



ПРИКАЗ №2/4

Об утверждении
Регламента по обработке персональных данных

г. Москва

«20» июля 2016 г.

В соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»), Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ, приказываю:

1. Утвердить:

- 1.1. Регламент по обработке персональных данных в Обществе с ограниченной ответственностью «ЕГЭ-Центр» (ООО «ЕГЭ-Центр»)(Приложение №1);
- 1.2. Перечень лиц, допущенных к обработке персональных данных (Приложение №2).

2. Работникам организации:

Генеральному директору Капралову К.А. - ознакомить должностных лиц, указанных в Приложении №2, с приложениями к настоящему приказу.

3. Контроль за исполнением настоящего Приказа оставляю за собой.

Генеральный директор
ООО «ЕГЭ-Центр»

Капралов К.А.

С приказом ознакомлены:

Дата

подпись

Ф.И.О.

Приложение №1
к приказу ООО «ЕГЭ-Центр»
№2/4 от 20 июля 2016 г.

**Регламент обработки персональных данных в Обществе с ограниченной
ответственностью «ЕГЭ-Центр» (ООО «ЕГЭ-Центр»)**

1.1. Настоящий Регламент разработан в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»), Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ, Приказом ФСТЭК от 18 февраля 2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. системы менеджмента информационной безопасности. Требования»; ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства безопасности. Практические правила менеджмента информационной безопасности»; ГОСТ Р ИСО/МЭК 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»и другими нормативно-правовыми актами, регулирующими вопросы обработки персональных данных.

Настоящий Регламент включает:

- Регламент по допуску лиц к обработке персональных данных;
- Регламент по реагированию на запросы субъектов персональных данных;
- Регламент по взаимодействию с органами государственной власти в сфере персональных данных;
- Регламент по реагированию на инциденты информационной безопасности;
- Регламент применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн;
- Регламент применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации.

1.2. В настоящем Регламенте термины используются в значении, предусмотренном Положением об обработке персональных данных обучающихся и иных в лиц в ООО «ЕГЭ-Центр». Кроме того, для целей настоящего Регламента, устанавливаются соответствующие значения терминов и сокращений:

Оператор ПДн, Оператор – юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

ПДн – персональные данные.

Субъект персональных данных - физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

Доступ к персональным данным - возможность получения персональных данных и их использования.

ИСПДн (Информационная система персональных данных) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационная безопасность – состояние защищенности информационных ресурсов Оператора, исключающее утечку защищаемой информации, а также несанкционированных и непреднамеренных воздействий на защищаемую информацию, в

том числе на обрабатываемые Оператором персональные данные (безопасность персональных данных).

Инцидент информационной безопасности – факт нарушения информационной безопасности, приведший к снижению уровня защищенности (защиты) персональных данных.

Информационные ресурсы - информация, зафиксированная на материальных носителях и хранящаяся в информационных системах, применяемых Оператором.

Конфиденциальность персональных данных - обязательное для соблюдения Оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Нарушитель информационной безопасности – физическое лицо, чьи действия (бездействие) повлекли возникновение инцидента информационной безопасности.

Носитель персональных данных – материальный объект, на котором размещены сведения, относящиеся к персональным данным субъектов персональных данных.

Реагирование на инцидент информационной безопасности – комплекс действий, направленных на устранение последствий нарушения информационной безопасности, повышение уровня защищенности персональных данных, разбирательство по факту нарушения информационной безопасности, а также предотвращение возникновения новых инцидентов.

Средство защиты информации - техническое, программное средство, предназначенное или используемое для защиты информации.

Угроза безопасности персональных данных (актуальная угроза) - совокупность условий и факторов, создающих 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. Устанавливается три типа угроз безопасности персональных данных:

Угрозы 1-го типа (связаны с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе).

Угрозы 2-го типа (связаны с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе).

Угрозы 3-го типа (не связаны с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе).

Уровень защищенности (защиты) персональных данных – характеристика информационной безопасности, означающая определенную степень защиты сведений, относящихся к персональным данным, при которой доступ к персональным данным третьих лиц невозможен или затруднен.

Уровень критичности инцидента информационной безопасности - класс инцидента информационной безопасности в соответствии с типами угроз безопасности персональных данных, установленных Оператором.

АРМ – автоматизированное рабочее место субъекта резервного копирования.

Восстановление персональных данных с резервных копий – действия субъекта резервного копирования, направленные на приведение персональных данных в исходное состояние в информационной системе персональных данных.

Резервная копия - запись персональных данных на носителе, предназначенная для восстановления персональных данных в случае их изменения или утраты.

Резервное копирование – действия субъекта резервного копирования, направленные на создание резервных копий персональных данных.

Система резервного копирования - оснащенный программным обеспечением комплекс оборудования, объем памяти которого достаточен для создания резервных копий необходимого объема в установленные сроки и с заданной периодичностью.

Субъект резервного копирования – Пользователь информационных систем персональных данных, применяемых у Оператора, согласно Инструкции пользователя систем персональных данных.

Хранение резервных копий – регламентированный порядок учета и поддержания резервных копий персональных данных в исходном состоянии в целях недопущения утраты персональных данных или иных действий, направленных на разглашение сведений, составляющих персональные данные.

1.3. В качестве Субъектов ПДн, персональные данные которых могут обрабатываться Оператором с использованием средств автоматизации или без использования таковых, понимаются следующие категории физических лиц:

1.3.1. Лица, имеющие договорные отношения гражданско-правового характера с Оператором или находящиеся на этапе преддоговорных отношений гражданско-правового характера;

1.3.2. Работники Оператора, то есть лица, имеющие трудовые отношения с Оператором, лица, ранее имевшие трудовые отношения с Оператором, а также соискатели на место работника Оператора, лица, проходящие практику (стажировку) у Оператора;

1.3.3. Иные Субъекты ПДн, обработка персональных данных которых подпадает под действие ФЗ «О персональных данных».

1.4. В состав персональных данных лиц, имеющих договорные отношения гражданско-правового характера с Оператором, клиентов, иных субъектов ПДн, обрабатываемых Оператором, помимо работников, входят:

- фамилия, имя, отчество;
- адрес электронной почты;
- фотографии;
- номер телефона;
- дата рождения;
- адрес проживания и(или) регистрации по месту жительства;
- данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации.

1.5. В состав персональных данных работников Оператора, то есть лиц, имеющих трудовые отношения с Оператором, лиц, ранее имевших трудовые отношения с Оператором, а также соискателей на место работника Оператора, обрабатываемых Оператором, входят:

- фамилия, имя, отчество;
 - пол;
 - дата рождения;
 - адрес регистрации по месту жительства и адрес фактического проживания;
 - номер телефона (домашний, мобильный);
 - данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации;
 - семейное положение, сведения о составе семьи, которые могут понадобиться работодателю для предоставления льгот, предусмотренных трудовым и налоговым законодательством;
 - отношение к воинской обязанности;
 - сведения о трудовом стаже, предыдущих местах работы (об опыте работы), доходах с предыдущих мест работы;
 - СНИЛС;
 - ИНН;
 - информация о приеме, переводе, увольнении и иных событиях, относящихся к трудовой деятельности в Организации;
 - сведения о доходах в Организации;
 - сведения о деловых и иных личных качествах, носящие оценочный характер;
 - материалы по проведению собеседований с соискателем на вакантную должность;
 - биометрические персональные данные: изображение человека (фотография в паспорте)
 - иные сведения, которые работник считает нужным предоставить работодателю.
- 1.6. Контроль исполнения требований настоящего Регламента, локальных

нормативных актов и положений законодательства об обработке персональных данных лежит на Кураторе ОПД.

1.7. Должностные лица Оператора, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работников, привлекаются к дисциплинарной ответственности в порядке, установленном Трудовым кодексом РФ.

1.8. В случаях однократного грубого нарушения должностным лицом Оператора трудовых обязанностей: разглашения персональных данных субъектов ПДн, ставших известными должностному лицу Оператора в связи с исполнением им своих трудовых обязанностей, Оператор вправе расторгнуть с таким должностным лицом трудовой договор. Работники Оператора, чьи трудовые обязанности связаны с обработкой персональных данных (согласно утвержденному перечню), должны быть ознакомлены с настоящим Регламентом под роспись.

1.9. Меры административной и уголовной ответственности, применяемые в связи с нарушением должностными лицами режима безопасности персональных данных субъектов ПДн, применяются в соответствии с действующим законодательством РФ.

1.10. Оператор несет ответственность за нарушение положений настоящего Регламента в пределах, предусмотренных действующим законодательством РФ.

2. Регламент по допуску лиц к обработке персональных данных

2.1. Общие положения.

2.1.1. Настоящий «Регламент по допуску лиц к обработке персональных данных» (далее — Регламент) разработан в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных») и другими нормативно-правовыми актами, регулирующими вопросы допуска лиц к обработке персональных данных.

2.1.2. Настоящий Регламент определяет основные требования к порядку допуска и обеспечения безопасности ПДн, а также обязанности должностных лиц Оператора в процессе обработки ПДн.

2.1.3. Основной задачей обеспечения безопасности ПДн при их обработке Оператором является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

Оператор принимает необходимые и достаточные меры для защиты обрабатываемых ПДн от неправомерного или случайного доступа к ним, от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними со стороны третьих лиц.

2.2. Назначение ответственных лиц.

2.2.1. Руководитель Оператора назначает лицо, ответственное за организацию обработки ПДн как с использованием средств автоматизации, так и без использования таковых (далее – Куратор ОПД). Куратор ОПД подотчетен руководителю Оператора.

2.2.2. На Куратора ОПД возлагается задача по организации выполнения требований действующего законодательства РФ и локальных нормативных актов Оператора, регламентирующих обработку ПДн субъектов ПДн.

2.2.3. Куратор ОПД обязан:

- осуществлять внутренний контроль соблюдения Оператором и его работниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных;

- доводить до сведения должностных лиц Оператора требования законодательства РФ о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;

- организовывать прием и обработку обращений и запросов Субъектов ПДн или их представителей и осуществлять контроль приема и обработки таких обращений и запросов.

На время отсутствия Куратора ОПД его обязанности исполняет должностное лицо, его замещающее, в случае отсутствия замещающего должностного лица – руководитель Оператора.

2.2.4. Ответственными за организацию выполнения требований локальных нормативных актов Оператора по вопросам обработки персональных данных и их защите в структурных подразделениях Оператора являются руководители этих подразделений, включенные в перечень работников, допущенных к сведениям, составляющим ПДн. На время отсутствия этих руководителей ответственными являются лица, замещающие их, в соответствии со штатным расписанием.

2.2.5. Ответственными за выполнение требований локальных нормативных актов Оператора по вопросам обработки персональных данных и их защите являются должностные лица - Пользователи Информационных систем персональных данных (ИСПДн) Оператора, согласно Инструкции пользователя ИСПДн, действующей у Оператора.

2.3. Должностные лица, уполномоченные обрабатывать персональные данные.

2.3.1. Доступ работников Оператора к обрабатываемым персональным данным осуществляется в соответствии с их должностными обязанностями и требованиями локальных нормативных актов Оператора.

2.3.2. Должностные лица, уполномоченные осуществлять обработку персональных данных, перед допуском к обработке персональных данных должны быть обязательно ознакомлены под роспись локальными нормативными актами Оператора по обработке ПДн.

2.4. Допуск к обработке персональных данных.

2.4.1. Допуск лиц к обработке ПДн в ИСПДн осуществляется на основании соответствующих разрешительных документов и (или) ключей (паролей) доступа.

2.4.2. Для должностных лиц, обрабатывающих ПДн с использованием средств автоматизации в соответствии со своими должностными обязанностями и (или) в рамках договорных отношений, допуск производится в соответствии с перечнем должностных лиц, допущенных к обработке информации в ИСПДн с применением средств автоматизации.

2.4.3. Факты получения доступа к ИСПДн, а также факты обработки ПДн регистрируются в соответствующих журналах учета получения доступа к ИСПДн, применяемых Оператором, в том числе с использованием средств обеспечения информационной безопасности. Информация о фактах получения доступа к обработке ПДн Субъектов ПДн хранится Оператором в течение 3 (Трех) лет.

2.4.4. Для исключения преднамеренного или непреднамеренного доступа третьих лиц к ПДн субъектов ПДн и носителям, их содержащим, при необходимости может быть введён пропускной режим в здание (помещения) Оператора и определён порядок приема, учета и контроля деятельности посетителей.

3. Регламент по реагированию на запросы субъектов персональных данных

3.1. Общие положения.

3.1.1. Настоящий Регламент регулирует отношения, возникающие при выполнении Оператором обязательств, согласно требованиям ст.ст.14, 20 и 21 Федерального закона «О персональных данных» 152-ФЗ от 27 июля 2006 года.

3.1.2. Положения настоящего Регламента распространяются на действия Оператора при получении запроса Субъекта персональных данных, его представителя или уполномоченного органа по защите прав субъектов персональных данных. Указанные действия Оператора направлены на подтверждение наличия согласия на обработку персональных данных, ознакомление с персональными данными, их уточнение или отзыв субъектом персональных данных, блокирование или уничтожение персональных данных, переданных на обработку, а также на устранение нарушений законодательства, допущенных при обработке персональных данных.

3.2. Правила рассмотрения запросов субъектов персональных данных или их представителей.

3.2.1. Субъект персональных данных имеет право на получение сведений, указанных в ч.7 ст.14 Федерального закона «О персональных данных», за исключением случаев, предусмотренных ч.8 ст.14 Федерального закона «О персональных данных».

Субъект ПДн или его законный представитель имеют право на получение информации, касающейся обработки ПДн Субъекта ПДн, в том числе содержащей:

- подтверждение обработки ПДн, а также правовые основания и цели такой обработки.
- способы обработки ПДн.
- сведения о лицах, которые имеют доступ к ПДн.
- перечень обрабатываемых ПДн и источник их получения.
- сроки обработки ПДн, в том числе сроки их хранения.
- информацию об осуществленной или о предполагаемой трансграничной передаче данных.

3.2.2. Сведения предоставляются Субъекту персональных данных или его представителю Оператором при получении Оператором соответствующего запроса Субъекта персональных данных или его представителя.

Запрос на предоставление сведений, касающихся ПДн Субъекта ПДн, должен содержать:

- номер основного документа, удостоверяющего личность Субъекта ПДн или его представителя,
- сведения о дате выдачи указанного документа и выдавшем его органе,
- сведения, подтверждающие участие Субъекта ПДн 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 Субъекта Оператором,
- запрашиваемые сведения;
- 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.

3.2.3. В случае поступления Запроса субъекта ПДн или его законного представителя по персональным данным Оператор должен выполнить следующие действия:

3.2.3.1. При получении запроса субъекта персональных данных или его представителя на наличие ПДн необходимо в течение 30 дней с даты получения запроса подтвердить обработку ПДн, в случае ее осуществления. Если обработка ПДн субъекта не ведется, то в течение 30 дней с даты получения запроса необходимо отправить уведомление об отказе подтверждения обработки ПДн.

3.2.3.2. При получении запроса Субъекта ПДн или его представителя на ознакомление с ПДн, необходимо в течение 30 дней с даты получения запроса предоставить для ознакомления ПДн, в случае осуществления обработки этих ПДн. Если обработка ПДн Субъекта не осуществляется, то в течение 30 дней с даты получения запроса необходимо отправить уведомление об отказе предоставления информации по ПДн.

3.2.3.3. При получении запроса Субъекта ПДн или его представителя на уточнение ПДн внести в них необходимые изменения в срок, не превышающий 7 рабочих дней со дня предоставления Субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, по предоставлению Субъектом ПДн или его представителю сведений, подтверждающих, что ПДн, которые относятся к соответствующему Субъекту и обработку которых осуществляет Оператор, являются персональные данные являются неполными, неточными или неактуальными и отправить уведомление о внесенных изменениях. Если обработка ПДн Субъекта не осуществляется или не были предоставлены сведения, подтверждающие, что ПДн, которые относятся к соответствующему Субъекту и обработку которых осуществляет Оператор, являются неполными, неточными или неактуальными, то в течение 30 дней с даты получения запроса следует отправить Субъекту ПДн или его представителю уведомление об отказе осуществления изменения ПДн.

3.2.3.4. При получении запроса Субъекта ПДн или его представителя на уничтожение ПДн, необходимо их уничтожить в срок, не превышающий 7 рабочих дней со дня предоставления Субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, и отправить соответствующее уведомление об уничтожении Субъекту ПДн или его представителю. Если обработка ПДн Субъекта не осуществляется, или не были предоставлены сведения, подтверждающие, что ПДн, которые относятся к соответствующему Субъекту и обработку которых осуществляет Оператор, являются незаконно полученными или не являются необходимыми для заявленной цели обработки, а также в силу необходимости обработки ПДн по требованиям иных нормативных актов, необходимо в течение 7 рабочих дней с даты получения запроса отправить уведомление об отказе в уничтожении ПДн.

3.2.3.5. При получении запроса на отзыв согласия на обработку ПДн, необходимо прекратить их обработку и, в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн в срок, не превышающий 30 дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого является Субъект ПДн, иным соглашением между Оператором и Субъектом ПДн, либо если Оператор не вправе осуществлять обработку персональных данных без согласия Субъекта ПДн на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами, регламентирующими обработку персональных данных.

3.2.3.6. При выявлении недостоверности ПДн при обращении или по запросу Субъекта ПДн или его представителя, необходимо их блокировать с момента получения такого запроса на период проверки. Если факт недостоверности ПДн подтвержден на основании сведений, представленных Субъектом ПДн, его представителем либо уполномоченным органом по защите прав субъектов персональных данных, необходимо уточнить содержание ПДн в течение 7 рабочих дней со дня представления таких сведений и снять блокирование ПДн. Если факт недостоверности ПДн не подтвержден, то необходимо отправить уведомление об отказе изменения ПДн Субъекту ПДн, его представителю или уполномоченному органу по защите прав субъектов персональных данных.

3.2.3.7. При выявлении неправомерных действий с ПДн Оператором при обращении или по запросу Субъекта ПДн или его представителя, необходимо в срок, не превышающий 3 рабочих дней с даты выявления осуществления неправомерных действий, прекратить неправомерную обработку персональных данных. В случае если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий 7 рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие ПДн. Об устраниении допущенных нарушений или об уничтожении ПДн Оператор обязан уведомить Субъекта персональных данных или его представителя, а в случае, если обращение Субъекта ПДн, его представителя, либо запрос уполномоченного органа по защите прав

субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также в указанный орган.

3.2.3.8. При достижении целей обработки ПДн Оператор обязан незамедлительно прекратить обработку ПДн и уничтожить соответствующие ПДн в срок, не превышающий 30 дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого является Субъект ПДн, иным соглашением между Оператором и Субъектом ПДн, либо если Оператор не вправе осуществлять обработку ПДн без согласия Субъекта ПДн на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами, регламентирующими порядок обработки персональных данных.

3.2.4. В случае поступления Запроса уполномоченного органа по защите прав субъектов персональных данных необходимо выполнить следующие действия:

3.2.4.1. При получении запроса о предоставлении информации уполномоченное должностное лицо Оператора в течение 30 дней предоставляет информацию, указанную в запросе и необходимую для осуществления деятельности указанного органа.

3.2.4.2. При выявлении недостоверности ПДн в связи с запросом уполномоченного органа по защите прав субъектов ПДн, необходимо их блокировать с момента получения такого запроса на период проверки. Если факт недостоверности ПДн был подтвержден на основании документов, предоставленных Субъектом ПДн или его законным представителем, необходимо в течении 7 рабочих дней уточнить ПДн у Субъекта ПДн и снять их блокирование. Если факт недостоверности ПДн не был подтвержден, то необходимо отправить уведомление об отказе изменения ПДн Субъекту ПДн и уполномоченному органу по защите персональных данных, и снять блокирование ПДн.

3.2.4.3. При выявлении неправомерных действий с ПДн Оператором по запросу уполномоченного органа по защите прав субъектов ПДн, необходимо прекратить неправомерную обработку ПДн в срок, не превышающий 3 (Трех) рабочих дней с момента получения такого запроса на период проверки. В случае невозможности обеспечения подтверждения правомерности обработки Оператором ПДн в срок, не превышающий 10 (Десяти) рабочих дней с даты выявления неправомерности действий с ПДн, необходимо уничтожить ПДн и отправить уведомление об уничтожении ПДн уполномоченному органу по защите прав субъектов персональных данных и Субъекту ПДн, персональные данные которого были уничтожены.

3.2.4.4. При достижении целей обработки ПДн, Оператор обязан незамедлительно прекратить обработку ПДн и уничтожить соответствующие ПДн в течение 30 дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого является Субъект ПДн, иным соглашением между Оператором и Субъектом ПДн, либо если Оператор не вправе осуществлять обработку ПДн без согласия Субъекта ПДн на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами, регламентирующими порядок обработки ПДн, и отправить уведомление об уничтожении ПДн уполномоченному органу по защите прав субъектов персональных данных и Субъекту ПДн, персональные данные которого были уничтожены.

3.2.5. В случае если сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления Субъекту ПДн по его запросу, Субъект ПДн вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений и ознакомления с такими персональными данными не ранее чем через 20 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 является Субъект ПДн.

3.2.6. Субъект ПДн вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в п. 3.2.5. настоящего Регламента в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п. 3.2.2. настоящего Регламента, должен содержать обоснование направления повторного запроса.

3.2.7. Оператор вправе в мотивированной форме отказать Субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным п.п. 2.5.-2.7. настоящего Регламента, в порядке, установленном Федеральным законом «О персональных данных». Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

3.2.8. Право Субъекта ПДн на доступ к его персональным данным может быть ограничено в соответствии с законодательством РФ.

3.3. Порядок реагирования на поступление запроса Субъекта ПДн и уполномоченного органа по защите прав субъектов ПДн.

3.3.1. При получении запросов, указанных в п.п.3.2.3-3.2.5 настоящего Регламента, работник Оператора, ответственный за обработку входящей корреспонденции, выполняет следующие действия:

3.3.1.1. В случае поступления запроса субъекта ПДн или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных, необходимо зарегистрировать поступивший запрос в «Журнале учета обращений субъектов персональных данных».

3.3.2. При личном обращении Субъекта ПДн к Оператору, уполномоченный работник Оператора принимает запрос в произвольной форме. После принятия запроса в произвольной форме уполномоченное должностное лицо Оператора сверяет сведения в запросе с предоставленными ему документами.

3.3.3. В случае отсутствия документов, удостоверяющих личность Субъекта ПДн или его законного представителя, работник Оператора вправе отказать в приеме запроса и потребовать переделать запрос в соответствии с положениями Федерального закона «О персональных данных». При отказе субъекта ПДн или его законного представителя переделать запрос, работник Оператора делает об этом запись в «Журнале учета обращений субъектов персональных данных».

3.3.4. В случае, если запрос оформлен в соответствии с требованиями действующего законодательства РФ, он принимается к обработке в соответствии с положениями п.п.3.2.1-3.2.8 настоящего Регламента.

4. Регламент по взаимодействию с органами государственной власти в сфере персональных данных.

4.1. Общие положения.

4.1.1. Настоящим Регламентом по взаимодействию с органами государственной власти в сфере персональных данных определяется порядок действий уполномоченных должностных лиц Оператора при осуществлении взаимодействия с органами государственной власти в области персональных данных.

4.1.2. Настоящий Регламент принят в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля», Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», иных нормативных актах, регулирующих порядок взаимодействия физических и юридических лиц с органами государственной власти.

4.2. Правила реагирования на запросы органов государственной власти в сфере персональных данных.

4.2.1. Все поступившие запросы со стороны органов государственной власти подлежат обязательному учету в Журнале учета запросов органов государственной власти.

4.2.2. Указанный Журнал учета запросов органов государственной власти ведется лицом, ответственным за обработку персональных данных.

4.2.3. В журнале учета запросов органов государственной власти указываются следующие сведения:

- дата и время поступления запроса;
- исходящий номер запроса;
- данные об органе государственной власти, направившем запрос;
- краткое содержание запроса;
- данные о лице, ответственном за исполнение запроса.

4.2.4. Все поступившие запросы подлежат обязательному рассмотрению лицом, ответственным за обработку персональных данных, в течение 5 (пяти) рабочих дней. В случае если в запросе указан срок, в который Оператор должен предоставить сведения, пояснения или дать ответ, такие сведения, пояснения и ответ должны быть направлены органу государственной власти в указанный в запросе срок.

В случае, если срок на ответ не указан, Оператор имеет право предоставить ответ в течение тридцати дней с момента получения указанного запроса.

При подготовке ответа на запрос проверяется соответствие запроса компетенции направившего его органа.

4.2.5. Ответ на запрос должен содержать наименование органа государственной власти, наименование Оператора, ссылку на дату и исходящий номер запроса, краткое описание запроса, а также ответ на запрос с приложением копий необходимых документов (если применимо). Ответственность за подготовку текста ответа на запрос несет лицо, ответственное за обработку персональных данных. Ответ подписывается руководителем Оператора, заверяется его печатью и направляется в государственный орган заказным письмом с уведомлением и описью вложения, либо передается нарочно под роспись работника государственного органа.

4.2.6. Ответственность за исполнение запросов органов государственной власти лежит на Кураторе ОПД.

4.2.7. В случае, если запрос государственного органа требует совершения Оператором каких-либо действий, данное требование должно быть исполнено Оператором в срок, указанный в предписании. Ответственность за исполнение предписания несет лицо, ответственное за обработку персональных данных. Совершение действий, не входящих в компетенцию лица, ответственного за обработку персональных данных, возможно после получения письменного согласия руководителя Оператора.

4.2.8. В течение 1 (одного) рабочего дня с момента исполнения предписания, лицо, ответственное за обработку персональных данных, направляет уведомление об исполнении предписания в соответствующий государственный орган заказным письмом с уведомлением и описью вложения, либо передает нарочно под роспись работника государственного органа, ответственного за прием корреспонденции.

4.2.9. Лицо, ответственное за обработку персональных данных обеспечивает сохранность всех запросов и предписаний государственных органов относительно обработки персональных данных Оператором, ответов на них, а также почтовых квитанций и описей, подтверждающих направление Оператором ответов, в течение 10 (десяти) лет.

4.2.10. В случае проведения государственным органом проверки в области обработки персональных данных, при такой проверке должны присутствовать единоличный исполнительный орган Оператора, а также лицо, ответственное за обработку персональных данных.

4.2.11. В случае если в ходе документарной проверки орган государственной власти направил Оператору мотивированный запрос о предоставлении необходимых для рассмотрения в ходе проведения документарной проверки документов, Оператор обязан предоставить указанные в запросе документы в течение десяти дней с момента получения запроса в виде копий, заверенных печатью (при ее наличии) и подписью руководителя или иного уполномоченного представителя Оператора. При этом орган государственной власти не вправе требовать нотариального удостоверения копий представляемых Оператором документов, если иное не предусмотрено законодательством Российской Федерации.

4.2.12. В случае если в ходе документарной проверки орган государственной власти направил Оператору информацию об обнаруженных противоречиях или несоответствии сведений в документах Оператора, касающихся обработки и защиты персональных данных, сведениям, имеющимся у органа государственной власти либо полученным им в ходе проведения государственного контроля, Оператор обязан в течение десяти рабочих дней представить необходимые пояснения в письменной форме.

4.2.13. Лицо, ответственное за обработку персональных данных, имеет право:

1) непосредственно присутствовать при проведении проверки, давать объяснения по вопросам, относящимся к предмету проверки;

2) получать от органа государственного контроля (надзора), органа муниципального контроля, их должностных лиц информацию, которая относится к предмету проверки и предоставление которой предусмотрено настоящим Федеральным законом;

3) знакомиться с результатами проверки и указывать в акте проверки о своем ознакомлении с результатами проверки, согласии или несогласии с ними, а также с отдельными действиями должностных лиц органа государственного контроля (надзора), органа муниципального контроля;

4) обжаловать действия (бездействие) должностных лиц органа государственного контроля (надзора), органа муниципального контроля, повлекшие за собой нарушение прав юридического лица, индивидуального предпринимателя при проведении проверки, в административном и (или) судебном порядке в соответствии с законодательством Российской Федерации;

5) привлекать Уполномоченного при Президенте Российской Федерации по защите прав предпринимателей либо уполномоченного по защите прав предпринимателей в субъекте Российской Федерации к участию в проверке.

4.2.14. Лицо, ответственное за обработку персональных данных, должно обеспечить необходимые условия для проведения проверки и обязан по требованию должностных лиц органа государственной власти, проводящих проверку, организовать доступ к оборудованию, в помещения, где осуществляется обработка персональных данных, предоставить необходимую информацию и документацию для достижения целей проверки.

4.2.15. Лицо, ответственное за обработку персональных данных, по итогам проведения проверки обязано потребовать от работников государственных органов, проводящих проверку, акт по установленной форме в двух экземплярах, один из которых передается Оператору. В указанном акте должны содержаться следующие сведения:

1) дата, время и место составления акта проверки;

2) наименование органа государственной власти;

3) дата и номер распоряжения или приказа руководителя, заместителя руководителя органа государственной власти;

4) фамилии, имена, отчества и должности должностного лица или должностных лиц, проводивших проверку;

5) наименование Оператора, а также фамилия, имя, отчество и должность руководителя, иного должностного лица или уполномоченного представителя Оператора, присутствовавших при проведении проверки;

6) дата, время, продолжительность и место проведения проверки;

7) сведения о результатах проверки, в том числе о выявленных нарушениях требований законодательства в сфере персональных данных, об их характере и о лицах, допустивших указанные нарушения;

8) сведения об ознакомлении или отказе в ознакомлении с актом проверки руководителя, иного должностного лица или уполномоченного представителя юридического лица, индивидуального предпринимателя, его уполномоченного представителя, присутствовавших при проведении проверки, о наличии их подписей или об отказе от совершения подписи, а также сведения о внесении в журнал учета проверок записи о проведенной проверке либо о невозможности внесения такой записи в связи с отсутствием у юридического лица, индивидуального предпринимателя указанного журнала;

9) подписи должностного лица или должностных лиц, проводивших проверку.

К акту проверки прилагаются протоколы или заключения проведенных исследований, испытаний и экспертиз, объяснения работников юридического лица, работников индивидуального предпринимателя, на которых возлагается ответственность за нарушение законодательства в сфере персональных данных, предписания об устранении выявленных нарушений и иные связанные с результатами проверки документы или их копии.

4.2.16. Лицо, ответственное за обработку персональных данных, обязано потребовать у должностных лиц органов государственной власти осуществить запись в журнале учета проверок о проведенной проверке, содержащей сведения о наименовании органа государственной власти, датах начала и окончания проведения проверки, времени ее проведения, правовых основаниях, целях, задачах и предмете проверки, выявленных нарушениях и выданных предписаниях, а также указываются фамилии, имена, отчества и должности должностного лица или должностных лиц, проводящих проверку, его или их подписи.

4.2.17. Лицо, ответственное за обработку персональных данных, по согласованию с единоличным исполнительным органом Оператора, в случае несогласия с фактами, выводами, предложениями, изложенными в акте проверки, либо с выданным предписанием об устранении выявленных нарушений, обязано в течение пятнадцати дней с даты получения акта проверки представить в соответствующий орган государственной власти в письменной форме возражения в отношении акта проверки и (или) выданного предписания об устранении выявленных нарушений в целом или его отдельных положений, приложив к таким возражениям документы, подтверждающие обоснованность таких возражений, или их заверенные копии либо в согласованный срок передать их в орган государственной власти.

5. Регламент по реагированию на инциденты информационной безопасности

5.1. Общие положения.

5.1.1. Настоящим Регламентом по реагированию на инциденты информационной безопасности (далее – Регламент) определяется порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений, а так же выявления, разбирательства и предотвращения иных инцидентов информационной безопасности при возникновении инцидентов информационной безопасности в связи с обработкой Оператором персональных данных субъектов ПДн.

5.2. Инциденты информационной безопасности.

5.2.1. К инцидентам информационной безопасности относятся:

- разглашение персональных данных, принятых на обработку Оператором;
- несанкционированный доступ третьих лиц к персональным данным, принятым на обработку Оператором;
- внедрение вредоносного программного обеспечения, приведшее к утечке сведений, составляющих персональные данные, принятые на обработку Оператором;
- компрометация учетной записи Пользователя информационных систем персональных данных, применяемых Оператором;
- нарушение правил хранения носителей персональных данных, приведшее к утрате указанных носителей;
- нарушение правил хранения персональных данных;
- иные факты нарушения информационной безопасности Оператора, приведшие к снижению уровня защищенности (защиты) персональных данных, принятых Оператором на обработку.

5.2.2. В случае выявления факта инцидента информационной безопасности Оператора, ответственность за реагирование на инцидент возлагается Оператором на Куратора ОПД.

5.3. Выявление инцидента информационной безопасности.

5.3.1. Инциденты информационной безопасности могут быть выявлены следующими способами:

- выявление фактов нарушения информационной безопасности работниками Оператора;
- результаты работы средств мониторинга информационной безопасности Оператора;
- результаты проверок и аудита (внутреннего или внешнего) деятельности Оператора;
- обращения субъектов персональных данных;
- запросы и предписания органов надзора за соблюдением прав субъектов персональных данных;
- оповещения антивирусных программ;
- другие источники информации.

5.3.2. О возникновении инцидента информационной безопасности, работники, обнаружившие инцидент, должны немедленно поставить в известность Старшего системного администратора.

5.3.3. После получения информации об инциденте, указанной в п.5.3.2. настоящего Регламента должностное лицо незамедлительно проводит первоначальный анализ полученных сведений.

5.3.4. В случае наличия признаков инцидента информационной безопасности в полученных сведениях, уполномоченное должностное лицо Оператора определяет предварительный класс опасности инцидента информационной безопасности и принимает решение о необходимости проведения разбирательства, информирует о необходимости проведения разбирательства.

5.3.5. При инциденте информационной безопасности, затрагивающем не более одного структурного подразделения, уполномоченное должностное лицо, указанное в п.5.4.4. настоящего Регламента, информирует о факте инцидента руководителя соответствующего структурного подразделения.

При инциденте информационной безопасности, затрагивающим более одного структурного подразделения, осуществляющее расследование уполномоченное должностное лицо информирует руководителей соответствующих подразделений и инициирует проведение расследования с привлечением ресурсов работников подразделения информационной безопасности.

5.3.6. Инцидент информационной безопасности (безопасности персональных данных) подлежит классификации согласно установленным Оператором, в соответствии с Постановлением Правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», типам угроз информационной безопасности (безопасности персональных данных).

5.3.7. Данные об инциденте (дата, время, источник данных, уровень критичности) подлежат занесению в регистрационный журнал инцидентов информационной безопасности. Ответственность за ведение и хранение журнала лежит на уполномоченном должностном лице Оператора, указанном в п.5.3.2. настоящего Регламента.

5.3.8. В срок не более 4(четырех) рабочих дней с момента поступления сведений об инциденте информационной безопасности, Куратор ОПД по согласованию с руководителем Оператора принимает первоочередные меры, направленные на локализацию инцидента информационной безопасности и минимизацию его последствий.

5.3.9. Руководитель Оператора определяет работника Оператора, ответственного за проведение расследования (при необходимости – формирует Комиссию по расследованию инцидента информационной безопасности), и передает ему (Комиссии) все имеющиеся сведения для проведения расследования, а также информацию о проведенных мероприятиях по локализации инцидента информационной безопасности.

5.3.10. В случае нарушения прав субъекта персональных данных при возникновении инцидента информационной безопасности, реагирование проводится в порядке и сроки, предусмотренные Регламентом по реагированию на запросы субъектов персональных данных и уполномоченных органов по защите прав субъектов персональных данных, действующего у Оператора.

5.4. Расследование инцидента информационной безопасности.

5.4.1. Целями расследования инцидента информационной безопасности являются:

- выработка организационных и технических решений, направленных на снижение рисков нарушения информационной безопасности, предотвращение подобных нарушений в будущем;
- обеспечение безопасности персональных данных;
- обеспечение прав субъектов персональных данных на обеспечение безопасности и конфиденциальности их персональных данных, принятых на обработку Оператором;
- предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации.

5.4.2. Оператор устанавливает следующие этапы расследования инцидента информационной безопасности:

- создание комиссии по расследованию инцидента информационной безопасности или определение лица, ответственного за проведение указанного расследования;
- определение сроков проведения расследования и пределов расследования, а также полномочий комиссии/ответственного должностного лица в рамках расследования;
- подтверждение/опровержение факта возникновения инцидента информационной безопасности;
- подтверждение/корректировка класса опасности инцидента информационной безопасности;
- уточнение дополнительных обстоятельств (деталей) инцидента информационной безопасности;
- получение (сбор) доказательств возникновения инцидента информационной безопасности, обеспечение их сохранности и целостности;
- минимизация последствий инцидента информационной безопасности;
- оформление итогов проведенного расследования путем составления акта о проведенном расследовании инцидента информационной безопасности.

5.4.3. В процессе проведения расследования информационной безопасности обязательными для установления являются:

- дата и время совершения инцидента информационной безопасности;
- ФИО, должность и структурное подразделение нарушителя информационной безопасности;
- уровень критичности инцидента информационной безопасности;
- обстоятельства и мотивы совершения инцидента информационной безопасности;
- информационные ресурсы, затронутые инцидентом информационной безопасности;
- характер и размер реального и потенциального ущерба Оператора и/или третьих лиц;
- обстоятельства, способствовавшие совершению инцидента информационной безопасности.

5.4.4. Осуществляющее расследование уполномоченное должностное лицо (или Комиссия) в процессе проведения расследования инцидента информационной безопасности при необходимости запрашивает информацию в соответствующих структурных подразделениях. Указанный запрос направляется на имя руководителя подразделения с обязательным указанием сроков предоставления информации (с учетом необходимости ее анализа, сбора и подготовки).

5.4.5. В течение 2 (двух) рабочих дней с момента назначения осуществляющего расследование должностного лица (формирования Комиссии по расследованию инцидента информационной безопасности), указанное лицо запрашивает у руководителя структурного подразделения объяснительную записку предполагаемого нарушителя информационной безопасности. Объяснительная записка должна быть составлена, подписана нарушителем информационной безопасности и представлена его непосредственным руководителем осуществляющему расследование должностному лицу в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа нарушителя информационной безопасности предоставить объяснительную записку, осуществляющему расследование должностному лицу руководителем структурного подразделения в указанный срок предоставляется акт об

отказе нарушителя информационной безопасности от дачи пояснений по существу инцидента информационной безопасности.

5.4.6. Осуществляющее расследование должностное лицо (Комиссия) проводит оценку негативных последствий инцидента информационной безопасности. В ходе данной оценки учитываются, в том числе:

- реальный ущерб для Оператора;
- потенциальный ущерб для Оператора;
- косвенные потери, связанные с недоступностью сервисов, потерей информации;
- другие виды ущерба или аспекты негативных последствий для Оператора или субъектов персональных данных.

5.4.7. С целью минимизации последствий инцидента информационной безопасности возможно временное отключение прав доступа нарушителя информационной безопасности к информационным ресурсам Оператора (в частности, информационным системам персональных данных) на время проведения расследования (блокировка Пользователя). Подобное отключение инициируется осуществляющим расследование должностным лицом с обязательным предварительным согласованием с непосредственным руководителем нарушителя информационной безопасности.

5.4.8. В случае, если у нарушителя информационной безопасности были отключены права доступа к информационным ресурсам Оператора на время проведения расследования, то по его результатам осуществляющее расследование должностное лицо по согласованию с непосредственным руководителем нарушителя информационной безопасности инициирует возвращение в полном или ограниченном объеме ранее имеющихся у нарушителя информационной безопасности прав доступа к информационным ресурсам Оператора.

5.4.9. Восстановление временно отключенных у нарушителя информационной безопасности прав доступа к информационным ресурсам Оператора (разблокировка Пользователя) может производиться только по заявке непосредственного руководителя нарушителя информационной безопасности или осуществляющего расследование должностного лица.

5.5. Оформление результатов реагирования на инцидент информационной безопасности.

5.5.1. Собранная в процессе расследования инцидента информационной безопасности информация фиксируется осуществляющим расследование должностным лицом (ответственным лицом Комиссии) в соответствующих графах журнала регистрационного учета инцидентов информационной безопасности и учитывается при составлении итогового заключения.

5.5.2. Результаты расследования оформляются лицом, осуществлявшим расследование, в виде письменного заключения с изложением причин инцидента, последствий инцидента, а также указанием лиц, виновных в нарушении информационной безопасности Оператора. Указанное заключение подписывается лицами, осуществлявшими расследование, с указанием должности и даты составления заключения.

5.5.3. Итоговое заключение по инциденту информационной безопасности осуществлявшее расследование лицо направляет Старшему системному администратору, а также руководителям структурных подразделений, затронутых инцидентом информационной безопасности.

5.5.4. По завершении расследования инцидента информационной безопасности, осуществлявшее расследование лицо передает собранные материалы и итоговое заключение (в объеме, достаточном для принятия решения) непосредственному руководителю нарушителя информационной безопасности для решения вопроса о целесообразности привлечения нарушителя информационной безопасности к дисциплинарной ответственности.

5.5.5. На основании полученных результатов расследования руководитель структурного подразделения в срок не более 7 (семь) рабочих дней организовывает проведение одного или нескольких мероприятий, направленных на снижение рисков информационной безопасности в будущем:

- анализ и пересмотр имеющихся прав доступа к информационным ресурсам Оператора нарушителя информационной безопасности;
- повторное ознакомление нарушителя информационной безопасности с локальными нормативными актами Оператора в сфере персональных данных;
- доведение до сведения всех работников структурного подразделения требований локальных нормативных актов Оператора в сфере персональных данных;
- обсуждение инцидента информационной безопасности на совещании руководителей структурного подразделения или совещании работников Оператора;
- отмена неактуальных прав доступа к информационным ресурсам Оператора;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- иные мероприятия.

5.5.6. В случае выявления в инциденте информационной безопасности признаков административного правонарушения или преступления, относящихся к информационной сфере, осуществлявшее расследование лицо передает все материалы по инциденту информационной безопасности руководителю Оператора для принятия решения о подаче соответствующего заявления в правоохранительные органы РФ.

5.5.7. В целях предупреждения возникновения инцидентов информационной безопасности в будущем, Оператор не реже раза в год проводит обучение работников всех структурных подразделений по вопросам информационной безопасности Оператора, в частности, в сфере обработки персональных данных субъектов персональных данных, и возможных мер реагирования на инциденты информационной безопасности.

6. Регламент применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн

6.1. Настоящим Регламентом применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн (далее – Регламент) определяются организационные и технические меры по обеспечению безопасности и сохранности ПДн при их обработке в автоматизированных ИСПДн, включая последовательность резервного копирования и восстановления персональных данных при их обработке в информационных системах персональных данных, применяемых Оператором.

6.2. Меры по обеспечению информационной безопасности (безопасности персональных данных).

6.2.1. 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 (далее - машинные носители персональных данных);
- 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;
- защита 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 (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

Обеспечение безопасности персональных данных достигается Оператором путем:

- определения типа угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- применения 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 нормативно-правовыми актами уровни защищенности персональных данных;

- применения прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- организации учета, хранения и обращения носителей персональных данных;

- обнаружения фактов несанкционированного доступа к персональным данным и принятие мер, в том числе: применение в необходимых случаях средств межсетевого экранирования, обнаружения вторжений, анализа защищенности и средств криптографической защиты информации;

- восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- установления правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

- организации пропускного режима на территорию Оператора, охрана помещений с помощью техническими средствами обработки персональных данных;

- контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

6.2.2. В целях обеспечения информационной безопасности (безопасности персональных данных) при обработке персональных данных субъектов персональных данных в информационных системах, применяемых Оператором, Оператор путем издания распорядительного акта определяет уровень защищенности персональных данных, в соответствии с Постановлением Правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

6.2.3. Для обеспечения уровней защищенности персональных данных Оператором принимаются следующие меры:

6.2.3.1. Для обеспечения Четвертого уровня защищенности:

а) организация режима обеспечения безопасности помещений, в которых размещена информационные системы, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем Оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения

безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

6.2.3.2. Для обеспечения Третьего уровня защищенности Оператором, помимо требований, установленных в п.6.2.3.1. настоящего Регламента, назначается уполномоченное должностное лицо, ответственное за обеспечение безопасности персональных данных в информационных системах (Куратор ОПД).

6.2.3.3. Для обеспечения Второго уровня защищенности, помимо требований, установленных в п.6.2.3.1. и п.6.2.3.2. настоящего Регламента, Оператором осуществляется контроль доступа к содержанию электронного журнала сообщений с тем, чтобы указанный доступ был возможен исключительно для должностных лиц Оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения трудовых обязанностей.

6.2.3.4. Для обеспечения Первого уровня защищенности, помимо требований, установленных в п.п.6.2.3.1.-6.2.3.3. настоящего Регламента, Оператором осуществляются следующие действия:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий работника Оператора по доступу к персональным данным, содержащимся в информационных системах;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационных системах, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

6.2.4. Состав и конкретное содержание иных организационных и технических мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, определяется в соответствии с Приказом ФСТЭК от 18 февраля 2013 г. № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

6.2.5. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

6.2.6. В целях исполнения требований п.6.2.3, 6.2.4 настоящего Регламента, Оператор возлагает ответственность за обеспечение информационной безопасности Оператора на Куратора ОПД.

6.3. Правила записи и хранения персональных данных в электронном виде.

6.3.1. Для записи и хранения ПДн, включая биометрические ПДн, в электронном виде используются следующие материальные носители: облачное хранилище.

6.3.2. Материальный носитель должен обеспечивать:

а) защиту от несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы персональных данных;

б) возможность доступа к записанным на материальный носитель биометрическим персональным данным, осуществляемого оператором и лицами, уполномоченными в соответствии с законодательством Российской Федерации на работу с биометрическими персональными данными (далее - уполномоченные лица);

в) возможность идентификации информационной системы персональных данных, в которую была осуществлена запись биометрических персональных данных, а также оператора, осуществившего такую запись;

г) невозможность несанкционированного доступа к биометрическим персональным данным, содержащимся на материальном носителе.

Материальный носитель должен использоваться в течение максимального срока 3 лет, но не более срока эксплуатации, установленного изготовителем материального носителя.

6.3.3. Материальные носители выдаются уполномоченным лицам Куратором ОПД под роспись в Журнале учета выдачи материальных носителей ПДн.

6.3.4. Куратор ОПД обязан:

- а) осуществлять учет количества экземпляров материальных носителей;
- б) осуществлять присвоение материальному носителю уникального идентификационного номера, позволяющего точно определить оператора, осуществившего запись биометрических персональных данных на материальный носитель;
- в) осуществлять контроль за раздельным хранением (на разных материальных носителях) информации об обучающихся и информации о персонале Оператора.

6.3.5. Технологии хранения биометрических персональных данных вне информационных систем персональных данных должны обеспечивать:

- а) доступ к информации, содержащейся на материальном носителе, для уполномоченных лиц;
- б) применение средств электронной подписи или иных информационных технологий, позволяющих сохранить целостность и неизменность биометрических персональных данных, записанных на материальный носитель;
- в) проверку наличия письменного согласия субъекта персональных данных на обработку его биометрических персональных данных или наличия иных оснований обработки персональных данных, установленных законодательством Российской Федерации в сфере отношений, связанных с обработкой персональных данных.

6.3.6. В случае если на материальном носителе содержится дополнительная информация, имеющая отношение к записанным биометрическим персональным данным, то такая информация должна быть подписана усиленной квалифицированной электронной подписью и (или) защищена иными информационными технологиями, позволяющими сохранить целостность и неизменность информации, записанной на материальный носитель.

6.3.7. Использование шифровальных (криптографических) средств защиты информации осуществляется в соответствии с законодательством Российской Федерации.

6.3.8. При хранении биометрических персональных данных вне информационных систем персональных данных должна обеспечиваться регистрация фактов несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы персональных данных.

6.4. Уничтожение ПДн в ИСПДн.

6.4.1. Уничтожение ПДн по истечении срока их хранения производится путем удаления соответствующих записей и объектов в электронных базах данных.

6.4.2. Решение об удалении ПДн принимается по представлению Куратора ОПД образованной по приказу руководителя Организации комиссией. В решении указывается исполнитель.

6.4.3. Контроль за исполнением решения об удалении ПДн осуществляют Куратор ОПд.

6.5. Правила осуществления резервного копирования персональных данных.

6.5.1. Резервному копированию подлежат персональные данные, указанные Оператором в п.1.4.-1.5. Регламента обработки персональных данных.

6.5.2. Резервное копирование персональных данных производится субъектом резервного копирования при получении персональных данных на обработку через информационные системы персональных данных, применяемые Оператором.

6.5.3. Порядок резервного копирования разрабатывается и утверждается должностным лицом соответствующего подразделения Оператора с учетом особенностей информационных систем персональных данных, применяемых Оператором.

6.5.4. В порядок резервного копирования персональных данных должны быть включены следующие сведения:

- описание системы резервного копирования, то есть наименования, версии, настройки оборудования и программного обеспечения;

- сведения о периодичности копирования персональных данных, времени хранения резервных копий, смене носителей персональных данных;
- информация о периодичности и порядке осуществления технического сопровождения системы резервного копирования;
- описание последовательности действий по осуществлению копирования персональных данных и по восстановлению персональных данных с резервных копий;
- информация об осуществлении тестирования резервных копий;
- иная информация, необходимая для осуществления резервного копирования персональных данных, принятых на обработку Оператором.

6.5.5. При осуществлении резервного копирования персональных данных соответствующим субъектом резервного копирования может быть использована следующая последовательность действий:

- получение персональных данных субъектов персональных данных через информационную систему персональных данных;
- регистрация субъекта персональных данных в журнале учета субъектов персональных данных;
- учет персональных данных субъекта персональных данных в соответствующем реестре;
- создание плана резервного копирования персональных данных;
- создание резервной копии записи реестра и сохранение ее на носителе персональных данных;
- учет созданной резервной копии в журнале резервных копий.

6.5.6. В целях осуществления резервного копирования уполномоченное должностное лицо соответствующего подразделения Оператора:

6.5.6.1. Осуществляет настройку системы резервного копирования в зависимости от характера и объема персональных данных, подлежащих резервному копированию;

6.5.6.2. Вводит в эксплуатацию систему резервного копирования;

6.5.6.3. Осуществляет техническое сопровождение системы резервного копирования, что включает в себя:

- мониторинг системы резервного копирования;
- проведение ремонтных работ АРМ Пользователей информационных систем персональных данных;
- формирование реестра резервных копий и контроль за ведением реестра субъектами резервного копирования;
- формирование и ведение журнала резервных копий;
- внесение изменений в настройки системы резервного копирования в соответствии с данными журнала резервных копий;
- обеспечение по истечении срока хранения резервной копии на носителе персональных данных уничтожения данной резервной копии и записи новой резервной копии на указанном носителе персональных данных, с осуществлением предварительной проверки его исправности;
- в случае неисправности носителя персональных данных такой носитель должен быть заменен новым исправным носителем персональных данных, а неисправный - уничтожен без возможности восстановления персональных данных, записанных на нем;
- восстановление персональных данных с резервных копий в случае утраты указанных персональных данных;
- осуществление контроля за хранением резервных копий таким образом, чтобы резервные копии хранились в изолированном от места нахождения системы резервного копирования помещении.

6.6. Правила осуществления хранения резервных копий персональных данных.

6.6.1. Резервные копии персональных данных подлежат хранению в реестрах информационных систем персональных данных, применяемых Оператором, а также на носителях персональных данных.

6.6.2. Резервные копии персональных данных хранятся в течение срока,

установленного в порядке резервного копирования, разработанного уполномоченным должностным лицом соответствующего подразделения Оператора с учетом требований действующего законодательства РФ. В случае отсутствия в соответствующих нормативно-правовых актах сроков хранения отдельных видов персональных данных, указанные персональные данные подлежат хранению в течение срока, указанного в письменном согласии на обработку персональных данных соответствующего субъекта персональных данных.

6.6.2. Хранение резервных копий персональных данных, цели обработки которых различны, должно осуществляться раздельно в рамках информационных систем персональных данных, применяемых Оператором, или, при условии хранения на носителях персональных данных, на различных носителях персональных данных.

6.6.3. Пользователь информационных систем персональных данных, обеспечивает хранение информации, содержащей персональные данные субъектов персональных данных, исключающее доступ к ним третьих лиц.

6.6.4. Все носители персональных данных подлежат обязательному учету в журнале учета носителей персональных данных, согласно положениям Регламента по учету и хранению носителей персональных данных, применяемого Оператором.

6.6.5. Неисправные носители персональных данных подлежат немедленной утилизации с занесением соответствующей информации в журнал учета носителей персональных данных. Носители с истекшим сроком хранения подлежат проверке на исправность уполномоченным должностным лицом соответствующего подразделения Оператора. В случае исправности носителя, персональные данные на носителе подлежат обновлению (перезаписи) на персональные данные, срок хранения которых не истек.

6.7. Правила осуществления восстановления персональных данных с резервных копий.

6.7.1. В случае утраты персональных данных уполномоченными должностными лицами Оператора (в связи с внештатной ситуацией в информационной системе персональных данных, уничтожением носителя персональных данных, нарушением правил хранения персональных данных, в иных случаях, при которых дальнейшая обработка персональных данных субъектов персональных данных невозможна), персональные данные подлежат восстановлению посредством использования резервных копий персональных данных.

6.7.2. Порядок восстановления персональных данных с резервных копий устанавливается уполномоченным должностным лицом соответствующего подразделения Оператора. Указанный порядок не может исключать следующих стадий:

- фиксирование причины восстановления персональных данных с резервных копий в соответствующем журнале учета резервных копий персональных данных;
- восстановление персональных данных с использованием сведений реестра информационных систем персональных данных, применяемых Оператором либо носителей персональных данных;
- создание резервной копии восстановленных персональных данных согласно плану резервного копирования, действующему у Оператора.

6.7.3. При восстановлении персональных данных с резервных копий Пользователь информационных систем персональных данных обязан соблюдать положения Инструкции пользователя ИСПДн, Положения по обработке персональных данных и иных локальных нормативных актов, действующих у Оператора, и регламентирующих порядок обработки персональных данных субъектов персональных данных.

7. Регламент применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации.

7.1. Настоящий Регламент применяется при такой обработке ПДн, когда такие действия, как их использование, уточнение, распространение, уничтожение персональных

данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека, в частности, при ведении в бумажном виде личных дел работников и личных дел обучающихся.

7.2. ПДн при их обработке, осуществляющейся без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).

7.3. При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы (ПДн работников Оператора и ПДн обучающихся). Для обработки различных категорий персональных данных, осуществляющейся без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

7.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляющейся без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляющуюся без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

7.5. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска Субъекта персональных данных на территорию, на которой находится Оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом Оператора, содержащим сведения о цели обработки персональных данных, осуществляющейся без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого Субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска Субъекта персональных данных на территорию, на которой находится оператор.

7.6. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

7.7. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Уничтожение ПДн по истечении срока их хранения производится комиссией, формируемой приказом руководителя Оператора.

7.7. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

7.8. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

7.9. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

7.10. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ, предусмотренные настоящим Регламентом (пропускной режим, установление перечня лиц, допущенных к обработке ПДн, контроль за исполнением локальных нормативных актов).

7.11. Осуществление внутреннего контроля соответствия обработки персональных данных настоящему Федеральному закону "О персональных данных" и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Оператора в отношении обработки персональных данных, локальным актам Оператора возлагается на Куратора ОПД.

Приложение №2
к приказу Генерального директора
ООО «ЕГЭ-Центр»
№2/4 от «20» июля 2016 г.

Перечень лиц, допущенных к обработке персональных данных

1. Куратор ОПД – Генеральный директор Капралов К.А.
 2. Лица, допущенные к обработке персональных данных:

ЛИСТ ОЗНАКОМЛЕНИЯ

РАБОТНИКОВ ОOO «ЕГЭ-Центр» с РЕГЛАМЕНТОМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ
ДАННЫХ, ПЕРЕЧНЕМ ЛИЦ, ДОПУЩЕННЫХ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

С ДОКУМЕНТАМИ ОЗНАКОМЛЕНЫ: