

**ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ФЕДЕРАЛЬНОМ
КАЗЕННОМ УЧРЕЖДЕНИИ ЗДРАВООХРАНЕНИЯ «РОСТОВСКИЙ-НА-ДОНУ
ПРОТИВОЧУМНЫЙ ИНСТИТУТ» РОСПОТРЕБНАДЗОРА**

1. Общие положения

1.1. Настоящее Положение об обработке и защите персональных данных в Федеральном казённом учреждении здравоохранения «Ростовский-на-Дону ордена Трудового Красного Знамени научно-исследовательский противочумный институт Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека» (далее — Положение) определяет цели, содержание и порядок обработки персональных данных, меры, направленные на защиту персональных данных, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных в указанном Институте.

1.2. Настоящее Положение определяет политику Института как оператора, осуществляющего обработку персональных данных, в отношении обработки и защиты персональных данных.

1.3. Настоящее Положение разработано на основании требований следующих нормативных правовых актов: Трудовой кодекс Российской Федерации, Кодекс Российской Федерации об административных правонарушениях, Федеральный закон от 27 июля 2006 года номер 152-ФЗ «О персональных данных», Федеральный закон от 27 июля 2006 года номер 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 27 мая 2003 года номер 58-ФЗ «О системе государственной службы Российской Федерации», Федеральный закон от 27 июля 2004 года номер 79-ФЗ «О государственной гражданской службе Российской Федерации», Федеральный закон от 25 декабря 2008 года номер 273-ФЗ «О противодействии коррупции», Федеральный закон от 27 июля 2010 года номер 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», Федеральный закон от 2 сентября 2006 года номер 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Федеральный закон от 7 июля 2003 года номер 126-ФЗ «О связи», Указ Президента Российской Федерации от 30 мая 2005 года номер 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела», постановление Правительства Российской Федерации от 16 марта 2009 года номер 228 «О Федеральной службе по надзору в сфере защиты прав потребителей и благополучия человека», постановление Правительства Российской Федерации от 1 ноября 2012 года номер 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановление Правительства Российской Федерации от 6 июля 2008 года номер 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», постановление Правительства Российской Федерации от 15 сентября 2008 года номер 687 «Об утверждении Поло-

жения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановление Правительства Российской Федерации от 21 марта 2012 года номер 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановление Правительства Российской Федерации от 10 сентября 2009 года номер 723 «О порядке ввода в эксплуатацию отделанных государственных информационных систем», приказ Федеральной службы по техническому и экспортному контролю России, Федеральной службы безопасности России, Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 года номер 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных», «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом Федеральной службы по техническому и экспортному контролю России номер семнадцать от 11 февраля 2013 года, «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом Федеральной службы по техническому и экспортному контролю России номер двадцать один от 18 февраля 2013 года, методический документ «Меры защиты информации в государственных информационных системах», утвержденный Федеральной службой по техническому и экспортному контролю России 11 февраля 2014 года, «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утвержденные приказом Федеральной службы безопасности России номер триста семьдесят восемь от 10 июля 2014 года, «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом Федеральной службы безопасности России номер шестьдесят шесть от 9 февраля 2005 года, «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 года номер сто пятьдесят два, а также Федеральный закон от 29 декабря 2022 года номер 572-ФЗ «О единой биометрической системе, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации».

1.4. Обработка персональных данных в Институте осуществляется с соблюдением принципов и условий, предусмотренных настоящим Положением и законодательством Российской Федерации в области персональных данных.

1.5. Юридические и физические лица, в соответствии со своими полномочиями владеющие, получающие и использующие информацию о субъектах персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную, предусмотрен-

ную законодательством Российской Федерации, ответственность за нарушение правил обработки и защиты этой информации.

1.6. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно до замены его новым Положением.

1.7. Все изменения в настоящее Положение вносятся на основании приказа директора Института.

1.8. Доступ сотрудника к работе разрешается только после ознакомления с настоящим Положением под подпись. Руководители структурных подразделений обязаны организовать своевременное ознакомление вновь принятых сотрудников, а также своих непосредственных подчиненных при изменении редакции настоящего Положения. Факт ознакомления фиксируется в Листе ознакомления, который является неотъемлемой частью личного дела или хранится вместе с трудовой книжкой (сведениями о трудовой деятельности). Согласие о неразглашении конфиденциальной информации (персональных данных), форма которого приведена в (Приложении № 4) к настоящему Положению, подписывается сотрудником одновременно с трудовым договором.

1.9. Проведение инструктажа по информационной безопасности и правилам обработки ПДн является обязательным условием допуска сотрудника к работе. Факт проведения инструктажа подлежит фиксации в Журнале учета инструктажей (Приложение № 10).

2. Термины и определения:

Автоматизированная обработка персональных данных — обработка персональных данных с использованием средств вычислительной техники.

Автоматизированная система — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Атака — целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой криптосредством информации или с целью создания условий для этого.

Безопасность — состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Безопасность объекта — состояние защищенности объекта от внешних и внутренних угроз.

Безопасность информации — состояние защищённости информации, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации.

Безопасность информационной технологии — состояние защищенности информационной технологии, при котором обеспечивается выполнение изделием, реализующим информационную технологию, предписанных функций без нарушений безопасности обрабатываемой информации.

Биометрические персональные данные — сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его

личность и которые используются оператором для установления личности субъекта персональных данных.

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

Доступ к информации — возможность получения информации и ее использования.

Жизненно важные интересы — совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

Защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информационная безопасность в организации — состояние защищенности интересов организации в условиях угроз в информационной сфере.

Информационный процесс — процесс создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.

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

Информационная сфера — совокупность информации, информационной инфраструктуры, субъектов осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Информационная технология — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация — сведения (сообщения, данные) независимо от формы их представления.

Инцидент информационной безопасности — любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Использование персональных данных — действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

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

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

Межсетевой экран — локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы).

Модель угроз — перечень возможных угроз информации.

Нарушение информационной безопасности в организации — случайное или преднамеренное неправомерное действие физического лица (субъекта, объекта) в отношении активов организации, следствием которого является нарушение безопасности информации при ее обработке техническими средствами в информационных системах, вызывающее негативные последствия (ущерб или вред) для организации.

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

Обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации определяемую по каким-либо признакам.

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.

Общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Объект информатизации — совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

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, а также действия (операции), совершаемые с персональными данными.

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

Пользователь информационной системы персональных данных — лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

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

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

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

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

Трансграничная передача персональных данных — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Уничтожение информации — действия, в результате которого невозможно восстановить содержание информации в информационной системе или в результате которых уничтожаются материальные носители информации.

Уполномоченное оператором лицо — лицо, которому на основании договора оператор поручает обработку персональных данных.

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

3. Порядок обработки персональных данных сотрудников Института

3.1. Персональные данные сотрудников, руководителей и заместителей руководителей Института, граждан, претендующих на замещение должностей Института и лиц, замещающих должности руководителей подразделений Института, обрабатываются в целях обеспечения кадровой работы, в том числе в целях содействия сотрудникам Института в прохождении государственной службы, формирования кадрового резерва государственной гражданской службы, обучения и должностного роста, учета результатов исполнения сотрудниками Института должностных обязанностей, обеспечения личной безопасности Института, лиц, замещающих должности руководителей подразделений Института, и членов их семьи, обеспечения сотрудникам Института установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, сохранности принадлежащего им имущества, а также в целях противодействия коррупции.

3.2. В целях, указанных в пункте 3.1 настоящего Положения, обрабатываются следующие категории персональных данных сотрудников Института, замещающих должности руководителей подразделений Института, граждан, претендующих на замещение должностей Института, а также граждан, претендующих на замещение должностей руководителей подразделений Института:

- 3.2.1. фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);
- 3.2.2. число, месяц, год рождения;
- 3.2.3. место рождения;
- 3.2.4. информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);
- 3.2.5. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- 3.2.6. адрес места жительства (адрес регистрации, фактического проживания);
- 3.2.7. номер контактного телефона или сведения о других способах связи;
- 3.2.8. реквизиты страхового свидетельства государственного пенсионного страхования;
- 3.2.9. идентификационный номер налогоплательщика;
- 3.2.10. реквизиты страхового медицинского полиса обязательного медицинского страхования;
- 3.2.11. реквизиты свидетельства государственной регистрации актов гражданского состояния;
- 3.2.12. семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);
- 3.2.13. сведения о трудовой деятельности;
- 3.2.14. сведения о воинском учете и реквизиты документов воинского учета; отношение к воинской обязанности (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);
- 3.2.15. сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);
- 3.2.16. сведения об ученой степени;
- 3.2.17. информация о владении иностранными языками, степень владения;
- 3.2.18. медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на службу в Институт и её дальнейшему прохождению;
- 3.2.19. фотография;
- 3.2.20. сведения о предыдущих местах работы, в том числе: дата, основания поступления на работу и назначения на должность, дата, размера денежного содержания;
- 3.2.21. информация, содержащаяся в трудовом договоре, дополнительных соглашениях к договору;

- 3.2.22. сведения о пребывании за границей;
 - 3.2.23. информация о наличии или отсутствии судимости;
 - 3.2.24. информация об оформленных допусках к государственной тайне;
 - 3.2.25. сведения о профессиональной переподготовке и (или) повышении квалификации;
 - 3.2.26. информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;
 - 3.2.27. сведения о доходах, об имуществе и обязательствах имущественного характера (для руководителей структурных подразделений);
 - 3.2.28. номер расчетного счета;
 - 3.2.29. номер банковской карты;
 - 3.2.30. согласие на обработку персональных данных;
 - 3.2.31. наличие (отсутствие) медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, подтвержденное заключением медицинского учреждения;
 - 3.2.32. иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 3.1 настоящего Положения;
 - 3.2.33. биометрические персональные данные (изображение лица, полученное с помощью фото-видео устройств, записи голоса, отпечатки пальцев, используемые для идентификации в системах контроля управления доступом).
- 3.3. Обработка персональных данных и биометрических персональных данных Института, граждан, претендующих на должности сотрудников Института, лиц, замещающих должности руководителей подразделений Института, а также граждан, претендующих на замещение должностей структурных подразделений Института, осуществляется при условии получения предварительного письменного согласия субъекта персональных данных, за исключением случаев, предусмотренных частью второй статьи одиннадцатой Федерального закона «О персональных данных» (реализация международных договоров о реадмиссии, осуществление правосудия, проведение обязательной государственной дактилоскопической регистрации).
- 3.4. Обработка специальных категорий персональных данных сотрудников Института, граждан, претендующих на замещение должностей Института, лиц, замещающих должности руководителей подразделений Института, а также граждан, претендующих на замещение должностей руководителей подразделений Института, осуществляется без согласия указанных лиц в рамках целей, определенных пунктом 3.1 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 у третьей стороны (в соответствии с пунктом 3 статьи 86 Трудового кодекса Российской Федерации требуется письменное согласие руководителей подразделений Института и граждан, претендующих на замещение указанной должности).

3.5. Обработка персональных данных сотрудников Института, граждан, претендующих на замещение должностей Института, лиц, замещающих должности руководителей подразделений Института, а также граждан, претендующих на замещение должностей руководителей подразделений Института, осуществляется при условии получения согласия указанных лиц в следующих случаях:

3.5.1. при передаче (распространении, предоставлении) персональных данных третьим лицам в случаях, не предусмотренных действующим законодательством Российской Федерации о государственной гражданской службе;

3.5.2. при трансграничной передаче персональных данных при трансграничной передаче персональных данных (по форме Согласия, указанной в Приложении № 8 к настоящему Положению);

3.5.2.1. Трансграничная передача персональных данных на территории иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется Институтом при условии получения предварительного письменного согласия субъекта персональных данных.

3.5.2.2. В случае осуществления трансграничной передачи персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, Институт обязан направить уведомление о намерении осуществлять такую передачу в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

3.5.2.3. До истечения 10 рабочих дней с даты подачи уведомления в Роскомнадзор (если от ведомства не поступило решение о запрете или ограничении), передача данных запрещена, за исключением случаев, когда передача необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных.

3.5.2.4. Запрещается трансграничная передача персональных данных иностранным лицам, чья деятельность признана нежелательной на территории Российской Федерации, а также организациям, находящимся под их контролем».

3.5.3. 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;

3.5.4. при использовании систем видеонаблюдения и биометрической идентификации для контроля доступа в режимные зоны и обеспечения безопасности (по формам Согласий, указанным в Приложениях № 3 и № 7 к настоящему Положению).

3.6. При заполнении информационных карт в Единой государственной информационной системе учета результатов научно-исследовательских, опытно-конструкторских и технологических работ гражданского назначения (ЕГИСУ НИОКТР) вносятся следующие персональные научные сотрудников института:

3.6.1. фамилия, имя, отчество;

3.6.2. число, месяц, год рождения;

3.6.3. информация о гражданстве;

3.6.4. реквизиты страхового свидетельства государственного пенсионного страхования;

3.6.5. идентификационный номер налогоплательщика;

3.6.6. идентификатор (ORCID, WOS Research ID, Scopus Author ID , ID РИНЦ);

3.7. В случаях, предусмотренных пунктом 3.5 настоящего Положения, согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом. Форма письменного согласия работника на обработку его персональных данных приведена в Приложении № 6 к настоящему Положению.

3.8. Обработка персональных данных сотрудников Института, граждан, претендующих на замещение должностей Института, лиц, замещающих должности руководителей подразделений Института, а также граждан, претендующих на замещение должностей руководителей подразделений Института, осуществляется Отделом кадров Института и 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, а также сбор, запись, преобразование, хранение и использование биометрических персональных данных.

3.9. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных Института, граждан, претендующих на замещение должностей Института, лиц, замещающих должности руководителей подразделений Института, а также граждан, претендующих на замещение должностей руководителей подразделений Института, осуществляется путем:

3.9.1. получения для ознакомления оригиналов документов, необходимых для идентификации личности сотрудника, составления или расторжения трудового договора (эффективного контракта) и оформления и ведения личного дела сотрудника, в соответствии с действующим трудовым и пенсионным законодательством (заявление о приеме на работу, паспорт, трудовая книжка, автобиография, иные документы, предоставляемые в Отдел кадров);

3.9.2. внесения сведений в учетные формы (на бумажных и электронных носителях);

3.9.3. формирования персональных данных в ходе кадровой работы;

3.9.4. внесения персональных данных в информационные системы, используемые кадровым подразделением Института;

3.9.5. фотографирования субъекта персональных данных и (или) сканирования папиллярных узоров пальцев рук специализированными техническими средствами для внесения шаблонов в информационную систему контроля управления доступом.

3.10. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от граждан, претендующих на замещение должностей Института, лиц, замещающих должности руководителей подразделений Института, а также граждан, претендующих на замещение должностей руководителей подразделений Института.

3.11. В случае возникновения необходимости получения персональных данных лиц, замещающих должности руководителей подразделений Института, у третьей стороны, следует известить об этом сотрудника либо лицо, замещающее должность руководителя подразделения Института заранее, получить их письменное согласие и сообщить им о целях, предполагаемых источниках и способах получения персональных данных.

3.12. Запрещается получать, обрабатывать и приобщать к личному делу сотрудника Института и лица, замещающего должность руководителя подразделения Института персональные данные, не предусмотренные пунктом

3.2 настоящего Положения, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

3.13. При сборе персональных данных сотрудник кадрового подразделения, осуществляющий сбор (получение) персональных данных непосредственно от граждан, претендующих на замещение должностей Института, лиц, замещающих должности руководителей подразделений Института, а также граждан, претендующих на замещение должностей руководителей подразделений Института, обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные, включая невозможность прохождения в контролируемые зоны Института при отказе от предоставления биометрических данных.

3.14. Передача (распространение, предоставление) и использование персональных данных граждан, претендующих на замещение должностей Института, лиц, замещающих должности руководителей подразделений Института, а также граждан, претендующих на замещение должностей руководителей подразделений Института, осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

4. Порядок обработки персональных данных третьих лиц в связи с предоставлением услуг и осуществлением уставной деятельности Института

4.1. В Институте обработка персональных данных третьих лиц осуществляется в целях предоставления следующих услуг и осуществления следующих видов уставной деятельности:

4.1.1. Для пропуска физических лиц — сотрудников сторонних организаций, для выполнения работ или оказания услуг, на основании заключенных договоров. С этой целью осуществляется обработка следующих персональных данных указанных лиц:

4.1.1.1. фамилия, имя, отчество;

4.1.1.2. номер контактного телефона или сведения о других способах связи;

4.1.1.3. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

4.1.1.4. автомобиль (номер, модель);

4.1.1.5. изображение лица (фотография) для разового пропуска.

4.1.2. Для приема проб биологического материала пациентов медицинских учреждений, для исследования и выдачи результатов исследований, по заявкам медицинских учрежде-

ний или на основании договоров с медицинскими учреждениями. С этой целью осуществляется обработка следующих персональных данных указанных лиц:

4.1.2.1. фамилия, имя, отчество, дата рождения;

4.1.2.2. номер контактного телефона или сведения о других способах связи;

4.1.2.3. вид, серия, номер документа, удостоверяющего личность, наименование органа выдавшего его, дата выдачи;

4.1.2.4. адрес регистрации по месту жительства или месту пребывания;

4.1.2.5. номер страхового медицинского полиса;

4.1.2.6. страховой номер индивидуального лицевого счета в системах обязательного пенсионного страхования и обязательного социального страхования (СНИЛС);

4.1.2.7. вид биоматериала;

4.1.2.8. диагноз;

4.1.2.9. наименование медучреждения отбора проб и приема ответа.

4.2. Обработка персональных данных, для целей, указанных в пунктах

4.1.2 настоящего Положения, осуществляется без согласия субъектов персональных данных в соответствии с пунктом 5 части 1 статьи 6 Федерального закона «О персональных данных».

4.3. Обработка персональных данных, для целей, указанных в пунктах

4.1.3 настоящего Положения, осуществляется без согласия субъектов персональных данных в соответствии с пунктом 4 части 1 статьи 6 Федерального закона «О персональных данных».

4.4. Обработка персональных данных, необходимых в связи с предоставлением услуг и осуществлением уставной деятельности, указанных в пункте 4.1 настоящего Положения, осуществляется структурными подразделениями Института, предоставляющими соответствующие услуги, и 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.

4.5. Действия с персональными данными, указанные в пункте

4.4 настоящего Положения, осуществляются лишь в случаях и в порядке, предусмотренных федеральными законами.

5. Порядок обработки персональных данных субъектов персональных данных в информационных системах

5.1. Обработка персональных данных в Институте осуществляется:

5.1.1. В «Информационной системе персональных данных Роспотребнадзор»;

5.1.2. На аттестованных под обработку персональных данных автоматизированных рабочих местах, входящих в состав «Единой информационной системы Роспотребнадзор»;

- 5.1.3. В информационной системе «1С: Предприятие 8»;
- 5.1.4. На автоматизированных рабочих местах сотрудников кадрового подразделения Института;
- 5.1.5. В информационной системе контроля и управления доступом (биометрическая система распознавания лиц и отпечатков пальцев);
- 5.1.6. На портативных средствах вычислительной техники (ноутбуки, защищенные смартфоны), учет которых ведется в Журнале (Приложение № 12).
- 5.1.7. Без применения аппаратно-вычислительных средств (на бумажных носителях) – в отношении персональных данных третьих лиц, обратившихся в Институт за оказанием услуги (медпункт).
- 5.2. «Информационная система персональных данных Роспотребнадзор» (далее — ИСПДн «Роспотребнадзор») содержит персональные данные Института, субъектов (заявителей), обратившихся в Институт в целях получения услуг или в связи с осуществлением уставной деятельности, и включает:
- 5.2.1. персональный идентификатор;
 - 5.2.2. фамилию, имя, отчество субъекта персональных данных;
 - 5.2.3. вид документа, удостоверяющего личность субъекта персональных данных;
 - 5.2.4. серию и номер документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе;
 - 5.2.5. адрес места жительства субъекта персональных данных;
 - 5.2.6. почтовый адрес субъекта персональных данных;
 - 5.2.7. контактный телефон, факс (при наличии) субъекта персональных данных;
 - 5.2.8. адрес электронной почты субъекта персональных данных;
 - 5.2.9. идентификационный номер налогоплательщика субъекта персональных данных.
- 5.3. Аттестованные в соответствии с законодательством Российской Федерации под обработку персональных данных автоматизированные рабочие места, входящие в состав «Единой информационной системы Роспотребнадзор» (далее — АРМ ЕИС Роспотребнадзор), включают персональные данные субъектов, получаемые сотрудниками Института в рамках предоставления государственных услуг и исполнения государственных функций, и включают:
- 5.3.1. персональный идентификатор;
 - 5.3.2. адрес места жительства субъекта персональных данных;
 - 5.3.3. почтовый адрес субъекта персональных данных;
 - 5.3.4. телефон субъекта персональных данных;
 - 5.3.5. адрес электронной почты субъекта персональных данных.

5.4. Информационная система «1С: Предприятие 8» и прикладные программные подсистемы «АКСИОК» и «1С Бухгалтерия», содержат персональные данные сотрудников Института и физических лиц, являющихся стороной гражданско-правовых договоров, заключаемых Институтом, и включает:

- 5.4.1. фамилию, имя, отчество субъекта персональных данных;
- 5.4.2. дату рождения субъекта персональных данных;
- 5.4.3. место рождения субъекта персональных данных;
- 5.4.4. реквизиты основного документа, удостоверяющего личность субъекта персональных данных;
- 5.4.5. адрес места жительства субъекта персональных данных;
- 5.4.6. почтовый адрес субъекта персональных данных;
- 5.4.7. телефон субъекта персональных данных;
- 5.4.8. идентификационный номер налогоплательщика субъекта персональных данных;
- 5.4.9. табельный номер субъекта персональных данных;
- 5.4.10. должность субъекта персональных данных;
- 5.4.11. номер приказа и дату приема на работу (увольнения) субъекта персональных данных.

5.5. Автоматизированные рабочие места сотрудников кадрового подразделения Института предполагают обработку персональных данных сотрудников Института, предусмотренных пунктом 3.2 настоящего Положения.

5.6. Классификация информационных систем персональных данных, указанных в пункте «Классификация ИСПДн Института осуществляется комиссией (согласно Приложению № 2 к настоящему Положению) с составлением Акта определения уровня защищенности».

5.7. Государственным служащим структурных подразделений Института, имеющим право осуществлять обработку персональных данных в информационных системах Института, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными регламентами Института. Информация может вноситься как в автоматическом режиме, при получении персональных данных с Единого портала государственных услуг или официального сайта Роспотребнадзор и других сайтов, так и в ручном режиме, при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

5.8. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных Института, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

- 5.8.1. определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных Института;
- 5.8.2. применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Института, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- 5.8.3. применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;
- 5.8.4. оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- 5.8.5. учет машинных носителей персональных данных;
- 5.8.6. обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- 5.8.7. восстановление персональных данных, модифицированных удаленных или уничтоженных вследствие несанкционированного доступа к ним;
- 5.8.8. установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных Института, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных Института;
- 5.8.9. структурное подразделение Института, ответственное за информационную безопасность, обеспечивает периодический контроль работоспособности средств защиты информации. Результаты проверок фиксируются в Журнале учета периодического тестирования (Приложение № 13);
- 5.8.10. применение сертифицированных средств криптографической защиты информации при передаче биометрических персональных данных между терминалами сбора данных и центральным сервером информационной системы контроля управления доступом;
- 5.8.11. учет применяемых средств защиты информации, их типов, сертификатов соответствия и мест установки осуществляется ответственным подразделением в Журнале учета средств защиты информации (Приложение № 14);
- 5.8.12. использование антивирусного программного обеспечения и межсетевых экранов для предотвращения внедрения вредоносного кода, способного перехватывать биометрические шаблоны;
- 5.8.13. проведение периодического контроля состояния уровня защищенности информационных систем персональных данных. Результаты проверок, устранения уязвимостей и выполнения плана мероприятий подлежат обязательной фиксации в Журнале учета мероприятий по контролю (Приложение № 15).
- 5.9. Структурное подразделение Института, ответственное за наполнение сайта/баз данных, организует ведение учета всех машинных носителей информации. Учет ведется в Журнале учета машинных носителей информации (Приложение № 11).

5.10. Структурное подразделение Института, ответственное за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных Института, должно обеспечить: 5.10.1. своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до ответственного за организацию обработки персональных данных в Институте и руководителя Института;

5.10.2. недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

5.10.3. возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5.10.4. постоянный контроль за обеспечением уровня защищенности персональных данных;

5.10.5. знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

5.10.6. учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

5.10.7. при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы персональных данных до выявления причин нарушений и устранения этих причин;

5.10.8. разбирательство 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 опасных последствий подобных нарушений.

5.11. Структурное подразделение Института, ответственное за обеспечение функционирования информационных систем персональных данных, принимает все необходимые меры по восстановлению персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним.

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

5.13. Доступ сотрудников Института к персональным данным, находящимся в информационных системах персональных данных Института, предусматривает обязательное прохождение процедуры идентификации и аутентификации, которая может осуществляться в том числе посредством биометрической идентификации.

5.14. В случае выявления нарушений порядка обработки персональных данных в информационных системах персональных данных Института уполномоченными должностными

лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

6. Порядок обработки персональных данных без использования средств автоматизации

6.1. Обработка персональных данных считается осуществленной без использования средств автоматизации (неавтоматизированной), если обработка персональных данных осуществляется без помощи средств вычислительной техники.

6.2. Обработка персональных данных без использования средств автоматизации осуществляется на законной и справедливой основе. Обработка персональных данных без использования средств автоматизации не может быть использована Институтом или его работниками в целях причинения материального и морального вреда субъектам персональных данных, затруднения реализации их прав и свобод.

6.3. Обработка персональных данных без использования средств автоматизации осуществляется в соответствии с требованиями «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 года номер 687.

6.4. В Институте без использования средств автоматизации обрабатываются персональные данные работников, соискателей и контрагентов. Обрабатываемые категории персональных данных для различных категорий субъектов установлены в главах три и четыре настоящего Положения соответственно.

6.5. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации их на отдельных материальных носителях информации (далее — материальные носители), в специальных разделах или на полях форм (бланков).

6.6. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

6.7. К обработке персональных данных без использования средств автоматизации допускаются только те работники, которые указаны в утвержденных Директором Института перечнях лиц, допущенных к обработке персональных данных.

6.8. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, подписывают соглашение о неразглашении и обязательство по обеспечению безопасности при работе со средствами вычислительной техники (по форме Приложения № 5 к настоящему Положению).

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

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

6.9.2. 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;

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

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

6.9.5. в случае, если типовая форма используется для сбора биометрических данных (например, анкета с местом для фотографии, используемой для идентификации), она должна содержать отдельное поле для получения письменного согласия именно на обработку биометрических персональных данных.

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

6.10.1. форма журнала является приложением к настоящему Положению и содержит сведения о цели обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых способов обработки персональных данных;

6.10.2. копирование содержащейся в журнале информации не допускается;

6.10.3. персональные данные каждого субъекта персональных данных могут заноситься в журнал не более одного раза в каждом случае пропуска субъекта персональных данных на территорию Института;

6.10.4. журналы учета посетителей, содержащие фотографии (биометрические данные), подлежат хранению в сейфах или запираемых шкафах в подразделении режима.

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

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

6.11.2. 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, не подлежащих уничтожению или блокированию;

6.11.3. при хранении материальных носителей, содержащих биометрические данные, обеспечивается использование отдельных конвертов или файлов, исключающих механическое повреждение поверхности носителя.

6.12. Для уничтожения персональных данных на материальных носителях в Институте утверждается состав комиссии по уничтожению персональных данных.

6.13. 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 изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

6.14. С целью обеспечения безопасности персональных данных при их обработке без использования средств автоматизации приказом директора Института определены места хранения персональных данных, а также назначены ответственные за обеспечение конфиденциальности персональных данных при их хранении.

6.15. Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях (разные места хранения для разных категорий субъектов персональных данных).

6.16. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

7. Обработка персональных данных в рамках межведомственного информационного взаимодействия с применением единой системы межведомственного электронного взаимодействия

7.1. Институт, в соответствии с законодательством Российской Федерации, осуществляет обработку персональных данных в рамках межведомственного электронного информационного взаимодействия в электронном виде с федеральными органами государственной власти с применением единой системы межведомственного электронного взаимодействия (далее — СМЭВ).

7.2. Институт в рамках СМЭВ на основании поступивших межведомственных запросов направляет информацию, включающую персональные данные субъектов, обрабатываемые в Институте, в следующие федеральные органы исполнительной власти:

7.2.1. в Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации — фамилию, имя, отчество, идентификационный номер налогоплательщика владельца лицензии на осуществление деятельности по оказанию услуг связи;

7.2.2. в Министерство внутренних дел Российской Федерации — для проверки кандидатов при приеме на работу и действующих сотрудников (в рамках периодических проверок): фамилию, имя, отчество, дату рождения, серию и номер документа, удостоверяющего личность, — в целях запроса сведений о наличии (отсутствии) судимости и фактов уголовного преследования, а также сведений об административных правонарушениях.

7.2.3. в Федеральное агентство по печати и массовым коммуникациям, Федеральную таможенную службу — фамилию, имя, отчество учредителя средства массовой информации.

7.3. Институт в рамках СМЭВ вправе направить межведомственные запросы о предоставлении информации, включающей персональные данные субъектов, в следующие федеральные органы исполнительной власти:

7.3.1. в Федеральную налоговую службу — о предоставлении информации из Единого государственного реестра юридических лиц и Единого государственного реестра индивидуальных предпринимателей (сведения об учредителях — физических лицах);

7.3.2. в Федеральную службу государственной регистрации, кадастра и картографии — о предоставлении информации из Единого государственного реестра прав на недвижимое имущество в отношении правообладателей (фамилия, имя, отчество, дата рождения, серия и номер основного документа, удостоверяющего личность, место рождения, адрес места жительства, гражданство);

7.3.3. в Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий — о предоставлении фамилии, имени, отчества судовладельца.

7.4. Обработка персональных данных также осуществляется Институтом при осуществлении электронного взаимодействия с федеральными государственными унитарными предприятиями радиочастотной службы в рамках полномочий, предусмотренных законодательством Российской Федерации.

8. Сроки обработки и хранения персональных данных

8.1. Сроки обработки и хранения персональных данных Института, граждан, претендующих на замещение должностей Института, лиц, замещающих должности руководителей подразделений Института, а также граждан, претендующих на замещение должностей руководителей подразделений Института, определяются в соответствии с законодательством Российской Федерации. С учетом положений законодательства Российской Федерации устанавливаются следующие сроки обработки и хранения персональных данных сотрудников Института:

8.1.1. Персональные данные, содержащиеся в приказах по личному составу Института (о приеме, о переводе, об увольнении, об установлении надбавок), подлежат хранению в кад-

ровом подразделении Института в течение двух лет, с последующим формированием и передачей указанных документов в архив Института или государственный архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение семидесяти пяти лет.

8.1.2. Персональные данные, содержащиеся в личных делах сотрудников Института, а также личных карточках сотрудников Института, хранятся в кадровом подразделении Института в течение десяти лет, с последующим формированием и передачей указанных документов в архив Института или государственный архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение семидесяти пяти лет.

8.1.3. Персональные данные, содержащиеся в приказах о поощрениях, материальной помощи Института, подлежат хранению в течение двух лет в кадровом подразделении Института с последующим формированием и передачей указанных документов в архив Института или государственный архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение семидесяти пяти лет.

8.1.4. Персональные данные, содержащиеся в приказах о предоставлении отпусков, о командировках, о дисциплинарных взысканиях, подлежат хранению в кадровом подразделении Института в течение пяти лет с последующим уничтожением.

8.1.5. Персональные данные, содержащиеся в документах претендентов на замещение вакантной должности государственной службы в Институте, не допущенных к участию в конкурсе, и кандидатов, участвовавших в конкурсе, хранятся в кадровом подразделении Института в течение трех лет со дня завершения конкурса, после чего подлежат уничтожению.

8.2. Сроки обработки и хранения персональных данных, предоставляемых субъектами персональных данных в Институт в связи с получением государственных услуг и осуществлением Институту уставной деятельности, указанных в пункте 4.1 настоящего Положения, определяются нормативными правовыми актами, регламентирующими порядок их сбора и обработки.

8.3. Персональные данные граждан, обратившихся в Институт лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, хранятся в течение пяти лет, после чего подлежат уничтожению.

8.4. Персональные данные, предоставляемые субъектами на бумажном носителе в связи с предоставлением Институту услуг и осуществлением уставной деятельности, хранятся на бумажных носителях в структурных подразделениях Института, к полномочиям которых относится обработка персональных данных в связи с предоставлением соответствующей услуги, согласно утвержденным положениям о соответствующих структурных подразделениях Института.

8.5. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

8.6. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях, определен-

ных настоящим Положением. 8.7. Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, осуществляют руководители структурных подразделений Института.

8.8. Срок хранения персональных данных, внесенных в информационные системы персональных данных, указанные в пункте 5.1 настоящего Положения, должен соответствовать сроку хранения бумажных оригиналов.

8.9. Биометрические персональные данные сотрудников, содержащиеся в информационной системе контроля управления доступом, хранятся до момента прекращения трудового договора, после чего подлежат гарантированному удалению в течение тридцати календарных дней.

9. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

9.1. Структурным подразделением Института, ответственным за документооборот и архивирование, осуществляется систематический контроль и выделение документов, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению.

9.2. Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается на заседании экспертной комиссии Института, состав которой утверждается приказом по Институту. 9.3. По итогам заседания комиссии составляются протокол и Акт о выделении к уничтожению документов, опись уничтожаемых дел, проверяется их комплектность, акт подписывается председателем и членами комиссии и утверждается руководителем Института.

9.4. Институт в порядке, установленном законодательством Российской Федерации, определяется подрядная организация, имеющая необходимую производственную базу для обеспечения установленного порядка уничтожения документов.

9.5. Должностное лицо Института, ответственное за архивную деятельность, сопровождает документы, содержащие персональные данные, до производственной базы подрядчика и присутствует при процедуре уничтожения документов (сжигание или химическое уничтожение).

9.6. По окончании процедуры уничтожения подрядчиком и должностным лицом Института, ответственным за архивную деятельность, составляется соответствующий Акт об уничтожении документов, содержащий подписи всех членов комиссии.

9.7. Уничтожение по окончании срока обработки персональных данных на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации, включая многократную перезапись секторов памяти, где хранились биометрические шаблоны.

10. Рассмотрение запросов субъектов персональных данных или их представителей

10.1. Сотрудники Института, граждане, претендующие на замещение должностей Института и подавшие документы на участие в конкурсе, а также граждане, персональные данные которых обрабатываются в Институте в связи осуществлением Институтом уставной деятельности, имеют право на получение информации, касающейся обработки их персональных данных, в том числе содержащей:

10.1.1. подтверждение факта обработки персональных данных Институтом;

10.1.2. правовые основания и цели обработки персональных данных;

10.1.3. применяемые в Институте способы обработки персональных данных;

10.1.4. наименование и место нахождения Института, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Институтом или на основании федерального закона;

10.1.5. сроки обработки и хранения персональных данных;

10.1.6. порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных данных;

10.1.7. информацию об осуществленной или предполагаемой трансграничной передаче данных;

10.1.8. наименование организации или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Института;

10.1.9. иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.

10.2. Лица, указанные в пункте 10.1 настоящего Положения (далее — субъекты персональных данных), вправе требовать от Института уточнения их 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.

10.3. Сведения, указанные в подпунктах 10.1.1 — 10.1.9 настоящего Положения, должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

10.4. Запрос субъекта персональных данных должен содержать реквизиты основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения, подтверждающие участие субъекта в правоотношениях с Институтом, 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.

10.5. В случае, если сведения, указанные в подпунктах 10.1.1 — 10.1.9 настоящего Положения, были предоставлены субъекту по его запросу, субъект вправе обратиться повторно не ранее чем через тридцать дней. Факт поступления обращения и результат его рассмот-

рения подлежат обязательной регистрации в Журнале учета обращений граждан-субъектов персональных данных (Приложение № 9 к настоящему Положению).

10.6. Субъект персональных данных вправе обратиться повторно в Институт до истечения тридцатидневного срока, если предоставил обоснование направления повторного запроса.

10.7. Институт вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 10.5 и 10.6 настоящего Положения. Такой отказ должен быть мотивированным.

10.8. 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.

11. Лицо, ответственное за организацию обработки персональных данных в Институте

11.1. Ответственный за организацию обработки персональных данных в Институте назначается руководителем Института из числа сотрудников Института, в соответствии с распределением обязанностей.

11.2. Ответственный за обработку персональных данных Института в своей работе руководствуется законодательством Российской Федерации в области персональных данных и настоящим Положением.

11.3. Ответственный за обработку персональных данных Института обязан:

11.3.1. организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых в Институте от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения;

11.3.2. осуществлять внутренний контроль за соблюдением сотрудниками Института требований законодательства Российской Федерации в области персональных данных;

11.3.3. доводить до сведения сотрудников Института положения законодательства Российской Федерации в области персональных данных и настоящего Положения;

11.3.4. организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей;

11.3.5. в случае нарушения в Институте требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

11.4. Ответственный за обработку персональных данных вправе:

11.4.1. иметь доступ к информации, касающейся обработки персональных данных в Институте, включая цели обработки, категории обрабатываемых данных, правовые основания, перечень действий с персональными данными, описание мер, предусмотренных статьями восемнадцать точка один и девятнадцать Федерального закона «О персональных данных», дату начала обработки, срок или условия прекращения обработки;

11.4.2. привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, сотрудников Института с возложением на них соответствующих обязанностей и закреплением ответственности.

11.5. Ответственный за обработку персональных данных в Институте несет ответственность за надлежащее выполнение возложенных функций по организации обработки персональных данных.

12. Порядок доступа в помещения, в которых ведется обработка персональных данных

12.1. В помещения, в которых ведется обработка персональных данных, допускаются сотрудники Института, в должностные обязанности которых входит обработка персональных данных (далее — защищаемая информация) либо осуществление доступа к защищаемой информации, а также субъекты персональных данных в соответствии со статьей четырнадцать Федерального закона от 27 июля 2006 года номер 152-ФЗ «О персональных данных».

12.2. Доступ в помещения, в которых ведется обработка персональных данных, осуществляется на основании списка федеральных государственных служащих, допущенных к работе в указанных помещениях (далее — список допущенных лиц), утвержденного директором Института.

12.3. Если в помещении ведется обработка персональных данных несколькими лицами, то в списке допущенных лиц указывается сотрудник Института, ответственный за данное помещение. 12.4. При изменении кадрового состава подразделения руководитель этого подразделения вносит изменения в список допущенных лиц.

12.5. Пребывание в помещениях, в которых ведется обработка персональных данных, лиц, не допущенных к работе в данном помещении, разрешается только в присутствии сотрудников, имеющих допуск к работе в этом помещении.

12.6. Установка нового оборудования, его замена или ремонт в помещениях, в которых ведется обработка персональных данных, проводится по согласованию с начальником подразделения, ответственным за обеспечение информационной безопасности.

12.7. Список допущенных лиц доводится до сотрудников Института под подпись.

12.8. Выдача ключей для вскрытия защищаемых помещений и прием этих помещений под охрану осуществляются на основании списка допущенных лиц.

12.9. При работе в защищаемых помещениях двери этих помещений должны быть закрыты.

12.10. В рабочее и нерабочее время при временном отсутствии ответственных лиц помещения должны закрываться на ключ.

12.11. Директор Института беспрепятственно допускается в любые защищаемые помещения.

12.12. Сотрудники Института, допущенные к работе в защищаемых помещениях, должны соблюдать условия, обеспечивающие сохранность защищаемой информации и исключать несанкционированный доступ к ней.

13. **Виды ответственности за нарушения в сфере обработки персональных данных**

В Российской Федерации за нарушения в сфере обработки персональных данных предусмотрена уголовная, административная и гражданско-правовая ответственность.

13.1. Статья девяносто Трудового кодекса Российской Федерации от 30 декабря 2001 года номер 197-ФЗ. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника: Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном настоящим Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

13.2. Статья восемьдесят один Трудового кодекса Российской Федерации от 30 декабря 2001 года номер 197-ФЗ. Расторжение трудового договора по инициативе работодателя: Трудовой договор может быть расторгнут работодателем в случаях: пункт шесть — однократного грубого нарушения работником трудовых обязанностей: подпункт «в» — разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника.

13.3. Статья двадцать четыре Федерального закона от 27 июля 2006 года номер 152-ФЗ «О персональных данных». Ответственность за нарушение требований настоящего Федерального закона:

1. Лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.
2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, подлежит возмещению в соответствии с законодательством Российской Федерации независимо от возмещения имущественного вреда.

13.4. Статья 13.11 Кодекса Российской Федерации об административных правонарушениях от 30 декабря 2001 года № 195-ФЗ (в редакции Федерального закона от 30.11.2024 № 420-ФЗ). Нарушение законодательства Российской Федерации в области персональных данных:

1. Нарушение правил обработки (ч. 1 ст. 13.11 КоАП РФ): Обработка персональных данных в случаях, не предусмотренных законодательством, либо обработка, несовместимая с целями сбора, влечет наложение административного штрафа на должностных лиц — от пятидесяти тысяч до ста тысяч рублей; на юридических лиц — от ста пятидесяти тысяч до трехсот тысяч рублей. Повторное совершение данного правонарушения влечет штраф на должностных лиц от двадцати тысяч до пятидесяти тысяч рублей; на юридических лиц — от трехсот тысяч до пятисот тысяч рублей.

2. Отсутствие согласия или нарушение требований к нему (ч. 2 ст. 13.11 КоАП РФ): Обработка персональных данных без согласия субъекта в письменной форме (когда оно обязательно) либо оформление согласия с нарушениями требований закона влечет наложение административного штрафа на должностных лиц — от ста тысяч до трехсот тысяч

рублей; на юридических лиц — от трехсот тысяч до семисот тысяч рублей. Повторное нарушение влечет штраф на должностных лиц от сорока тысяч до ста тысяч рублей; на индивидуальных предпринимателей — от пятисот тысяч до одного миллиона рублей; на юридических лиц — от одного миллиона до полутора миллионов рублей.

3. Обработка биометрических данных без согласия (ч. 11 ст. 13.11 КоАП РФ): Обработка биометрических персональных данных без письменного согласия субъекта влечет наложение административного штрафа на должностных лиц — от пятидесяти тысяч до ста тысяч рублей; на юридических лиц — от трехсот тысяч до пятисот тысяч рублей.

4. Неопубликование политики (ч. 3 ст. 13.11 КоАП РФ): Невыполнение обязанности по опубликованию или обеспечению доступа к настоящему Положению о защите персональных данных влечет наложение административного штрафа на должностных лиц — от шести тысяч до двенадцати тысяч рублей; на юридических лиц — от тридцати тысяч до шестидесяти тысяч рублей.

5. Невыполнение требования об уточнении/блокировке (ч. 5 ст. 13.11 КоАП РФ): Невыполнение требования субъекта или Роскомнадзора об уточнении, блокировании или уничтожении неточных/незаконных данных влечет штраф на должностных лиц — от восьми тысяч до двадцати тысяч рублей; на юридических лиц — от пятидесяти до девяноста тысяч рублей.

6. Нарушение локализации баз данных (ч. 8 ст. 13.11 КоАП РФ): Невыполнение обязанности по обеспечению записи, систематизации и хранения персональных данных граждан РФ с использованием баз данных, находящихся на территории Российской Федерации, влечет наложение административного штрафа на должностных лиц — от ста тысяч до двухсот тысяч рублей; на юридических лиц — от одного миллиона до шести миллионов рублей. Повторное нарушение — от пятидесяти тысяч до восьмисот тысяч рублей (должн. лица) и от шести до восемнадцати миллионов рублей (юрлица).

7. Утечка данных (новое основание с 30 мая 2025 г., ч. 12–14 ст. 13.11 КоАП РФ):

- Неправомерная передача данных от 1 000 до 10 000 субъектов: штраф на юрлиц от 3 до 5 миллионов рублей.
- От 10 000 до 100 000 субъектов: штраф от 5 до 10 миллионов рублей.
- Более 100 000 субъектов: штраф от 10 до 15 миллионов рублей.
- Повторная утечка: штраф от 1% до 3% совокупной выручки организации за год, но не менее 20 миллионов рублей и не более 500 миллионов рублей.

8. Утечка биометрии (новое основание с 30 мая 2025 г., ч. 17 ст. 13.11 КоАП РФ): Действия, повлекшие неправомерную передачу биометрических данных, влекут наложение административного штрафа на юридических лиц в размере от пятнадцати миллионов до двадцати миллионов рублей.

9. Уголовная ответственность (ст. 272 УК РФ): Неправомерный доступ к компьютерной информации (включая базы данных Института), если это деяние повлекло копирование, модификацию или уничтожение информации, наказывается штрафом до двухсот тысяч рублей, исправительными работами либо лишением свободы на срок до двух лет. При наличии корыстной заинтересованности или причинении крупного ущерба — лише-

ние свободы на срок до четырех лет. Если деяние совершено группой лиц — до семи лет лишения свободы.

13.5. Статья сто тридцать семь Уголовного кодекса Российской Федерации от 13 июня 1996 года номер 63-ФЗ. Нарушение неприкосновенности частной жизни:

1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, за исключением случаев, предусмотренных статьей 272.1 настоящего Кодекса, -

наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

2. Те же деяния, совершенные лицом с использованием своего служебного положения, -

наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо принудительными работами на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового, либо арестом на срок до шести месяцев, либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

3. Незаконное распространение в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего, или психическое расстройство несовершеннолетнего, или иные тяжкие последствия, -

наказывается штрафом в размере от ста пятидесяти тысяч до трехсот пятидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период от восемнадцати месяцев до трех лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от трех до пяти лет, либо принудительными работами на срок до пяти лет с лишением пра-

ва занимать определенные должности или заниматься определенной деятельностью на срок до шести лет или без такового, либо арестом на срок до шести месяцев, либо лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до шести лет.

13.6. Статья двести семьдесят два Уголовного кодекса Российской Федерации от 13 июня 1996 года номер 63-ФЗ. Неправомерный доступ к компьютерной информации:

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, наказывается штрафом, исправительными работами или лишением свободы.
2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, наказывается штрафом, принудительными работами или лишением свободы.
3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой, наказываются лишением свободы.
4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, наказываются лишением свободы. Примечания:
5. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.
6. Крупным ущербом признается ущерб, сумма которого превышает один миллион рублей.