Приложение 2
к Приказу № 266А
от «13» сентября 2016 г.

УТВЕРЖДАЮ

И.о. ректора
Российского химико-
технологического университета
имени Д.И. Менделеева

_____ Е.В. Юртов

«___» _сентября_____ 2016 г.

ПОЛОЖЕНИЕ

**об обработке и защите персональных данных
в информационных системах персональных данных
Российского химико-технологического университета
имени Д.И. Менделеева**

2016 г.

Содержание

Список принятых сокращений и обозначений

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.

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

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

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

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

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

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.

1. Область применения

1.1. Положение об обеспечении безопасности персональных данных (далее – Положение) в информационных системах персональных данных Российского химико-технологического университета имени Д.И. Менделеева (далее – Учреждение) разработано в целях выполнения требований законодательства Российской Федерации в области защиты персональных данных.

1.2. Настоящее Положение определяет порядок и правила организации и проведения работ по обеспечению безопасности персональных данных в ИСПДн Учреждения.

1.3. Настоящий документ учитывает положения основных нормативных правовых актов в области защиты персональных данных, а именно:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

1.3.1. Нормативных актов ФСТЭК России:

- «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной Заместителем Директора ФСТЭК России 15 февраля 2008 г.;
- «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной Заместителем Директора ФСТЭК России 14 февраля 2008 г.
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3.2. Нормативных актов ФСБ России:

- «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную

тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622;

- «Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденных руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/54-144.
- Приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

1.4. Настоящее Положение предназначено для всех работников Учреждения, доступ которых к ИСПДн необходим для выполнения трудовых обязанностей, а также для лиц, получающих временный доступ к обрабатываемым в ИСПДн Учреждения ПДн на законном основании.

1.5. Настоящее Положение вступает в силу с момента его утверждения И.о. ректора Учреждения и действует до замены его новым Положением.

1.6. Плановая актуализация настоящего Положения проводится не реже раза в год. Внеплановая актуализация проводится при возникновении одного из следующих условий:

1) изменение целей и/или состава обрабатываемых персональных данных;

2) возникновение условий, существенно влияющих на процессы обработки персональных данных и не регламентированных настоящим документом;

3) по результатам контрольных мероприятий и проверок контролирующих органов исполнительной власти Российской Федерации, выявивших несоответствия требованиям по обеспечению безопасности ПДн;

4) при появлении новых требований к обеспечению безопасности ПДн со стороны российского законодательства и контролирующих органов исполнительной власти Российской

Федерации.

1.7. Ответственным за пересмотр настоящего Положения и составление рекомендаций по изменению является работник, ответственный за обеспечение безопасности ПДн.

1.8. Внесение изменений в настоящее Положение производится на основании соответствующего приказа, который утверждает И.о. ректора Учреждения.

2. Общие положения

2.1. Учреждение является оператором ПДн.

2.2. В ИСПДн Учреждения осуществляется обработка ПДн следующих категорий субъектов ПДн: работников Учреждения; абитуриентов и студентов.

2.3. Обработка ПДн в Учреждении проводится с целью и в сроки, указанные в Политике обработки ПДн.

2.4. В Учреждении обработка ПДн осуществляется с использованием средств автоматизации и без использования таких средств.

2.5. Сроки хранения ПДн определяются в соответствии со сроками, устанавливаемыми законодательством и указаны в Политике обработки ПДн.

3. Организация работ по обеспечению безопасности персональных данных

3.1. Под организацией работ по обеспечению безопасности ПДн понимается формирование и всестороннее обеспечение реализации совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию как непосредственного, так и опосредованного ущерба от реализации угроз безопасности ПДн, и осуществляемых в целях:

- предотвращения возможных (потенциальных) угроз безопасности ПДн;
- нейтрализации и/или парирования реализуемых угроз безопасности ПДн;
- ликвидации последствий реализации угроз безопасности ПДн.

3.2. Организация работ по обеспечению безопасности ПДн в ИСПДн Учреждения должна осуществляться в соответствии с действующими нормативными правовыми актами и разработанными для этих целей организационно-распорядительными документами по защите ПДн в Учреждении.

3.3. Задачи по приведению ИСПДн Учреждения в соответствие с требованиями законодательства Российской Федерации в области защиты ПДн возлагаются на специально создаваемую для этих целей комиссию.

3.4. В случаях, когда Учреждение на основании договора поручает обработку ПДн, обрабатываемых в ИСПДн Учреждения, другому лицу/сторонней организации, необходимо выполнить одно из следующих условий:

- в тексте договора в требованиях к контрагенту прописать обязанность обеспечения контрагентом безопасности и конфиденциальности ПДн;
- в случае невозможности или нецелесообразности изменения текста договора оформить дополнительное соглашение к договору или соглашение о конфиденциальности, в которых прописать обязанность обеспечения контрагентом конфиденциальности персональных данных и безопасности ПДн при их обработке.

3.5. Работы по приведению ИСПДн Учреждения в соответствие с требованиями законодательства Российской Федерации ведутся по двум направлениям: обеспечение безопасности ПДн, обрабатываемых без использования средств автоматизации, и обеспечение безопасности ПДн в ИСПДн Учреждения.

3.6. Работы по обеспечению безопасности ПДн, обрабатываемых без использования средств автоматизации, ведутся по следующим направлениям:

- определение перечня лиц, осуществляющих обработку ПДн в ИСПДн Учреждения;
- информирование работников Учреждения об установленных правилах обработки ПДн и требований по их защите, повышение осведомленности в вопросах обеспечения безопасности ПДн;
- учет и защита носителей ПДн;
- разграничение доступа к ресурсам ПДн.

3.7. Организация и выполнение мероприятий по обеспечению безопасности ПДн, обрабатываемых в ИСПДн Учреждения, осуществляются в рамках системы защиты персональных данных ИСПДн (далее - СЗПДн), развертываемой в ИСПДн Учреждения в процессе ее создания или модернизации.

3.8. СЗПДн ИСПДн представляет собой совокупность организационных мер и технических средств защиты информации, а также используемых в ИСПДн информационных технологий, функционирующих в соответствии с определенными целями и задачами обеспечения безопасности ПДн.

3.9. Система защиты ПДн должна являться неотъемлемой составной частью каждой вновь создаваемой ИСПДн Учреждения.

3.10. Структура, состав и основные функции СЗПДн определяются в соответствии с уровнем защищенности, который требуется обеспечить для ПДн, обрабатываемых в ИСПДн Учреждения и моделью угроз безопасности персональных данных при их обработке в ИСПДн Учреждения.

4. Проведение работ по обеспечению безопасности персональных данных в ИСПДн

4.1. В целях оценки уровня защищённости обрабатываемых в ИСПДн Учреждения ПДн и своевременного устранения несоответствий требованиям законодательства РФ в области защиты ПДн в Учреждении раз в год должен проводиться анализ изменений процессов защиты ПДн.

4.2. Анализ изменений проводится по следующим основным направлениям:

- перечень лиц (подразделений), участвующих в обработке ПДн в ИСПДн Учреждения, степень их участия в обработке ПДн и характер взаимодействия между собой;
- перечень и объем обрабатываемых ПДн;
- цели обработки ПДн;
- процедуры сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления и уничтожения ПДн;
- способы обработки ПДн (автоматизированная, неавтоматизированная);
- перечень сторонних организаций, в том числе государственных регулирующих органов, в рамках отношений, с которыми осуществляется передача ПДн;
- перечень программно-технических средств, используемых для обработки ПДн;
- конфигурация и топология ИСПДн Учреждения в целом и ее отдельных компонентов, физические, функциональные и технологические связи как внутри системы, так и с другими системами различного уровня и назначения;
- способы физического подключения и логического взаимодействия компонентов ИСПДн Учреждения, способы подключения к сетям связи общего пользования и международного информационного обмена с определением пропускной способности линий связи;
- режимы обработки ПДн в ИСПДн Учреждения в целом и в отдельных компонентах;
- состав используемого комплекса средств защиты ПДн и механизмов идентификации, аутентификации и разграничения прав доступа пользователей ИСПДн Учреждения на уровне операционных систем, баз данных и прикладного программного обеспечения;
- перечень организационно-распорядительной документации, определяющей порядок обработки и защиты ПДн;
- физические меры защиты ПДн, организация пропускного режима.

4.3. Результаты анализа изменений используются для оценки корректности требований по обеспечению безопасности ПДн, обрабатываемых с использованием средств автоматизации и без использования таких средств, и при необходимости их уточнения.

4.4. Доступ к ПДн регламентируется Положение о разграничении доступа к ПДн.

4.5. Лица, участвующие в обработке ПДн в ИСПДн Учреждения, должны быть проинформированы:

- о факте обработки ими ПДн – реализуется путем ознакомления лиц, обрабатывающих ПДн, с Перечнем должностей и третьих лиц, имеющих доступ к персональным данным, обрабатываемым в ИСПДн Учреждения;
- о категориях, обрабатываемых ПДн – реализуется путем ознакомления с утвержденным Перечнем персональных данных, обрабатываемых в ИСПДн Учреждения;
- о правилах осуществления обработки ПДн – реализуется путем ознакомления под подпись с организационно-распорядительной документацией ИСПДн Учреждения, регламентирующей процессы обработки ПДн, в Журнале ознакомления с организационно-распорядительной документацией и требованиями законодательства Российской Федерации в области персональных данных.

4.6. Неавтоматизированная обработка ПДн в ИСПДн Учреждения должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения материальных носителей и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ. В ИСПДн Учреждения должен вестись учет носителей ПДн.

4.7. Фиксация ПДн должна осуществляться на отдельных материальных носителях (отдельных документах). ПДн должны отделяться от иной информации.

4.8. Фиксация на одном материальном носителе ПДн, цели обработки которых заведомо несовместимы, не допускается. В случае если на одном материальном носителе все же зафиксированы ПДн, цели обработки которых несовместимы, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

- при необходимости использования или распространения определенных ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн: например, копирование части страницы, содержащей ПДн, которые необходимо использовать,

предварительно закрыв остальную часть страницы чистым листом бумаги, либо копирование только необходимых страниц сшитого документа;

- при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию: например, копирование только необходимой части страницы, закрыв оставшуюся часть чистым листом бумаги.

4.9. Должен осуществляться мониторинг фактов несанкционированного доступа к персональным данным и приниматься соответствующие меры при их обнаружении. Мониторинг осуществляется Администратором информационной безопасности.

4.10. В ИСПДн Учреждения работником, отвечающим за обеспечение безопасности ПДн, должен осуществляться контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

4.11. При обработке ПДн в ИСПДн Учреждения, ответственные работники должны иметь возможность и средства для восстановления ПДн при их модификации или уничтожении вследствие несанкционированного доступа к ним.

4.12. Должен быть определен перечень помещений, используемых для обработки ПДн в ИСПДн Учреждения. При этом организация режима безопасности, охрана этих помещений должны обеспечивать сохранность носителей ПДн, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

4.13. Пользователи ИСПДн Учреждения должны обеспечивать сохранность съемных носителей, содержащих ПДн. В случае утраты носителя пользователи должны немедленно сообщить об этом Администратору информационной безопасности.

4.14. Если при работе с ПДн в ИСПДн Учреждения работнику необходимо покинуть рабочее место, материальные носители ПДн должны быть защищены от неконтролируемого доступа к ним. Для этого материальные носители запираются в отведенных для этого шкафах или сейфах.

4.15. В случае достижения цели обработки ПДн Учреждение прекращает обработку ПДн или обеспечивает ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) и уничтожает ПДн или обеспечивает их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, либо после окончания установленного срока хранения ПДн, если иное не предусмотрено локальными и федеральными законодательными

актами.

4.16. Проведение работ по созданию (модернизации) СЗПДн ИСПДн Учреждения включает следующие стадии:

- предпроектная стадия;
- стадия проектирования;
- стадия реализации СЗПДн;
- стадия ввода в действие СЗПДн.

4.17. На предпроектной стадии проводится определение требуемого уровня защищенности ИСПДн, формируется модель угроз безопасности ПДн при их обработке в ИСПДн, разрабатывается техническое задание на СЗПДн.

4.18. Определение уровня защищенности ПДн, обрабатываемых в ИСПДн осуществляется в соответствии с положениями Постановления Правительства Российской Федерации от 01 ноября 2012 г. №1119.

4.19. В связи с тем, что в ИСПДн Учреждения, помимо обеспечения конфиденциальности обрабатываемых ПДн, требуется обеспечить целостность и доступность ПДн. ИСПДн Учреждения указана в Перечне информационных систем персональных данных Учреждения.

4.20. Уровень защищенности ПДн, обрабатываемых в ИСПДн Учреждения, оформляется соответствующим актом.

4.21. Модель угроз безопасности ПДн при их обработке в ИСПДн Учреждения формируется на основании руководящих документов ФСТЭК России и ФСБ России.

4.22. Перечень актуальных угроз формируется для ИСПДн Учреждения с учетом условий функционирования ИСПДн и особенностей обработки ПДн.

4.23. По итогам определения УЗ ПДн, обрабатываемых в ИСПДн Учреждения, и результатам определения актуальных угроз безопасности ПДн формируются требования по обеспечению безопасности ПДн, обрабатываемых в ИСПДн. Данные требования оформляются в виде технического задания на СЗПДн.

4.24. Стадия проектирования СЗПДн включает разработку СЗПДн в составе ИСПДн, а именно – разработку разделов задания и проекта проведения по созданию (модернизации) СЗПДн в соответствии с требованиями технического задания;

4.25. Стадия реализации СЗПДн включает:

- закупку совокупности используемых в СЗПДн сертифицированных технических, программных и программно-технических средств защиты информации и их установку;
- определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации с их обучением;
- разработку эксплуатационной документации на СЗПДн и средства

защиты информации.

4.26. На стадии ввода в действие СЗПДн осуществляются:

- предварительные испытания средств защиты информации в комплексе с другими техническими и программными средствами;
- устранение несоответствий по итогам предварительных испытаний;
- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.

4.27. В процессе функционирования ИСПДн может осуществляться модернизация СЗПДн. В обязательном порядке модернизация проводится в случае, если:

- произошло изменение номенклатуры обрабатываемых ПДн, влекущее за собой изменение уровня защищенности ПДн, обрабатываемых ИСПДн;
- произошло изменение номенклатуры и/или актуальности угроз безопасности ПДн;
- изменилась структура ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн и т.п.).

4.28. Задачи по приведению ИСПДн Учреждения в соответствие с требования законодательства РФ в области защиты ПДн возлагаются на администратора безопасности ИСПДн.

4.29. При возникновении условий, влияющих на безопасность ПДн (компрометация паролей, нарушение целостности и доступности персональных данных и пр.), необходимо незамедлительно проинформировать об этом администратора безопасности ИСПДн.

4.30. Лица, виновные в нарушении требований, предъявляемых законодательством РФ к защите ПДн, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.

5. Категории пользователей ИСПДн

5.1. Пользователем ИСПДн является лицо, участвующее в функционировании ИСПДн или использующее результаты ее функционирования. Пользователем ИСПДн является любой работник Учреждения, имеющий доступ к ИСПДн и к ее ресурсам в соответствии с установленным порядком, получивший доступ для выполнения должностных обязанностей.

5.2. Пользователи ИСПДн делятся на три основные категории:

5.2.1. **Администратор ИСПДн**. В эту группу включаются работники Учреждения, которые занимаются настройкой, внедрением и сопровождением системы. **Администратор ИСПДн** обладает следующим уровнем доступа:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

5.2.2. **Администратор безопасности ИСПДн**, работник Учреждения, ответственный за функционирование СЗИ, включая обслуживание и настройку административной, серверной и клиентской компонент. Администратор безопасности ИСПДн обладает следующим уровнем доступа и знаний:

- обладает правами администратора ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности ИСПДн уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других Учреждений.

5.2.1. **Пользователь ИСПДн** - работник Учреждения, участвующий в процессе в обработки информации в ИСПДн. Пользователь ИСПДн обладает следующим уровнем доступа:

- обладает всеми необходимыми атрибутами (например, логином и паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- имеет доступ к техническим средствам обработки информации и данным ИС в рамках своих полномочий и прав доступа;
- располагает конфиденциальными данными, к которым имеет доступ.

Категории пользователей должны быть определены для каждой ИСПДн. Должно быть уточнено разделение работников внутри категорий, в соответствии с типами пользователей определенными в Политике информационной безопасности.

5.1. Все выявленные группы пользователей отражаются в Аналитическом отчете об организации обеспечения безопасности ПДн Учреждения (Акт обследования). На основании Аналитического отчета определяются права доступа к элементам ИСПДн для всех групп пользователей и отражаются в Матрице доступа и в Положении о разграничении прав доступа к ИСПДн.

6. Сбор, обработка и защита персональных данных

6.1. Порядок получения (сбора) персональных данных:

6.1.1. Все персональные данные субъекта следует получать у него лично с его письменного согласия, кроме случаев, определенных в п. 6.1.4 и 6.2 настоящего Положения и иных случаях, предусмотренных законами.

6.1.2. Согласие субъекта на использование его персональных данных хранится в бумажном виде в его деле.

6.1.3. Согласие субъекта на обработку персональных данных действует в течение всего срока действия договора, а также в течение 5 лет с даты прекращения действия договорных отношений субъекта с Учреждением. По истечении указанного срока действие согласия считается продленным на каждые следующие пять лет при отсутствии сведений о его отзыве.

6.1.4. Если персональные данные субъекта возможно получить только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Третье лицо, предоставляющее персональные данные субъекта, должно обладать согласием субъекта на передачу персональных данных Учреждению. Учреждение обязано получить подтверждение от третьего лица, передающего персональные данные субъекта персональных данных о том, что персональные данные передаются с согласия субъекта. Учреждение обязано при взаимодействии с третьими лицами заключить с ними соглашение о конфиденциальности информации, касающейся персональных данных субъектов.

6.1.5. Учреждение обязано сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта персональных данных дать письменное согласие на их получение.

6.2. Обработка персональных данных субъектов без их согласия

осуществляется в следующих случаях:

6.2.1 Персональные данные являются общедоступными.

6.2.2 По требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

6.2.3 Обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора.

6.2.4 Обработка персональных данных осуществляется в целях заключения и исполнения договора, одной из сторон которого является субъект персональных данных.

6.2.5 Обработка персональных данных осуществляется для статистических целей при условии обязательного обезличивания персональных данных.

6.2.6 В иных случаях, предусмотренных законом.

6.3. Учреждение не имеет права получать и обрабатывать персональные данные субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях.

6.4. Порядок обработки персональных данных:

6.4.1. Субъект персональных данных предоставляет запрашивающему сотруднику Учреждения достоверные сведения о себе.

6.4.2. На основании полученной информации сотрудник Учреждения проверяет наличие данного субъекта, зарегистрированного в информационной системе. Если субъект отсутствует в информационной системе, то сотрудник заносит полную информацию о субъекте, после получения письменного согласия последнего. В случае наличия информации о субъекте в информационной системе – сверяет данные с ранее предоставленными (при необходимости вносит соответствующие изменения).

6.4.3. Обработка персональных данных субъекта может осуществляться исключительно в целях осуществления комплекса медицинских услуг и соблюдения законов и иных нормативных правовых актов

6.4.4. При определении объема и содержания, обрабатываемых персональных данных Учреждение должно руководствоваться требованиями Минздрава РФ, ФСБ, ФСТЭК и иных контролирующих органов, Конституцией Российской Федерации, закона о персональных данных, Трудовым кодексом Российской Федерации и иными федеральными законами.

6.5. Защита персональных данных:

6.5.1. Под защитой персональных данных субъекта понимается комплекс мер (организационных, технических), направленных на предотвращение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных субъектов, а также от иных неправомерных действий.

6.5.2. Защита персональных данных субъекта осуществляется за счёт Учреждения в порядке, установленном федеральным законом.

6.5.3. Учреждение при защите персональных данных субъектов принимает все необходимые организационные и технические меры, в том числе:

- Шифровальные (криптографические) средства.
- Антивирусная защита.
- Анализ защищённости.
- Обнаружение и предотвращение вторжений.
- Управления доступом.
- Регистрация и учет.
- Обеспечение целостности.
- Организация нормативно-методических локальных актов, регулирующих защиту персональных данных.

7. Блокировка, обезличивание, уничтожение персональных данных

7.1. Порядок блокировки и разблокировки персональных данных:

7.1.1. Блокировка персональных данных субъектов осуществляется с письменного заявления субъекта персональных данных.

7.1.2. Блокировка персональных данных подразумевает:

7.1.3. Запрет редактирования персональных данных.

7.1.4. Запрет распространения персональных данных любыми средствами (e-mail, сотовая связь, материальные носители).

7.1.5. Запрет использования персональных данных в массовых рассылках (sms, e-mail, почта).

7.1.6. Изъятие бумажных документов, относящихся к субъекту персональных данных и содержащих его персональные данные из внутреннего документооборота Учреждения и запрет их использования.

7.1.7. Блокировка персональных данных субъекта может быть временно снята, если это требуется для соблюдения законодательства.

7.1.8. Разблокировка персональных данных субъекта осуществляется с его письменного согласия или заявления.

7.1.9. Повторное согласие субъекта персональных данных на обработку его данных влечет разблокирование его персональных

данных.

7.2. Порядок обезличивания и уничтожения персональных данных:

7.2.1. Обезличивание персональных данных субъекта происходит по письменному заявлению субъекта персональных данных, при условии, что все договорные отношения завершены и от даты окончания последнего договора прошло не менее 5 лет.

7.2.2. При обезличивании персональные данные в информационных системах заменяются набором символов, по которому невозможно определить принадлежность персональных данных к конкретному субъекту.

7.2.3. Бумажные носители документов при обезличивании персональных данных уничтожаются.

7.2.4. Операция обезличивания персональных данных субъекта необратима.

7.2.5. Учреждение обязано обеспечить конфиденциальность в отношении персональных данных при необходимости проведения испытаний информационных систем на территории разработчика и произвести обезличивание персональных данных в передаваемых разработчику информационных системах.

7.2.6. Уничтожение персональных данных субъекта подразумевает прекращение какого-либо доступа к персональным данным субъекта.

7.2.7. При уничтожении персональных данных субъекта работники Учреждения не могут получить доступ к персональным данным субъекта в информационных системах.

7.2.8. Бумажные носители документов при уничтожении персональных данных уничтожаются, персональные данные в информационных системах обезличиваются. Персональные данные восстановлению не подлежат.

7.2.9. Операция уничтожения персональных данных необратима.

7.2.10. Срок, после которого возможна операция уничтожения персональных данных субъекта определяется окончанием срока, указанным в пункте 2.5 настоящего Положения.

8. Передача и хранение персональных данных

8.1. Передача персональных данных:

8.1.1. Под передачей персональных данных субъекта понимается распространение информации по каналам связи и на материальных носителях.

8.1.2. При передаче персональных данных работники Учреждения должны соблюдать следующие требования:

8.1.2.1. Не сообщать персональные данные субъекта в коммерческих целях. Обработка персональных данных субъектов в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи не допускается.

8.1.2.2. Осуществлять передачу персональных данных субъектов в пределах Учреждения в соответствии с настоящим Положением, нормативно-технологической документацией и должностными инструкциями.

8.1.2.3. Разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения должностных обязанностей.

8.1.2.4. Передавать персональные данные субъекта представителям субъекта в порядке, установленном законодательством и нормативно-технологической документацией и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

8.2. Хранение и использование персональных данных:

8.2.1. Под хранением персональных данных понимается существование записей в информационных системах и на материальных носителях.

8.2.2. Персональные данные субъектов обрабатываются и хранятся в информационных системах, а также на бумажных носителях в Учреждении.

8.2.3. Хранение персональных данных субъекта может осуществляться не дольше, чем этого требуют цели обработки, если иное не предусмотрено федеральными законами.

8.2.4. В течение срока хранения персональные данные не могут быть обезличены или уничтожены.

8.2.5. По истечении срока хранения персональные данные могут быть обезличены в информационных системах и уничтожены на бумажном носителе.

9. Доступ к персональным данным

9.1. Право доступа к персональным данным субъектов имеют работники, назначенные соответствующим приказом.

9.2. Работники Учреждения, получившие доступ к персональным данным субъекта, обязаны использовать их лишь в целях, для которых сообщены персональные данные и обязаны соблюдать режим секретности

(конфиденциальности) обработки и использования полученной информации (персональных данных субъектов).

9.3. Субъект может получить доступ к своим персональным данным с письменного заявления, включая право на безвозмездное получение копий любой записи, содержащей персональные данные субъекта.

10. Обработка персональных данных, осуществляемая без использования средств автоматизации

10.1. Обработка персональных данных, содержащихся в информационных системах персональных данных либо извлеченные из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

10.2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

10.3. Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Учреждения, должны применяться с учетом требований настоящего Положения.

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

10.5. 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.

10.6. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе работники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления

такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Учреждения.

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

10.7.1. 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, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

10.7.2. 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, - при необходимости получения письменного согласия на обработку персональных данных;

10.7.3. 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;

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

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

10.8.1. необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена 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;

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

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

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

10.9.1. 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;

10.9.2. 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, подлежащих уничтожению или блокированию.

10.10. 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).

10.11. Правила, предусмотренные пунктами 5.9. и 5.10. настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

10.12. 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.

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

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

10.15.При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

11. Права оператора персональных данных

11.1. Учреждение вправе:

11.1.1. Отстаивать свои интересы в суде.

11.1.2. Предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.).

11.1.3. Отказать в предоставлении персональных данных в случаях, предусмотренных законом.

11.1.4. Использовать персональные данные субъекта без его согласия, в случаях, предусмотренных законом.

12. Права субъекта персональных данных

12.1. Субъект персональных данных имеет право:

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

12.1.2 Требовать перечень обрабатываемых персональных данных, имеющихся в Организации и источник их получения.

12.1.3 Получать информацию о сроках обработки персональных

данных, в том числе о сроках их хранения.

12.1.4 Требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

12.1.5 Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных.

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

Соглашение о неразглашении сведений ограниченного доступа, ставших известными работнику при исполнении служебных обязанностей

13.1. Работник Учреждения обязуется:

13.1.1. Не разглашать персональные данные о работниках и субъектах персональных данных, обработка данных которых ведется в Учреждении, а также информацию о сторонних предприятиях и организациях, переданные работнику в ходе трудовой деятельности, персональные данные физических лиц, другие сведения ограниченного доступа (далее – сведения ограниченного доступа), которые ему будут доверены или станут известны в период действия Трудового договора работника в Учреждении.

13.1.2. Не сообщать устно или письменно кому бы то ни было сведения ограниченного доступа без соответствующего разрешения имеющих на то право лиц.

13.1.3. В случае попытки посторонних лиц получить сведения ограниченного доступа немедленно сообщать об этом своему руководителю и администратору по безопасности.

13.1.4. Не использовать известные сведения ограниченного доступа для занятий любой деятельностью, которая в качестве конкурентного действия может нанести ущерб Учреждению.

13.1.5. При прекращении действия Трудового договора работника в Учреждении все носители сведений ограниченного доступа (документы, машинные носители, черновики, распечатки на принтерах и пр.), которые находились в его распоряжении в связи с выполнением должностных обязанностей, передать администратору безопасности.

13.1.6. Об утрате или недостаче носителей сведения ограниченного доступа, удостоверений, пропусков, ключей от сейфов (хранилищ), личных печатей и других фактах, которые могут привести к разглашению сведений ограниченного доступа, а также о причинах и

условиях возможной утечки этих сведений немедленно сообщать администратору безопасности.

13.1.7. Использовать переданные ему и установленные на рабочем месте технические средства обработки и передачи информации исключительно для выполнения обязанностей, предусмотренных Трудовым договором работника.

13.2. В период работы в Учреждении работнику предоставляются необходимые условия для выполнения требований по охране конфиденциальности персональных данных, к которым допускается работник – хранилища для документов, средства для доступа к информационным ресурсам (ключи, пароли и т.п.) и др., определяемые обязанностями, выполняемыми работником.

13.3. Работник разрешает уполномоченному работнику Учреждения - администратору безопасности, производить контроль использования работником технических средств обработки и передачи информации.

13.4. Администратор безопасности Учреждения оставляет за собой право, но не принимает каких-либо обязательств контролировать надлежащие использование Работником технических средств обработки и хранения информации, соблюдение им мер по охране конфиденциальности.

13.5. Работник подтверждает, что не имеет никаких обязательств перед какими-либо физическими или юридическими лицами, которые входят в противоречие с Трудовым договором работника или которые ограничивают его трудовую деятельность в соответствии с текущим Трудовым договором работника.

13.6. Работнику будет предоставлена возможность ознакомления с перечнем информации, составляющей сведения ограниченного доступа, разглашение которых может нанести ущерб в работе Учреждения и нарушить текущий Трудовой договор работника.

13.7. Работник, которому в связи с выполнением своих трудовых обязанностей или конкретного задания при работе в Учреждении стал известен секрет производства, обязан сохранять конфиденциальность полученных сведений до прекращения действия исключительного права на секрет производства работодателя или его контрагентов, которым секрет производства передан по договору об отчуждении исключительного права на секрет производства, в том числе – и после прекращения действия трудового договора.

13.8. Работнику известно, что разглашение сведений ограниченного доступа, ставших ему известными в период действия текущего Трудового договора работника, может повлечь дисциплинарную, материальную, административную, гражданско-правовую, уголовную ответственность, предусмотренную действующим законодательством Российской Федерации.