

Федеральное медико-биологическое агентство
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«ФЕДЕРАЛЬНЫЙ НАУЧНО-КЛИНИЧЕСКИЙ ЦЕНТР
ИНФЕКЦИОННЫХ БОЛЕЗНЕЙ
ФЕДЕРАЛЬНОГО МЕДИКО-БИОЛОГИЧЕСКОГО АГЕНТСТВА»
(ФГБУ ФНКЦИБ ФМБА России)

«УТВЕРЖДАЮ»

Генеральный директор


 В.А.Ратников

«10» марта 2026 г.

ПОЛОЖЕНИЕ
по организации и порядку проведения работ по обеспечению безопасности
персональных данных при их обработке в информационных системах
ФГБУ ФНКЦИБ ФМБА России

ЛИСТ СОГЛАСОВАНИЯ
к Положению по организации и порядку проведения работ по обеспечению
безопасности персональных данных при их обработке в информационных системах
ФГБУ ФНКЦИБ ФМБА России

Директор по развитию



В.С. Глебов

Начальник управления
цифровой трансформации
и инновационных цифровых
технологий



В.А. Забаев

Разработчик:

В.В. Воронов
Начальник отдела защиты информации
и информационных технологий

1. Термины и определения

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

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.

Обезличивание персональные данные – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту 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.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

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.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному назначению и техническим характеристикам.

2. Общие положения

2.1. Настоящее Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Семейным кодексом Российской Федерации, Федеральным законом от 01 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете и системе обязательного пенсионного страхования», Федеральным законом от 29 декабря 2006 г. № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством», Федеральным законом от 29 ноября 2010 г. № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», Федеральным законом от 31 июля 1998 г. №146-ФЗ «Налоговый кодекс РФ. Часть первая» (ст. 24), Федеральным законом от 15 декабря 2001 г. №167 «Об обязательном пенсионном страховании РФ» (ст. 14), Федеральным законом от 17 декабря 2001 г. №173-ФЗ «О трудовых пенсиях в Российской Федерации», Федеральным законом от 15 декабря 2001 г. №166-ФЗ «О государственном пенсионном обеспечении в Российской Федерации», Федеральным законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Постановлением Правительства РФ от 5 мая 2018 г. № 555 «О единой государственной информационной системе в сфере здравоохранения»,

Приказом Минздрава России от 28 октября 2022 г. № 708н № «Об утверждении порядка ведения персонализированного учета лиц, участвующих в осуществлении медицинской деятельности и фармацевтической деятельности, лиц, обучающихся по образовательным программам среднего профессионального и высшего медицинского образования, образовательным программам среднего профессионального и высшего фармацевтического образования», Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции», Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», приказом ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», и другими нормативными правовыми актами Российской Федерации, регулируемыми отношения, связанные с обработкой персональных данных и определяет порядок организации и проведения работ по обеспечению безопасности персональных данных в Федеральном государственном бюджетном учреждении «Федеральный научно-клинический центр инфекционных болезней Федерального медико-биологического агентства».

2.2. Федеральное государственное бюджетное учреждение «Федеральный научно-клинический центр инфекционных болезней Федерального медико-биологического агентства» является оператором, самостоятельно организующим и осуществляющим обработку персональных данных субъектов персональных данных (далее - персональные данные), а также определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.3. Настоящим Положением определяется порядок получения, обработки, хранения, передачи и любого другого использования персональных данных в Федеральном государственном бюджетном учреждении «Федеральный научно-клинический центр инфекционных болезней Федерального медико-биологического агентства»¹ с использованием средств автоматизации или без использования таких средств.

2.4. Все работники Оператора должны быть ознакомлены под роспись с настоящим положением и изменениями к нему.

2.5. Методическое руководство и контроль за соблюдением требований по обработке персональных данных, контроль за соблюдением прав и свобод субъектов персональных данных возлагается на должностное лицо Оператора, назначенное ответственным за организацию обработки персональных данных.

3. Принципы обработки персональных данных

3.1. Обработка персональных данных осуществляется на основе следующих 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 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;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.
- обеспечения точности персональных данных, их достаточности, актуальность по отношению к целям обработки персональных данных;
- осуществления хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных.

3.2. Запрещается получать, обрабатывать и приобщать к совокупности персональных данных субъекта персональных данных не установленные федеральными законами

¹ Далее – Оператор.

персональные данные о его политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах.

3.3. При принятии решений, затрагивающих интересы субъекта персональных данных, запрещается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей.

3.4. Защита персональных данных от неправомерного их использования или утраты обеспечивается за счет средств Оператора. Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в информационной системе оценивается при проведении государственного контроля и надзора, и периодического внутреннего контроля.

4. Состав и субъекты персональных данных

4.1. К субъектам персональных данных, чьи сведения обрабатываются Оператором, относятся:

- граждане, состоящие (состоявшие) в трудовых отношениях с Оператором (далее – сотрудники Оператора);
- граждане, претендующие на замещение вакантных должностей Оператора, граждане, с которыми заключаются договоры на оказание услуг (выполнение работ);
- члены семей сотрудников Оператора;
- граждане, получающие медицинскую помощь, подвергающиеся медицинскому наблюдению и/или лечению по поводу какого-либо заболевания, патологического состояния или иного нарушения здоровья и жизнедеятельности, а также пользующиеся медицинскими услугами независимо от наличия у них заболевания (далее – действительные пациенты);
- граждане, претендующие на получение медицинской помощи или лечения по поводу какого-либо заболевания у Оператора (далее – потенциальные пациенты);
- представители (в силу закона и по доверенности) действительных и потенциальных пациентов Оператора;
- члены семей и иные родственники действительных и потенциальных пациентов Оператора;
- посетители помещений, зданий и территории Оператора;
- сотрудники и представители сторонних медицинских организаций;

– лица, участвующие в гражданском, арбитражном, уголовном, административном процессах и исполнительном производстве (участником которых является Оператор).

– Обучающиеся.

4.2. Перечень персональных данных, обрабатываемых у Оператора, определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами Оператора с учетом целей обработки персональных данных. Состав персональных данных, обрабатываемых у Оператора, определяется в «Перечне персональных данных».

4.3. Обработка персональных данных работников Оператора, физических лиц, претендующих на замещение вакантных должностей Оператора, физических лиц, с которыми заключены гражданско-правовые договоры, лица, участвующие в гражданском, арбитражном, уголовном, административном процессах и исполнительном производстве (участником которых является Оператор) осуществляется в целях:

– обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации;

– осуществления функций, полномочий и обязанностей, возложенных на Оператора законодательством Российской Федерации, в том числе по предоставлению персональных данных в органы государственной власти;

– ведения кадрового учета, учёта сведений о доходах сотрудников Оператора и начисления им заработной платы;

– выполнения требований законодательства в сфере труда и налогообложения;

– ведения текущего бухгалтерского и налогового учёта, формирование, изготовление и своевременная подача бухгалтерской, налоговой и статистической отчётности;

– реализации прав на социальные гарантии уволенных работников и реализация их прав на судебную защиту, получение информации о периодах работы и (или) иной деятельности для подтверждения страхового стажа, соблюдение социальных гарантий уволенных пенсионеров (ежегодное предоставление социальных выплат);

– подбора кандидатов на имеющиеся вакантные должности;

– осуществления прав и законных интересов Оператора в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Оператора;

– выполнения требований Федерального закона от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции»;

- обеспечения работникам Оператора установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, учета результатов исполнения им должностных обязанностей;
- оформления банковских карт работникам, начисление заработной платы и иных выплат;
- формирования материалов для внутреннего информационного обеспечения деятельности Оператора, его отделений;
- исполнения судебных актов, актов других органов или должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации;
- защиты интересов Оператора в судебных спорах;
- поддержания контактов с субъектом персональных данных или его законными представителями;
- соблюдения правовых интересов Оператора во взаимоотношениях с контрагентами при заключении, изменении и расторжении договоров, а также исполнение гражданско-правовых договоров;
- формирования и обработка расчетных документов для частных лиц и организаций, заключивших договоры с Оператором;
- обеспечения прохождения медицинских осмотров работниками;
- исполнения иных полномочий, возложенных на Оператора.

4.4. Обработка персональных данных членов семьи работника, осуществляется в целях:

- обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации;
- осуществления функций, полномочий и обязанностей, возложенных на Оператора законодательством Российской Федерации, в том числе по предоставлению персональных данных в органы государственной власти;
- реализации прав на социальные гарантии уволенных работников и реализация их прав на судебную защиту, получение информации о периодах работы и (или) иной деятельности для подтверждения страхового стажа, соблюдение социальных гарантий уволенных пенсионеров (ежегодное предоставление социальных выплат);
- осуществления прав и законных интересов Оператора в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Оператора;

- выполнения требований Федерального закона от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции»;
- обеспечения работникам Оператора установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, учета результатов исполнения им должностных обязанностей;
- формирования материалов для внутреннего информационного обеспечения деятельности Оператора, его отделений;
- исполнения судебных актов, актов других органов или должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации;
- защиты интересов Оператора в судебных спорах;
- поддержания контактов с субъектом персональных данных или его законными представителями;
- соблюдения правовых интересов Оператора во взаимоотношениях с контрагентами при заключении, изменении и расторжении договоров, а также исполнение гражданско-правовых договоров;
- исполнения иных полномочий, возложенных на Оператора.

4.5. Обработка персональных данных физических лиц, обучающихся у Оператора, осуществляется в целях:

- осуществления прав и законных интересов Оператора в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Оператора;
- обеспечение соблюдения законодательства Российской Федерации в сфере образования;
- исполнение функций научно-исследовательского учреждения, и образовательной организации;
- осуществление научной, литературной или иной творческой деятельности;
- исполнения иных полномочий, возложенных на Оператора.

4.6. Обработка персональных данных действительных, потенциальных пациентов, их представителей (в силу закона и по доверенности), а также членов их семей и/или иных родственников, осуществляется в целях:

- осуществления прав и законных интересов Оператора в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Оператора;

- оказания первичной медико-санитарной помощи, специализированной, и/или высокотехнологичной медицинской помощи;
- оказания скорой, в том числе скорой специализированной, медицинской помощи (включая медицинскую эвакуацию);
- проведения диспансеризации и периодических медицинских осмотров;
- проведения экспертизы профессиональной пригодности (связи заболевания с профессией);
- проведения периодических психофизиологических обследований;
- осуществления судебно-медицинской экспертизы;
- осуществления заготовки, хранения, транспортировки и обеспечения безопасности донорской крови и ее компонентов;
- проведения прикладных научных, клинических и прикладных исследований
- заключения и исполнения договоров на оказание медицинских услуг;
- подготовки платежных документов по договору оказания медицинских услуг;
- исполнения иных полномочий, возложенных на Оператора.

4.7. Обработка персональных данных посетителей помещений, зданий и территории Оператора, сотрудников и представителей сторонних медицинских организаций, осуществляется в целях:

- осуществления прав и законных интересов Оператора в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Оператора;
- организации пропускного и внутриобъектового режимов на территории Оператора;
- обеспечения сохранности, имущества Оператора;
- исполнения иных полномочий, возложенных на Оператора.

4.8. Обработка персональных данных физических лиц, обратившихся к Оператору, осуществляется в целях:

- реализации прав и законных интересов Оператора в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Оператора;
- исполнения иных полномочий, возложенных на Оператора.

5. Порядок обработки персональных данных

5.1. Получение персональных данных

5.1.1. Обработка персональных данных субъектов персональных данных, указанных в п. 4.1 настоящего Положения, осуществляется следующими структурными подразделениями Оператора:

- Штаб по делам ГО, ЧС и мобилизационной подготовке;
- Служба охраны труда и пожарной безопасности;
- Отдел кадров;
- Юридический отдел;
- Бухгалтерия;
- Планово-экономический отдел;
- Управление материально-технического обеспечения;
- Управление делами;
- Управление цифровой трансформации и инновационных цифровых технологий;
- Информационно-аналитическое управление;
- Управление организационно-методической и образовательной деятельности;
- НИО по организации и сопровождению научно-исследовательских работ;
- Приемное отделение;
- Дифференциально-диагностическое отделение для детей (1 отделение);
- Детское нейрореабилитационное отделение (2 отделение);
- Отделение кишечных инфекций (3 отделение);
- Отделение респираторных (капельных) инфекций (4 отделение);
- Детское психоневрологическое отделение (5 отделение);
- Отделение реанимации и интенсивной терапии (6 отделение);
- Дневной стационар (7 отделение);
- 8-е реабилитационное отделение;
- Дифференциально-диагностическое отделение для взрослых (9 отделение);
- Отдел контроля качества и безопасности медицинской деятельности);
- Отдел делопроизводства и документационного обеспечения;
- Аптека;
- Отделение трансфузиологии;
- Кабинет экстракорпоральной гемокоррекции и фототерапии;
- Клинико-диагностическая лаборатория;
- Лаборатория патоморфологии;

- Эндоскопический кабинет;
- Отделение ультразвуковой диагностики;
- Отделение функциональной диагностики;
- Рентгеновское отделение;
- Отдел развития продаж и клиентского сервиса;
- Консультационно-диагностический центр;
- организационно-методический отдел;
- Эпидемиолог.

5.1.2. Обработка персональных данных субъектов персональных данных включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

5.1.3. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от субъектов персональных данных либо их законных представителей.

5.1.4. Уполномоченные работники отдела кадров Оператора получают сведения о персональных данных работников и граждан, претендующих на замещение вакантных должностей, из следующих документов:

- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка и/или документы, подтверждающие трудовой стаж;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о присвоении ИНН (при его наличии);
- документы воинского учета - для военнообязанных и лиц, подлежащих воинскому учету;
- документ об образовании, о квалификации или наличии специальных знаний;
- анкета, заполняемая при приеме на работу;
- санитарная книжка; медицинская справка о прохождении медицинского осмотра;
- справка о доходах, расходах, имуществе и обязательствах имущественного характера супруги (супруга) и несовершеннолетних детей;
- свидетельство о государственной регистрации актов гражданского состояния;
- иные документы и сведения, предоставляемые субъектом персональных данных при приеме на работу, а также в процессе трудовой деятельности.

5.1.5. Уполномоченные работники образовательного отдела получают сведения о персональных данных физических лиц, проходящих практику у Оператора и физических лиц, обучающихся у Оператора по целевым договорам, из следующих документов:

- паспорт или иной документ, удостоверяющий личность;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о присвоении ИНН (при его наличии);
- документы воинского учета - для военнообязанных и лиц, подлежащих воинскому учету;
- документ об образовании, о квалификации или наличии специальных знаний;
- иные документы и сведения, предоставляемые субъектом персональных данных при приеме на обучение, а также предоставленные им в процессе обучения.

5.1.6. Уполномоченные работники управления по безопасности получают сведения о персональных данных посетителей помещений, зданий и территории Оператора, и сотрудников сторонних организаций, располагающихся на территории Оператора:

- паспорт или иной документ, удостоверяющий личность.

5.1.7. При оформлении работника к Оператору уполномоченным работником заполняется унифицированная форма Т-2 «Личная карточка», в которой отражаются следующие анкетные и биографические данные работника:

- общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, знание иностранного языка, образование, профессия, ученая степень, стаж работы, состояние в браке, состав семьи, паспортные данные, адрес места жительства, номер телефона);
- сведения о воинском учете;
- данные о приеме на работу;

5.1.8. В дальнейшем в личную карточку вносятся:

- сведения о переводах на другую работу;
- сведения об аттестации;
- сведения о повышении квалификации;
- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- сведения о социальных льготах.

5.1.9. Субъект персональных данных обязан представлять Оператору достоверные сведения о себе. Оператор имеет право проверять достоверность указанных сведений

в порядке, не противоречащим законодательству РФ. Субъект персональных данных обязан своевременно, в срок, не превышающий одного месяца, сообщать Оператору об изменении своих персональных данных.

5.1.10. При сборе персональных данных уполномоченный работник, осуществляющий сбор (получение) персональных данных непосредственно от субъекта персональных данных, обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

5.1.11. Если в соответствии с федеральным законом предоставление персональных данных и (или) получение Оператором согласия на обработку персональных данных являются обязательными, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку.

5.1.12. Работник, принимающий от субъекта документальные сведения, содержащие персональные данные, проверяет их достаточность и полноту, а также правильность их заполнения.

5.1.13. В случае возникновения необходимости получения персональных данных субъекта персональных данных у третьей стороны следует известить об этом субъекта персональных данных заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных.

5.1.14. Запрещается получать, обрабатывать и приобщать к документам субъекта персональных данных персональные данные касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни без его согласия.

5.2. Обработка и хранение персональных данных

5.2.1. Обработка персональных данных субъектов персональных данных, указанных в п. 4.1 настоящего Положения, может осуществляться без согласия указанных лиц в рамках целей, определенных пунктом 4.3 настоящего Положения, в соответствии с пунктом 2 части 1 статьи 6 и частью 2 статьи 11 Федерального закона «О персональных данных», Федерального закона «О противодействии коррупции», Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Административным кодексом Российской Федерации.

5.2.2. Обработка специальных категорий персональных данных субъектов персональных данных, может осуществляться без согласия указанных лиц в рамках целей, определенных пунктом 4.3 настоящего Положения, в соответствии с подпунктом 2.3 пункта 2 части 2 статьи 10 Федерального закона «О персональных данных» и

положениями Трудового кодекса Российской Федерации, за исключением случаев получения персональных данных работника Оператора у третьей стороны.

5.2.3. Обработка персональных данных субъектов персональных данных, осуществляется при условии получения согласия указанных лиц в следующих случаях:

- при передаче (распространении, предоставлении) персональных данных третьим лицам в случаях, не предусмотренных действующим законодательством Российской Федерации;
- при трансграничной передаче персональных данных;
- при принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

5.2.4. В случаях, предусмотренных пунктом 5.2.3 настоящего Положения, согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных» (Приложение № 1).

5.2.5. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов персональных данных, осуществляется путем:

- получения оригиналов необходимых документов (заявление, трудовая книжка, автобиография, иные документы, предоставляемые Оператором);
- копирования оригиналов документов;
- внесения сведений в учетные формы (на бумажных и электронных носителях);
- формирования набора персональных данных в ходе работы (анкетирование, осмотр пациентов);
- внесения персональных данных в информационные системы Оператора.

5.2.6. Документы, содержащие персональные данные работника Оператора составляют его личное дело. Личное дело ведется на протяжении всей его трудовой деятельности. Изменения, вносимые в личное дело, подтверждаются соответствующими документами.

5.2.7. В личное дело работника вносятся его персональные данные и иные сведения, связанные с поступлением на работу, ее прохождением и увольнением с работы и необходимые для обеспечения деятельности Оператора.

5.2.8. Персональные данные, внесенные в личные дела работников, иные сведения, содержащиеся в личных делах, относятся к сведениям конфиденциального характера (за исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации). К личному делу

приобщаются документы, предусмотренные федеральными законами и иными нормативными правовыми актами Российской Федерации.

5.2.9. У Оператора создаются и хранятся следующие группы документов, содержащих персональные данные работников в единичном или сводном виде:

- документы, содержащие персональные данные работников (комплект документов, сопровождающих процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплект материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; дела, содержащие материалы по аттестации работников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Оператора, руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения);

- внутренняя документация Оператора, работе структурных подразделений и отделов (положения, должностные инструкции, распоряжения);

- документы по планированию, учету, анализу и отчетности в части работы с персоналом Оператора.

5.2.10. У Оператора создаются и хранятся следующие группы документов, содержащие персональные данные граждан, обрабатываемые в целях, предусмотренных пунктом 4.5 в единичном или сводном виде:

- документы, содержащие персональные данные обучающегося (комплект документов, сопровождающих процесс оформления договора на предоставление образовательных услуг);

- документы по организации процесса обучения (журналы успеваемости, посещения занятий и пр.);

- документы, получаемые в процессе и в результате обучения (дипломы, справки, курсовые, научные и исследовательские работы).

5.2.11. У Оператора создаются и хранятся следующие группы документов, содержащие персональные данные граждан, обрабатываемые в целях, предусмотренных пунктом 4.6 в единичном или сводном виде:

- комплект документов, содержащий персональные данные пациентов.

5.2.12. У Оператора создаются и хранятся следующие группы документов, содержащие персональные данные граждан, обрабатываемые в целях, предусмотренных пунктами 4.7 и 4.8 в единичном или сводном виде:

– документы, получаемые в процессе организации пропускного режима на территорию Оператора (постоянные, временные и разовые пропуска, журнал учёта посетителей и пр.).

5.2.13. Для хранения персональных данных на бумажных и электронных носителях используются специально оборудованные шкафы или сейфы, которые запираются на ключ. Ключ от шкафов и сейфов, в которых хранятся персональные данные, находится у уполномоченного лица.

5.2.14. Персональные данные субъектов персональных данных могут проходить дальнейшую обработку и передаваться на хранение в электронном виде - локальной компьютерной сети и компьютерной программе (информационной системе).

5.2.15. При обработке персональных данных руководитель Оператора вправе определять способы обработки, документирования, хранения и защиты персональных данных на базе современных информационных технологий.

5.2.16. В обязанности работников Оператора, осуществляющих обработку персональных данных, входит:

- обеспечение сохранности документов, содержащих персональные данные;
- обеспечение конфиденциальности персональных данных, в соответствии с федеральными законами, иными нормативными правовыми актами Российской Федерации, а также в соответствии с настоящим Положением.

5.2.17. Сроки обработки и хранения персональных данных субъектов персональных данных, определяются в соответствии с законодательством Российской Федерации и Приказом Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения».

5.2.18. Персональные данные работников Оператора, в том числе родственников работника, используются в течение трудовой деятельности в соответствии с трудовым договором, а также на протяжении установленного законодательством срока хранения личного дела в архиве (75 лет).

5.2.19. Срок обработки и хранения персональных данных, внесенных в информационные системы Оператора, должен соответствовать сроку хранения бумажных оригиналов.

5.3. Доступ к персональным данным

5.3.1. Круг лиц, допущенных к работе (получению, обработке, передаче и хранению персональных данных субъекта) с документами, содержащими персональные данные

субъектов персональных данных, определяется руководителем Оператора. Уполномоченные лица имеют право получать только те персональные данные, которые необходимы для выполнения конкретных заранее определенных функций.

5.3.2. Процедура оформления доступа работника к персональным данным включает в себя:

- ознакомление работника под роспись с внутренними документами, содержащими требования по обработке и обеспечению безопасности персональных данных в части, касающейся их должностных обязанностей.

- истребование с работника письменного обязательства о соблюдении режима конфиденциальности персональных данных, подготовленного по установленной форме (Приложение № 2). Данное обязательство хранится в личном деле работника.

5.3.3. Разрешительная система доступа пользователей к информационным ресурсам оформляется лицом, ответственным за обеспечение безопасности персональных данных, в виде матриц доступа, утверждаемых руководителем Оператора, и реализуется с помощью средств защиты от несанкционированного доступа, стандартных средств операционной системы и ролевой модели доступа информационных систем. Разрешительная система доступа отражает полномочия пользователей по выполнению конкретных действий в отношении информационных ресурсов информационной системы (чтение, запись, корректировка, удаление).

5.3.4. Внешний доступ со стороны третьих лиц к персональным данным субъектов персональных данных осуществляется с его письменного согласия, за исключением случаев, когда такой доступ необходим в целях предупреждения угрозы жизни и здоровью работника или других лиц, и иных случаев, установленных законодательством.

5.4. Передача персональных данных

5.4.1. Передача (распространение, предоставление) и использование персональных данных субъектов персональных данных осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

5.4.2. При передаче персональных данных запрещается:

- сообщать персональные данные субъекта персональных данных третьей стороне 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 других случаях, предусмотренных федеральными законами;

- сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия.

5.4.3. При возникновении необходимости передачи персональных данных уполномоченные работники предупреждают лиц, получающих персональные данные субъекта персональных данных, 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 субъекта персональных данных, обязаны соблюдать режим конфиденциальности таких данных.

5.4.4. Передача персональных данных субъекта персональных данных представителям субъекта персональных данных осуществляется в порядке, установленном федеральными законами. Передаваемая информация ограничивается только теми персональными данными субъекта персональных данных, которые необходимы для выполнения указанными представителями их функций.

5.4.5. Передача и предоставление персональных данных законным пользователям осуществляется способом, не допускающим возможность несанкционированного доступа к ним посторонних лиц.

5.4.6. Запрещается предоставлять персональные данные субъекта персональных данных лицам, не уполномоченным федеральным законом на получение персональных данных, либо при отсутствии письменного согласия субъекта персональных данных на предоставление его персональных данных. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных.

5.4.7. Передача персональных данных субъекта третьим лицам осуществляется только с письменного согласия субъекта, которое оформляется по установленной форме (Приложение № 3). Согласие субъекта на передачу его персональных данных третьим лицам не требуется в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта; когда согласие субъекта на передачу его персональных данных третьим лицам получено от него в письменном виде при заключении договора с Оператором; когда третьи лица оказывают услуги Оператору на основании заключенных договоров, а также в случаях, установленных федеральным законом и настоящим Положением.

5.4.8. Работники, передающие персональные данные субъектов третьим лицам, должны передавать их с обязательным составлением акта приема-передачи документов (иных материальных носителей), содержащих персональные данные субъектов. Передача документов (иных материальных носителей), содержащих персональные данные субъектов, осуществляется при наличии у лица, уполномоченного на их получение:

- договора на оказание услуг Оператору;

- соглашения о неразглашении конфиденциальной информации либо наличие в договоре с третьим лицом пунктов о неразглашении конфиденциальной информации, в том числе, предусматривающих защиту персональных данных субъекта;

- письма-запроса от третьего лица, которое должно включать в себя основания необходимости получения доступа к запрашиваемой информации, содержащей персональные данные субъекта, её перечень, цель использования, Ф.И.О. и должность лица, которому поручается получить данную информацию.

5.4.9. Факт передачи персональных данных субъекта регистрируются в «Журнале учета передачи персональных данных» (Приложение № 4). В журнале фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, перечень передаваемой информации. Ответственность за соблюдение вышеуказанного порядка предоставления персональных данных субъекта несет работник Оператора и его непосредственный руководитель.

5.4.10. Представителю субъекта (в том числе адвокату) персональные данные передаются в порядке, установленном действующим законодательством и настоящим Положением. Информация передается при наличии одного из документов:

- нотариально удостоверенной доверенности представителя субъекта;
- письменного заявления субъекта, написанного в присутствии уполномоченного работника Оператора.

5.4.11. Доверенности и заявления приобщаются к совокупности документов субъекта персональных данных.

5.4.12. Документы, содержащие персональные данные субъекта, могут быть отправлены почтовым отправлением. При этом должна быть обеспечена их конфиденциальность. Документы, содержащие персональные данные вкладываются в конверт, к нему прилагается сопроводительное письмо. На конверте делается надпись о том, что содержимое конверта является конфиденциальной информацией, и за незаконное ее разглашение законодательством предусмотрена ответственность. Далее, конверт с сопроводительным письмом вкладывается в другой конверт, на который наносятся только реквизиты, предусмотренные правилами обмена почтовыми сообщениями для заказных почтовых отправлений.

5.4.13. Трансграничная передача персональных данных запрещена.

5.5. Уточнение, изменение, блокирование персональных данных

5.5.1. Оператор обязан безвозмездно предоставить субъекту персональных данных возможность ознакомления с персональными данными, относящимися к соответствующему субъекту, а также внести в них необходимые изменения, уничтожить

или блокировать соответствующие персональные данные по предоставлению субъектом сведений, подтверждающих, что персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Оператор обязан уведомить соответствующего субъекта персональных данных и третьих лиц, которым персональные данные этого субъекта были переданы.

5.5.2. 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, уполномоченными работниками Оператора вносятся в них необходимые изменения.

5.5.3. В случае выявления неточных персональных данных или неправомерной обработки 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 осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки. В случае подтверждения факта неточности персональных данных Оператор на основании соответствующих документов уточняет персональные данные в течение семи дней и снимает их блокирование.

5.5.4. 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.

5.6. Уничтожение персональных данных

5.6.1. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что его персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уполномоченные работники Оператора уничтожают такие записи о персональных данных и материальные носители их содержащие (полученные в ходе обработки без использования средств автоматизации).

5.6.2. В случае выявления неправомерной обработки персональных данных, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных. В случае, если обеспечить

правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие записи о персональных данных и материальные носители их содержащие (полученные в ходе обработки без использования средств автоматизации).

5.6.3. В случае достижения цели обработки персональных данных Оператор прекращает обработку персональных данных и уничтожает персональные данные 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 федеральными законами.

5.6.4. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператор прекращает их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные в срок, не превышающий тридцати 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 федеральными законами.

5.6.5. В случае обращения субъекта персональных данных к Оператору с требованием о прекращении обработки персональных данных Оператор обязан в срок, не превышающий 10 рабочих дней с даты получения Оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона «О персональных данных». Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

5.6.6. Перед уничтожением персональных данных необходимо:

- убедиться в наличии правовых оснований уничтожения персональных данных;
- убедиться в том, что уничтожаются именно те персональные данные, которые предназначены для уничтожения;
- уничтожить персональные данные подходящим способом, указанным в соответствующем требовании или распорядительном документе;
- проверить необходимость уведомления об уничтожении персональных данных субъекта персональных данных, или его представителя, или третьих лиц в предусмотренном случае.

5.6.7. 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).

5.6.8. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пункте 5.6.5, 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 6 месяцев, если иной срок не установлен федеральными законами.

5.6.9. Подтверждение уничтожения персональных данных осуществляется в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных.

6. Права субъектов персональных данных

6.1. В целях обеспечения защиты персональных данных, субъекты персональных данных имеют право:

- получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);
- осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральным законом;
- требовать исключения или исправления неверных, или неполных персональных данных, а также данных, обработанных с нарушением Федерального закона. Субъект персональных данных при отказе Оператора исключить или исправить персональные

данные имеет право заявить в письменной форме Оператору о своем несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера субъект персональных данных имеет право дополнить заявлением, выражающим его собственную точку зрения;

- требовать от Оператора уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта персональных данных, обо всех произведенных в них изменениях или исключениях из них;

- обжаловать в суде любые неправомерные действия или бездействие Оператора при обработке и защите персональных данных субъекта персональных данных.

6.2. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

6.3. Субъект персональных данных не должен отказываться от своих прав на сохранение и защиту охраняемой законом тайны.

7. Правила рассмотрения запросов субъектов персональных данных

7.1. Субъекты, персональные данные которых обрабатываются у Оператора, имеют 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, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании действующего законодательства Российской Федерации;

- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен действующим законодательством Российской Федерации;

- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных действующим законодательством Российской Федерации;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных в подразделении Оператора;
- информацию о способах исполнения оператором обязанностей, установленных статьей 18.1 Федерального закона «О персональных данных»;
- иные сведения, предусмотренные действующим законодательством Российской Федерации.

7.2. 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.

7.3. Запрос субъекта персональных данных направляется Оператору для рассмотрения в письменной форме. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных, 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 ранее были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Оператору или направить повторный запрос в целях получения сведений, 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 действующим законодательством Российской Федерации.

7.5. Повторный запрос субъекта персональных данных наряду с необходимыми сведениями должен содержать обоснование его направления.

7.6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса в случае, если сведения, указанные в п. 7.1, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу в полном объеме, и субъект персональных данных обратился повторно к Оператору или направить ему повторный запрос ранее чем через 30 дней

после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен действующим законодательством Российской Федерации.

7.7. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

7.8. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных при получении запроса уполномоченный работник Оператора обязан дать в письменной форме мотивированный ответ, содержащий ссылку на статью 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» или иной федеральный закон, являющийся основанием для такого отказа, в срок, не превышающий 30 дней со дня обращения субъекта персональных данных либо с даты регистрации данного запроса.

7.9. В день поступления запроса к Оператору от субъекта персональных данных указанный запрос проверяется на повторность и регистрируется в «Журнале учета обращений субъектов персональных данных по вопросам обработки персональных данных» (Приложение № 5).

7.10. После регистрации запросы субъектов персональных данных передаются не позднее следующего рабочего дня руководителям и ответственным работникам подразделения Оператора, имеющим доступ к запрашиваемым персональным данным в соответствии с их должностными обязанностями, для подготовки ответа.

7.11. Сведения, указанные в п. 7.1 настоящего Положения, предоставляются субъекту персональных данных или его представителю уполномоченным должностным лицом структурного подразделения Оператора, осуществляющего обработку соответствующих персональных данных при обращении либо при получении запроса субъекта персональных данных или его представителя.

7.12. Исполнитель обеспечивает рассмотрение запроса субъектов персональных данных и подготовку ответа.

7.13. Сведения должны быть предоставлены субъекту персональных данных в течение 10 рабочих дней с момента обращения либо получения Оператором запроса субъекта персональных данных или его представителя 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.

7.14. Срок предоставления ответа может быть продлен, но не более чем на пять рабочих дней в случае направления Оператором в адрес субъекта персональных данных

мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

7.15. Оператор предоставляет сведения, указанные п. 7.1, субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

7.16. Запрос считается исполненным, если субъекту персональных данных предоставлена информация в полном объеме и даны необходимые разъяснения в соответствии с действующим законодательством Российской Федерации.

7.17. Непосредственный контроль за соблюдением установленного действующим законодательством Российской Федерации и настоящим Положением порядка рассмотрения запросов субъектов персональных данных осуществляет лицо, ответственное за организацию обработки персональных данных.

8. Меры, направленные на обеспечение безопасности персональных данных

8.1. Общие меры

8.1.1. Оператор при осуществлении обработки персональных данных:

- принимает меры, необходимые и достаточные для обеспечения выполнения требований законодательства Российской Федерации и локальных нормативных актов Оператора в области защиты персональных данных;

- принимает правовые, организационные и технические меры 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;

- назначает лицо, ответственное за организацию обработки персональных данных у Оператора;

- издает локальные нормативные акты, определяющие политику Оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

– сообщает в установленном порядке субъектам персональных данных или их представителям информацию о наличии персональных данных, относящихся к соответствующим субъектам, предоставляет возможность ознакомления с этими персональными данными при обращении и (или) поступлении запросов указанных субъектов персональных данных или их представителей, если иное не установлено законодательством Российской Федерации;

– прекращает обработку и уничтожает персональные данные в случаях, предусмотренных законодательством Российской Федерации в области персональных данных;

– в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям у Оператора проводятся периодические проверки условий обработки персональных данных;

– совершает иные действия, предусмотренные законодательством Российской Федерации в области персональных данных.

8.1.2. Работники Оператора, ответственные за хранение персональных данных, а также работники Оператора, владеющие персональными данными в силу своих должностных обязанностей, подписывают обязательство о неразглашении информации ограниченного доступа.

8.1.3. Помещения, в которых хранятся персональные данные, оборудуются сейфами, надежными замками, противопожарной сигнализацией. В рабочее время при отсутствии работников помещения запираются на ключ. Проведение уборки помещений, в которых хранятся персональные данные, производится в присутствии соответствующих работников Оператора.

8.1.4. Лица, назначенные ответственными за обеспечение безопасности персональных данных у Оператора, осуществляют ознакомление работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных.

8.1.5. Не реже одного раза в год проводится внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами Оператора.

8.1.6. В целях информационного обеспечения у Оператора создаются общедоступные источники персональных данных работников (далее – Справочники), в

которые включаются его фамилия, имя, отчество, сведения о занимаемой им должности, номер служебного телефона, иные персональные данные, предоставленные субъектом персональных данных.

8.1.7. Формирование, ведение и иные действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, содержащихся в Справочниках, осуществляются подразделениями Оператора, ответственными за ведение каждого Справочника.

8.2. Меры, направленные на обеспечение безопасности персональных данных при их обработке в информационных системах

8.2.1. Обработка персональных данных субъектов персональных данных, указанных в п. 4.1 настоящего Положения, осуществляется в информационных системах Оператора.

8.2.2. Классификация информационных систем и определение уровня защищенности информационных систем осуществляется в порядке, установленном законодательством Российской Федерации.

8.2.3. Работникам Оператора, имеющим право осуществлять обработку персональных данных в информационных системах Оператора, предоставляется уникальный логин и пароль для доступа к информационной системе. Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными регламентами.

8.2.4. Для обеспечения безопасности персональных данных при их обработке в информационных системах (далее – ИС) осуществляется защита информации, обрабатываемой техническими средствами, под которыми понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации.

8.2.5. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного доступа к персональным данным, результатом которого может стать уничтожение, блокирование, изменение, копирование, распространение персональных данных, а также иных несанкционированных действий, а также принятия следующих мер по обеспечению безопасности:

- определением угроз безопасности персональных данных при их обработке в информационной системе;

- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни (классы) защищенности персональных данных;

- применением прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

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

- учетом машинных носителей персональных данных;

- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер реагирования;

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

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

- организацией контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровня (класса) защищенности информационной системы.

8.2.6. Организуется режим защиты помещений, в которых осуществляется обработка персональных данных, размещение технических средств ИС, машинных носителей информации, исключающий возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

8.2.7. Все магнитные, оптические и другие машинные носители персональных данных подлежат обязательному учету. На носители информации наносится маркировка, позволяющая идентифицировать и организовать их учет. Машинные носители информации, в том числе с резервными копиями персональных данных, регистрируются в журнале учета машинных носителей персональных данных, в котором отражается:

- тип и емкость носителя;

- учетный номер носителя;

- место установки (использования) носителя;

- дата установки носителя;

- ответственное должностное лицо;

- сведения о списании носителя и уничтожении информации.

8.2.8. Пользователям запрещается использовать съемные носители информации за исключением случаев, когда использование съемных носителей необходимо в рамках должностных обязанностей.

8.2.9. Структурное подразделение (ответственное лицо) Оператора, ответственное за обеспечение информационной безопасности у Оператора, организует и контролирует ведение учета материальных носителей персональных данных.

8.2.10. Структурное подразделение (ответственное лицо) Оператора, ответственное за обеспечение безопасности персональных данных при их обработке в информационных системах, обеспечивает:

- своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до ответственного за организацию обработки персональных данных у Оператора;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных;
- знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- принятие всех необходимых мер по восстановлению персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;
- незамедлительное приостановление предоставления персональных данных пользователям информационной системы персональных данных при обнаружении нарушений порядка предоставления персональных данных (до момента выявления причин нарушений и устранения их причин);
- проведение разбирательств и составление заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня

защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

8.2.11. Обмен персональными данными при их обработке в информационных системах Оператора осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

8.3. Меры, направленные на обеспечение безопасности персональных данных при их обработке без использования средств автоматизации

8.3.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, осуществляется 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.

8.3.2. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных.

8.3.3. Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

8.3.4. Работники Оператора, осуществляющие обработку персональных данных без использования средств автоматизации, проинформированы о факте обработки ими персональных данных, обработка которых осуществляется у Оператора без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных законодательством и локальными нормативными актами Оператора.

8.3.5. 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, принимаются меры по обеспечению раздельной обработки персональных данных, в частности:

- 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;

- 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.

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

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

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

- 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;

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

8.3.7. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию Оператора, или в иных аналогичных целях, должны соблюдаться следующие условия:

- необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена локальным актом Оператора, содержащим сведения о цели обработки персональных данных, осуществляемой 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;

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

- 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 Оператора.

8.3.8. 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).

8.3.9. 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.

9. Первичный инструктаж лица, допущенного к работе с персональными данными

9.1. Первичный инструктаж лица, допущенного к работе с персональными данными (далее – лицо), проводит администратор безопасности после утверждения руководителем документа о наделении лица правом доступа к персональным данным до непосредственного доступа этого лица к персональным данным.

9.2. Лицо получает непосредственный доступ к персональным данным только после прохождения первичного инструктажа.

9.3. Лицо должно быть ознакомлено с нормативными правовыми актами Российской Федерации в сфере защиты персональных данных.

9.4. Лицо должно быть ознакомлено с локальными актами Оператора, регламентирующими вопросы защиты персональных данных.

9.5. Лицо, являющееся пользователем ИС, должно иметь доступ только к тем функциям ИС, которые необходимы для выполнения им его должностных обязанностей.

9.6. Администратор безопасности, проводящий инструктаж лица, обязан разъяснить ему, какие действия в ИС лицо имеет право совершать, а какие действия ему запрещены.

9.7. Лицо, допущенное к работе с персональными данными, должно быть предупреждено:

- об обязанностях выполнения всех правил и требований, предусмотренных локальными актами Оператора в области защиты персональных данных;
- о проведении разбирательств по фактам совершения действий, связанных с доступом к персональным данным и повлекших за собой негативные последствия, в соответствии с установленным Порядком проведения разбирательств по фактам нарушения требований по обеспечению безопасности персональных данных.

9.8. Факт прохождения лицом первичного инструктажа регистрируется администратором безопасности в соответствующем «Журнале учета пользователей, имеющих право доступа к информационным системам» (Приложение № 6).

10. Правила работы с обезличенными данными

10.1. Обезличивание персональных данных у Оператора проводится с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

10.2. При использовании процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

10.3. Способы обезличивания при условии дальнейшей обработки персональных данных:

- замена части сведений идентификаторами;
- изменение состава или семантики – изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения, преобразования или удаления части сведений;
- декомпозиция (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим отдельным хранением подмножеств);
- перемешивание (перестановка отдельных записей, а также групп записей в массиве персональных данных).

10.4. Решение о необходимости обезличивания персональных данных принимает руководитель Оператора.

10.5. Работники Оператора, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.

10.6. Работники Оператора, непосредственно осуществляющие обработку персональных данных, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

10.7. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

10.8. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

10.9. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями (если они используются);
- правил резервного копирования;
- правил доступа в помещения, где расположены элементы информационных систем.

10.10. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;
- правил доступа к ним и в помещения, где они хранятся.

11. Порядок взаимодействия с уполномоченным органом по защите прав субъектов персональных данных

11.1. В целях уведомления уполномоченного органа по защите прав субъектов персональных данных (Роскомнадзор) лицо, ответственное за организацию обработки персональных данных у Оператора, направляет уведомление о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных, в следующих случаях:

- о намерении осуществлять обработку персональных данных;
- при вводе в эксплуатацию новых информационных систем персональных данных у Оператора;
- при внесении существенных изменений в существующие информационные системы персональных данных Оператора.

11.2. Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается руководителем Оператора.

11.3. Уведомление должно содержать следующие сведения:

- наименование, адрес Оператора;
- цель обработки персональных данных;
- категории персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовое основание обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых Оператором способов обработки персональных данных;
- описание принятых мер защиты персональных данных, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
- фамилию, имя, отчество работника Оператора, ответственного за организацию обработки персональных данных, и номера контактных телефонов, почтовые адреса и адреса электронной почты;
- дату начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации;
- фамилия, имя, отчество физического лица или наименование юридического лица, имеющих доступ и (или) осуществляющих на основании договора обработку персональных данных, содержащихся в государственных и муниципальных информационных системах.

11.4. Лицо, ответственное за организацию обработки персональных данных у Оператора, осуществляет контроль соответствия сведений, внесенных уполномоченным органом по защите прав субъектов персональных данных в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.

11.5. В случае изменения сведений, указанных в п. 11.3, Оператор не позднее 15-го числа месяца, следующего за месяцем, в котором возникли такие изменения, обязан уведомить уполномоченный орган по защите прав субъектов персональных данных обо

всех произошедших за указанный период изменениях. В случае прекращения обработки персональных данных Оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение 10 рабочих дней с даты прекращения обработки персональных данных.

11.6. При получении запроса от уполномоченного органа по защите прав субъектов персональных данных лицо, ответственное за организацию обработки персональных данных у Оператора, осуществляет подготовку и направление ответа в течение тридцати дней с даты получения такого запроса.

11.7. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Оператор обязан с момента выявления такого инцидента Оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

- течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

12. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

12.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными актами у Оператора организовывается проведение периодических проверок условий обработки персональных данных с последующей регистрацией в «Журнале учета проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных» (Приложение № 7).

12.2. Проверки осуществляются ответственным за организацию обработки персональных данных у Оператора либо комиссией, назначаемой руководителем Оператора.

12.3. В проведении проверки не может участвовать работник Оператора, прямо или косвенно заинтересованный в её результатах.

12.4. Проверки соответствия обработки персональных данных установленным требованиям у Оператора проводятся на основании утвержденного ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего к Оператору письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

12.5. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- состояние учета машинных носителей персональных данных;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- осуществление мероприятий по обеспечению целостности персональных данных.

12.6. Ответственный за организацию обработки персональных данных у Оператора (комиссия) имеет право:

- запрашивать у работников Оператора информацию, необходимую для реализации полномочий;

– требовать от уполномоченных на обработку персональных данных работников уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем персональных данных;

– принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

– вносить руководителю Оператора предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

– вносить руководителю Оператора предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

12.7. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных у Оператора (комиссии) в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

12.8. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, руководителю Оператора докладывает ответственный за организацию обработки персональных данных либо председатель комиссии, в форме письменного заключения.

12.9. Руководитель Оператора обязан контролировать своевременность и правильность проведения проверки.

13. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ

«О персональных данных»

13.1. Оценкой вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» является определение юридических последствий в отношении субъекта персональных данных.

13.2. К юридическим последствиям относятся случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или иным образом затрагивающее его права, свободы и законные интересы.

13.3. При обработке персональных данных должны определяться и документально оформляться все возможные юридические или иным образом затрагивающие права и законные интересы последствия в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

13.4. Определение таких юридических последствий необходимо для недопущения нарушения и обеспечения 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.

13.5. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» оформляется документально.

13.6. В процессе осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных производится оценка соотношения вреда, который может быть причинен субъектам персональных данных и применяемых мер, направленных на выполнение обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

13.7. При оценке соотношения вреда, который может быть причинен субъектам персональных данных, для каждой ИС производится экспертное сравнение заявленной Оператором в своих локальных актах оценки вреда, который может быть причинен субъектам персональных данных, и применяемых мер, направленных на выполнение обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», и изложенных в настоящем Положении.

13.8. По итогам сравнений принимается решение о достаточности применяемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области персональных данных и возможности или необходимости принятия дополнительных мер или изменения установленного порядка организации и проведения работ по обеспечению безопасности персональных данных при их обработке.

14. Порядок проведения служебных проверок по фактам нарушения требований по обеспечению безопасности персональных данных

14.1. Классификация нарушений требований по обеспечению безопасности персональных данных

14.1.1. Нарушения требований по обеспечению безопасности персональных данных и их последствия классифицируются по значимости на:

- нарушения I категории;
- нарушения II категории;
- нарушения III категории.

14.1.2. Служебная проверка назначается по нарушениям I и II категорий.

14.2. Перечень нарушений требований по обеспечению безопасности персональных данных

14.2.1. Нарушения I категории, к которым относятся нарушения, повлекшие за собой разглашение (утечку), уничтожение (искажение) персональных данных и/или утрату машинных носителей персональных данных, выведение из строя технических и программных средств, входящих в состав ИС, а именно:

- успешный подбор административного пароля;
- несанкционированная реконфигурация параметров ИС;
- утрата или кража резервной копии базы, содержащей персональных данных;
- необоснованная передача информационных массивов ИС;
- организация утечки сведений по техническим каналам;
- умышленное нарушение работоспособности ИС;
- НСД к персональным данным;
- несанкционированное внесение изменений в ИС;
- целенаправленное заражение персональных электронных вычислительных машин (далее – ПЭВМ) и серверов, входящих в состав ИС, вирусами;
- проведение работ с ИС, повлекшее за собой необратимую потерю данных;
- другие действия, попадающие под действия статей, приведенных в следующей таблице.

Номер статьи	Название статьи
Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации»	
ст. 17	Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации
Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»	
ст. 24	Ответственность за нарушение требований Федерального закона «О персональных данных»
Кодекс Российской Федерации об административных правонарушениях	
ст. 13.11	Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)
ст. 13.11.1	Распространение информации о свободных рабочих местах или вакантных должностях, содержащей ограничения дискриминационного характера
ст. 13.12	Нарушение правил защиты информации
ст. 13.14	Разглашение информации с ограниченным доступом
Уголовный кодекс Российской Федерации	
ст. 137	Нарушение неприкосновенности частной жизни
ст.140	Отказ в предоставлении гражданину информации
ст. 272	Неправомерный доступ к компьютерной информации
ст. 273	Создание, использование и распространение вредоносных компьютерных программ
ст. 274	Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
Трудовой кодекс Российской Федерации	
ст. 90	Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

14.2.2. Нарушения II категории, к которым относятся нарушения, в результате которых возникают предпосылки к разглашению (утечке), уничтожению (искажению) персональных данных, утрате машинных носителей персональных данных, выведению из строя технических и программных средств, входящих в состав ИС, а именно:

- ошибка при входе в ИС (набор не назначенного пароля, более 3 (Трех) раз подряд, периодически);

- оставление ПЭВМ включенной (незаблокированной) во время отсутствия на рабочем месте;
- перезагрузка ПЭВМ при сбоях в работе, в т.ч. аварийная (неоднократная) перезагрузка путем нажатия кнопки RESET;
- утрата учетного машинного носителя персональных данных;
- многократная неудачная попытка входа под чужим именем, паролем;
- удачная попытка входа под чужим именем, паролем;
- несанкционированная очистка журналов аудита;
- несанкционированное копирование персональных данных на внешние носители информации;
- несанкционированная установка (удаление) программного обеспечения (далее – ПО) в ИС;
- несанкционированное изменение конфигурации ПО ИС;
- попытка получения прав администратора на ПЭВМ (увеличения полномочий собственных прав, получение прав на отладку программ) удачная и неудачная;
- попытка получения прав администратора в домене или на удаленной машине, удачная и неудачная;
- совершение действий, приводящих к заражению ПЭВМ компьютерными вирусами;
- несанкционированное использование сканирующего ПО;
- несанкционированное использование анализаторов протоколов (снифферов);
- несанкционированный просмотр, вывод на печать и т.п. персональных данных.

14.2.3. Нарушения III категории, к каковым относятся нарушения, не несущие признаков нарушений I и II категорий, а именно:

- ошибка при входе в ИС (набор неправильного пароля, сетевого имени более 3 (трех) раз подряд, не периодическая);
- периодическая попытка неудачного доступа к персональным данным ИС;
- перевод времени на ПЭВМ;
- однократная перезагрузка ПЭВМ при сбоях в работе ПЭВМ, в т.ч. аварийная перезагрузка, путем нажатия кнопки RESET;
- нецелевое использование корпоративных ресурсов (печать, Internet, mail, и т.п.).

14.3. Назначение и проведение служебных проверок

14.3.1. Служебная проверка назначается по нарушениям I и II категорий.

14.3.2. Служебная проверка может быть инициирована на основании устного заявления, докладной или служебной записки любого работника по выявленному отдельному факту нарушения, либо по факту группы нарушений.

14.3.3. Служебная проверка проводится комиссией, состав которой утверждает руководитель Оператора. Члены комиссии имеют право:

- требовать документального подтверждения факта нарушения;
- устанавливать причины допущенных нарушений любым из способов, не противоречащим законодательству Российской Федерации;
- брать письменные объяснения по поводу выявленных нарушений у любого работника.

14.4. Оформление результатов работы комиссии

14.4.1. Результаты работы комиссии должны быть оформлены в виде аналитического экспертного заключения, в котором отражается:

- состав комиссии;
- период времени, в течение которого проводилась служебная проверка;
- основание для проведения служебной проверки;
- документальное подтверждение фактов нарушений, выявленных в ходе служебной проверки и имеющих значение в определении наличия нарушений, а также иных фактов, которые могут привести к нарушению конфиденциальности персональных данных или к снижению уровня защищенности персональных данных;
- установленные причины выявленных нарушений;
- вывод о значимости нарушений, их причинах и виновных, допустивших данные нарушения;
- рекомендации по совершенствованию обеспечения безопасности персональных данных, исключающие в дальнейшем подобные нарушения.

15. Порядок приостановления обработки персональных данных

15.1. При обнаружении нарушений I категории обработка персональных данных незамедлительно приостанавливается до выявления причин нарушений и устранения этих причин.

15.2. Принятие решения о приостановлении обработки персональных данных принимается руководителем Оператора.

15.3. По факту нарушения требований по обеспечению безопасности, повлекшего приостановление обработки персональных данных, проводится служебная проверка.

16. Порядок обращения со средствами защиты информации

16.1. Учет средств защиты информации

16.1.1. Под средствами защиты информации (далее – СЗИ) в настоящем разделе понимается СЗИ, не являющееся средствами криптографической защиты (далее – СКЗИ).

16.1.2. Инсталлирующие СЗИ носители, установленные СЗИ, эксплуатационная и техническая документация к СЗИ подлежат поэкземплярому учету в «Журнале учета средств защиты информации, эксплуатационной и технической документации к ним» (Приложение № 8).

16.2. Распространение средств защиты информации

16.2.1. СЗИ доставляются фельдъегерской (в том числе ведомственной) связью или со специально выделенными работниками при соблюдении мер, исключающих бесконтрольный доступ к СЗИ во время доставки.

16.2.2. При пересылке СЗИ помещаются в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия. Эксплуатационная и техническая документация к СЗИ пересылается заказными, ценными почтовыми отправлениями или доставляется специально выделенными работниками.

16.2.3. При пересылке СЗИ, эксплуатационной и технической документации к ним подготавливается сопроводительное письмо, в котором указывается: что посылается и в каком количестве, учетные номера изделий или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывается в одну из упаковок.

16.2.4. Отправитель контролирует доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель направляет ему запрос и принимает меры к уточнению местонахождения отправлений.

16.3. Получение средств защиты информации

16.3.1. Полученные упаковки вскрываются только лицом, для которого они предназначены.

16.3.2. Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получателем составляется акт, который высылается отправителю. Полученные с такими отправлениями СЗИ до получения указаний от отправителя применять не разрешается.

16.3.3. При обнаружении бракованных СЗИ один экземпляр бракованного изделия возвращается отправителю для установления причин происшедшего и их устранения

в дальнейшем, а оставшиеся экземпляры хранятся до поступления дополнительных указаний от отправителя.

16.3.4. Получение СЗИ, эксплуатационной и технической документации к ним подтверждается отправителю в соответствии с порядком, указанным в сопроводительном письме.

16.4. Уничтожение средств защиты информации

16.4.1. СЗИ уничтожаются (утилизируются) по решению руководителя Оператора.

16.4.2. Намеченные к уничтожению (утилизации) СЗИ изымаются из аппаратных средств, с которыми они функционировали. При этом СЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СЗИ процедура удаления программного обеспечения СЗИ и они полностью отсоединены от аппаратных средств.

16.4.3. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения используются после уничтожения СЗИ без ограничений.

16.4.4. Уничтожение большого объема устанавливающих СЗИ носителей оформляется актом. Уничтожение по акту производится комиссией в составе не менее трех человек из числа лиц, допущенных к работе с СЗИ. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых устанавливающих СЗИ носителей. Исправления в тексте акта оговариваются и заверяются подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в журнале учета средств защиты информации, эксплуатационной и технической документации к ним.

16.4.5. Эксплуатационная и техническая документация к СЗИ уничтожается путем сжигания или с помощью любых бумагорезательных машин. Факт уничтожения эксплуатационной и технической документации к СЗИ оформляется в журнале учета средств защиты информации, эксплуатационной и технической документации к ним.

16.4.6. Уничтожение большого объема эксплуатационной и технической документации к СЗИ оформляется актом. Уничтожение по акту производится комиссией в составе не менее трех человек из числа лиц, допущенных к работе с СЗИ. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемой эксплуатационной и технической документации к СЗИ. Исправления в тексте акта оговариваются и заверяются подписями всех членов комиссии, принимавших участие в

уничтожении. О проведенном уничтожении делаются отметки в журнале учета средств защиты информации, эксплуатационной и технической документации к ним.

16.5. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены средства защиты информации

16.5.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СЗИ, должны обеспечивать сохранность персональных данных, СЗИ, исключать возможность неконтролируемого проникновения или пребывания в помещениях, где установлены СЗИ, посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

16.5.2. При оборудовании помещений, где установлены СЗИ, должны выполняться требования к размещению и монтажу СЗИ, а также другого оборудования, функционирующего с СЗИ.

16.5.3. Инсталлирующие СЗИ носители, эксплуатационная и техническая документация к СЗИ должна храниться в металлических хранилищах (ящиках, шкафах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

16.5.4. Помещения, где установлены СЗИ, должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

16.5.5. Для предотвращения просмотра извне помещений, где установлены СЗИ, их окна должны быть оборудованы шторами или жалюзи.

17. Ответственность за нарушение требований, регулирующих получение, обработку и хранение персональных данных

17.1. Работники Оператора, уполномоченные на обработку персональных данных, могут привлекаться в соответствии с законодательством Российской Федерации к дисциплинарной и иной ответственности за разглашение конфиденциальных сведений, содержащихся в указанных личных делах, а также за иные нарушения порядка ведения личных дел, установленного законодательством РФ.

17.2. Лица, виновные в нарушении норм, регулирующих обработку персональных данных, несут административную ответственность по статьям 13.11, 13.14 Кодекса об административных правонарушениях РФ.

17.3. Предоставление персональных данных посторонним лицам, в том числе, работникам Оператора, не имеющим права их обрабатывать, распространение персональных данных, утрата материальных носителей информации, содержащих персональные данные субъекта, а также иные нарушения обязанностей по обработке

персональных данных, установленных настоящим Положением, локальными актами Оператора, влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарного взыскания: замечания, выговора или увольнения.

17.4. Лица, имеющие доступ к персональным данным субъектов, виновные в незаконном сборе или передаче персональных данных, а также осуществившие неправомерный доступ к охраняемой законом компьютерной информации, несут уголовную ответственность в соответствии со ст.ст. 137, 272 Уголовного кодекса РФ.