	актуальная
27	Несанкционированное внедрение и использование неучтенных программ, не являющихся необходимыми для выполнения сотрудниками своих служебных обязанностей	10	1,0	средняя	актуальная
28	То же, внешний нарушитель	5	0,75	средняя	актуальная
29	Неумышленное повреждения внешних кабельных систем связи	2	0,6	низкая	актуальная
30	Возникновение пожаров в непосредственной близости к помещениям, в которых обрабатываются ПД и архивам ПД результате неисправной электропроводки, неисправных технических средств, нарушения сотрудниками пр	2	0,6	высокая	актуальная
31	Разрушение зданий, отдельных помещений	0	0,5	высокая	актуальная
32	Возникновение стихийных очагов пожаров	2	0,6	низкая	актуальная
33	Аварии в системах электропитания	5	0,75	низкая	актуальная
34	4. Аварии в системах отопления и водоснабжения в непосредственной близости к помещениям, в которых обрабатываются ПД и архивам ПД	2	0,75	средняя	актуальная

С локальным актом «Политика обработки персональных данных оператора ООО «Автолицей Автокурс» ИНН 7727467182 ознакомлен:

№ п/п	Работник (ФИО)	Должность	Дата	Подпись