**УТВЕРЖДАЮ**

Главный врач
ГБУЗ «Стоматологическая
поликлиника г. Копейск»

_____ / Ф.А. Шайхутдинов /
(подпись)

«29» октября 2024 г.

# ПОЛИТИКА
# В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

# Содержание

1. Общие положения ..... 3
2. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных ..... 7
3. Цели обработки персональных данных ..... 9
4. Содержание обрабатываемых персональных данных ..... 9
5. Обработка персональных данных ..... 9
6. Категории субьектов персональных данных ..... 10
7. Сроки обработки и хранения персональных данных ..... 11
8. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований ..... 11
9. Основыные права и обязанности Оператора персональных данных ..... 12
10. Основыные права и обязанности субъекта персональных данных ..... 13
11. Порядок обработки персональных данных в информационных системах ..... 13
12. Передача персональных данных ..... 16

## 1. Общие положения

1.1. Политика в отношении обработки персональных данных в ГБУЗ «Стоматологическая поликлиника г. Копейск» (далее – Политика) устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют ГБУЗ «Стоматологическая поликлиника г. Копейск» (далее – Оператор) как оператора, осуществляющего обработку персональных данных, и для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

1.2. Политика разработана в соответствии с:

- Конституцией Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;
- Федеральным законом от 02.09.2006 №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- постановлением Правительства Российской Федерации от 21.03.2012 №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»;
- постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- постановлением Правительства Российской Федерации от 15.09.2008 № 697 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановлением Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

1.3. Обработка персональных данных Оператором осуществляется в связи с выполнением учреждением функций, предусмотренных ее учредительными документами, и определяемых Федеральным законом от 21 ноября 2011 № 323-ФЗ «Об основах охраны здоровья граждан в РФ».

Обработка персональных данных Оператором осуществляется с соблюдением принципов и условий, предусмотренных настоящей Политикой и законодательством Российской Федерации в области персональных данных.

Для обеспечения безопасности персональных данных Оператор руководствуется следующими принципами:

- законность: защита персональных данных основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов области обработки и защиты персональных данных;
- системность: обработка персональных данных Оператором осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных;
- комплексность: защита персональных данных строится с использованием функциональных возможностей информационных технологий, реализованных в

информационных системах Оператора и других имеющихся в учреждении систем, и средств защиты;

- непрерывность: защита персональных данных обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки персональных данных, в том числе при проведении ремонтных и регламентных работ;
- своевременность: меры, обеспечивающие надлежащий уровень безопасности персональных данных, принимаются до начала их обработки;
- преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты персональных данных осуществляется на основании результатов анализа практики обработки персональных данных Оператора с учетом выявления новых способов и средств реализации угроз безопасности персональных данных, отечественного и зарубежного опыта в сфере защиты информации;
- персональная ответственность: ответственность за обеспечение безопасности персональных данных возлагается на работника в пределах их обязанностей, связанных с обработкой и защитой персональных данных;
- минимизация прав доступа: доступ к персональным данным представляется работникам только в объеме, необходимом для выполнения их должностных обязанностей;
- гибкость: обеспечение выполнения функций защиты персональных данных при изменении характеристик функционирования информационных систем персональных данных Оператора, а также обмена и состава обрабатываемых персональных данных;
- специализация и профессионализм: реализация мер по обеспечению безопасности персональных данных осуществляется работниками, имеющим необходимые квалификацию и опыт;
- эффективность процедур отбора кадров: кадровая политика Оператора предусматривает тщательный подбор персонала и мотивацию работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности персональных данных;
- наблюдаемость и прозрачность: меры по обеспечению персональных данных должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющие контроль;
- непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты персональных данных, а результаты контроля регулярно анализируются.

Кроме того, обработка персональных данных Оператором осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых учреждение выступает в качестве работодателя (глава 14 Трудового кодекса РФ), в связи с реализацией Оператором своих прав и обязанностей как юридического лица.

1.4. Термины и принятые сокращения

1.4.1. Термины и понятия, используемые в настоящей Политике, применяются в значениях, определенных в статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.4.2. Пациент – физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния;

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

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

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

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

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

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

1.4.9. Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

1.4.10. Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

1.4.11. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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

1.5. Обработка персональных данных в учреждении - выполняется с использованием средств автоматизации или без использования таких средств (смешанная обработка) и включает сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных субъектов, персональные данные которых обрабатываются Оператором.

1.6. Обезличивание персональных данных не осуществляется.

1.7. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, сведений, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные) не осуществляется.

1.8. Трансграничная передача персональных данных не осуществляется.

1.9. Оператором не осуществляется принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

1.10. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению учреждения, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

1.11. Работники учреждения, включенные в Перечень должностей, уполномочены осуществлять обработку персональных данных либо осуществлять доступ к персональным

данным Оператора. Обработка персональных данных либо доступ к персональным данным работниками Оператора, не уполномоченными на совершение таких действий с персональными данными в порядке, предусмотренном настоящей Политикой, запрещены.

1.12. Лицо, ответственное за организацию обработки персональных данных осуществляет ведение перечня лиц, которые уполномочены осуществлять обработку персональных данных либо осуществлять доступ к персональным данным.

1.13. Ответственность за наличие у руководителей структурных подразделений Оператора полномочий осуществлять обработку персональных данных либо осуществлять доступ к персональным данным в учреждении несет лицо, ответственное за организацию обработки персональных данных. Ответственность за наличие у остальных работников учреждения полномочий осуществлять обработку персональных данных либо осуществлять доступ к персональным данным несут руководители структурных подразделений учреждения.

1.14. Работники, уполномоченные осуществлять обработку персональных данных либо осуществлять доступ к персональным данным, могут осуществлять обработку персональных данных как неавтоматизированным, так и автоматизированным способами.

## 2. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

Для выявления и предотвращения нарушений, предусмотренных законодательством Российской Федерации в сфере персональных данных, в учреждении используются следующие процедуры:

2.1. Осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2.2. Ознакомление работников Оператора, которые уполномочены осуществлять обработку персональных данных либо осуществлять доступ к персональным данным, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), приказами Оператора по вопросам обработки персональных данных.

Перед началом обработки персональных данных работники Оператора, которые уполномочены осуществлять обработку персональных данных либо осуществлять доступ к персональным данным, подписывают обязательство работника учреждения, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей (далее - обязательство прекратить обработку персональных данных), и предоставляют его в отдел кадров учреждения.

Обработка персональных данных за исключением своих собственных персональных данных работниками Оператора до момента подписания обязательства запрещается.

Подписание работниками обязательства прекратить обработку персональных данных, предусмотренного настоящей Политикой, обеспечивает начальник отдела кадров.

В случае если работник, который уполномочен осуществлять обработку персональных данных либо осуществлять доступ к персональным данным в учреждении, переведен или назначен на другую должность, включенную в Перечень должностей, то он перед началом обработки персональных данных на новой должности повторно подписывает обязательство на обработку персональных данных и предоставляет его в отдел кадров.

Подписанные обязательства приобщаются к личным делам работников.

2.3. Ограничение обработки персональных данных достижением цели обработки.

2.4. Соответствие содержания и объема обрабатываемых персональных данных заявленным целям обработки.

2.5. Осуществление обработки персональных данных в соответствии с принципами и условиями обработки персональных данных, установленными законодательством Российской Федерации в сфере персональных данных.

2.6. Недопущение объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

2.7. Обеспечение при обработке персональных данных точности персональных данных, их достаточности, а в необходимых случаях – актуальности по отношению к целям обработки персональных данных.

2.8. Соблюдение условий при хранении носителей персональных данных, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним, посредством принятия мер обеспечения безопасности, включающих:

2.8.1. Хранение бумажных и машинных носителей информации (магнитные и оптические диски, флеш-накопители, накопители на жестких магнитных дисках, твердотельные накопители и другие), содержащих персональные данные (далее - машинные носители персональных данных), только в помещениях, включенных в перечень помещений, в которых осуществляется обработка, в том числе хранение, персональных данных (носителей персональных данных) в учреждении, утвержденный приказом по учреждению, в условиях, исключающих возможность доступа посторонних лиц к персональным данным, в закрываемых сейфах или шкафах (ящиках).

2.8.2. Резервное копирование персональных данных, содержащихся в информационных системах персональных данных, применяемых в учреждении, на резервные машинные носители персональных данных.

2.8.3. Раздельное хранение персональных данных, обработка которых осуществляется в различных целях, определенных настоящей Политикой, на разных материальных носителях, которое обеспечивается структурными подразделениями Оператора, осуществляющими обработку персональных данных неавтоматизированным способом (без использования средств вычислительной техники).

2.8.4. Уничтожение персональных данных на машинных носителях персональных данных в случае их передачи (в том числе в составе технических средств) для их дальнейшей эксплуатации в другие структурные подразделения Оператора или иные организации, а также при передаче таких машинных носителей персональных данных (в том числе в составе технических средств) на ремонт в сторонние организации, не имеющие права доступа к персональным данным, содержащимся на соответствующих машинных носителях персональных данных, или при выводе из эксплуатации (списании) указанных машинных носителей персональных данных (в том числе в составе технических средств).

2.9. Принятие мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, применяемых Оператором.

2.10. Запрет на передачу работниками Оператора персональных данных, за исключением персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом, по незащищенным каналам связи, в том числе средствами факсимильной связи и электронной почты, а также на вынос носителей персональных данных из служебных помещений Оператора в целях, не связанных со служебной необходимостью.

2.11. Лица, виновные в нарушении требований Федерального закона от 27.07.2006 № 152- ФЗ «О персональных данных», несут предусмотренную законодательством Российской Федерации ответственность.

## 3. Цели обработки персональных данных

3.1. Ведение кадрового и бухгалтерского учета;
3.2. Обеспечение соблюдения трудового законодательства РФ;
3.3. Обеспечение соблюдения налогового законодательства РФ;
3.4. Обеспечение соблюдения пенсионного законодательства РФ;
3.5. Обеспечение соблюдения законодательства РФ в сфере здравоохранения;
3.6. Подготовка, заключение и исполнение гражданско-правового договора;
3.7. Обеспечение пропускного режима на территорию оператора;
3.8. Подбор персонала (соискателей) на вакантные должности оператора;
3.9. Обеспечение своевременного рассмотрения в полном объеме устных и письменных обращений граждан;
3.10. Создание общедоступных источников информационного обеспечения (в том числе справочники, адресные книги, ведение официального сайта организации);
3.12. Осуществление медицинской и иной деятельности, предусмотренной Уставом; в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг; защита жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц;
3.12. Начисление заработной платы, пособий и иных выплат;
3.13. Соблюдение прав граждан в сфере охраны здоровья и обеспечение связанных с этими правами государственных гарантий, доступность и качество медицинской помощи, реализация иных уставных задач.

## 4. Содержание обрабатываемых персональных данных

Содержание обрабатываемых персональных данных для каждой цели обработки персональных данных определено Перечнем персональных данных, обрабатываемых Оператором.

## 5. Обработка персональных данных

5.1. Получение персональных данных.

5.1.1. Все персональные данные следует получать от самого субъекта. Если персональные данные субъекта можно получить только у третьей стороны, то субъект должен быть уведомлен об этом или от него должно быть получено согласие.

5.1.2. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, характере которого действует согласие, и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

5.1.3. Документы, содержащие персональные данные, создаются путем:

а) копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др);

б) внесение сведений в учетные формы;

в) получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.),

Порядок доступа субъекта персональных данных к его персональным данных, обрабатываемым учреждением, определяется в соответствии с законодательством и внутренними регулятивным и документами Оператора.

5.2. Обработка персональных данных

5.2.1 Обработка персональных данных осуществляется:

– с согласия субъекта персональных данных на обработку его персональных данных;

– в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных законодательством РФ функций, полномочий и обязанностей;

– в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее персональные данные, сделанные общедоступными субъектом персональных данных).

Доступ работников к обрабатываемым персональным данным осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Оператора.

Допущенные к обработке персональных данных работники под роспись знакомятся с документами организации, устанавливающими порядок обработки персональных данных, включая документы, устанавливающие права и обязанности конкретных работников.

Оператором производится устранение выявленных нарушений законодательства об обработке и защите персональных данных.

## 6. Категории субъектов персональных данных

6.1. Оператором обрабатываются персональные данные следующих категорий субъектов персональных данных:

6.1.1. Работники;

6.1.2. Соискатели;

6.1.3. Родственники работников;

6.1.4. Уволенные работники;

6.1.5. Контрагенты;

6.1.6. Посетители сайта;

6.1.7. Учащиеся

5.1.8. Пациенты;

6.1.9. Законные представители;

6.1.10. Исполнители;

6.1.11. Гражданин, направивший обращение;

6.1.12. Родственники уволенных работников;

6.1.13. Представители юридических лиц.

6.2. Категории субъектов персональных данных для каждой цели обработки персональных данных определены Перечнем персональных данных, обрабатываемых в учреждении.

6.3. В случаях, предусмотренных Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных» получение согласий субъектов персональных данных на обработку их персональных данных Оператором обеспечивается структурными подразделениями, которые осуществляют сбор персональных данных у субъектов персональных данных.

Согласия субъектов персональных данных на обработку их персональных данных Оператора, полученные в письменной форме, хранятся в структурных подразделениях Оператора, которые осуществляют сбор персональных данных, в течение 3 лет с даты прекращения обработки персональных данных соответствующих субъектов персональных данных, если иное не предусматривается федеральными законами, договорами.

Ответственность за наличие согласия субъектов персональных данных на обработку их персональных данных несут руководители структурных подразделений, которыми осуществляется сбор персональных данных.

## 7. Сроки обработки и хранения персональных данных

7.1. Сроки обработки и хранения персональных данных в учреждении определяются правовыми актами, регламентирующими порядок их сбора и обработки.

В случае если правовыми актами конкретный срок обработки и хранения персональных данных не установлен, то их обработка осуществляется до достижения цели обработки персональных данных или утраты необходимости в достижении цели обработки персональных данных.

7.2. Срок хранения персональных данных в электронном виде должен соответствовать сроку хранения персональных данных на бумажных носителях, если иное не установлено законодательством Российской Федерации.

7.3. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных обработка соответствующих персональных данных Опертором должна быть прекращена, если Оператор не вправе осуществлять обработку таких персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных» или другими федеральными законами.

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

8.1. Уничтожению подлежат обрабатываемые персональные данные по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.

Срок уничтожения персональных данных не должен превышать тридцати дней с даты достижения цели обработки персональных данных (утраты необходимости в достижении цели обработки персональных данных), если иное не предусмотрено законодательством Российской Федерации.

8.2. Руководителями структурных подразделений Оператора осуществляется контроль и отбор по истечении срока хранения, установленного законодательством Российской Федерации, обрабатываемых персональных данных, содержащихся на бумажных и машинных
носителях персональных данных, в том числе в информационных системах персональных данных, подлежащих уничтожению.

Уничтожение персональных данных, срок хранения которых истек, производится работниками Оператора, которые уполномочены осуществлять обработку персональных данных либо осуществлять доступ к персональным данным.

8.3. В случае отсутствия возможности уничтожения персональных данных ответственный за организацию обработки персональных данных Оператора осуществляет блокирование таких персональных данных и уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен законодательством Российской Федерации.

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

8.5. Уничтожение персональных данных на машинных носителях персональных данных осуществляется с использованием средств гарантированного удаления информации или путем физического разрушения машинного носителя персональных данных, исключающего дальнейшее восстановление информации.

Уничтожение персональных данных, внесенных в информационные системы персональных данных, применяемые в учреждении, осуществляется ответственным за

организацию обработки персональных данных по заявкам, поступившим от структурных подразделений Оператора.

8.6. В целях реализации меры, предусмотренной подпунктом 2.8.4 настоящей Политики, структурные подразделения Оператора направляют письменную заявку ответственному за организацию обработки персональных данных на уничтожение персональных данных на машинном носителе персональных данных (физическое разрушение машинного носителя персональных данных).

В срок, не превышающий 10 рабочих дней с даты поступления заявки, ответственным за организацию обработки персональных данных направляется заявителю уведомление в письменной форме, содержащее результаты уничтожения персональных данных на машинном носителе персональных данных (физического разрушения машинного носителя персональных данных), к которому прилагается соответствующий машинный носитель персональных данных (в случае если машинный носитель персональных данных не подвергался физическому разрушению).

## 9. Основные права и обязанности Оператора персональных данных

9.1. Оператор при сборе персональных данных обязан предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его персональных данных.

9.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

9.3. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети интернет, Оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных Федеральном законе «О персональных данных».

9.4. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

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

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

9.7. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных». В поручении Оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом,

осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

## 10. Основные права и обязанности субъекта персональных данных

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

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

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

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

## 11. Порядок обработки персональных данных в информационных системах

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

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

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

11.4. Информация может вноситься как в автоматическом режиме при получении персональных данных с официального сайта в сети интернет, так и в ручном режиме при

получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

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

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

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

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации и технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

11.8. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы первого типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы второго типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы третьего типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных».

11.9. В соответствии с пунктом 11 статьи 19 Федерального закона «О персональных данных» под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

При обработке персональных данных в информационных системах устанавливаются четыре уровня защищенности персональных данных.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

г) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает биометрические персональные данные;

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

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

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

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

11.10. Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении к Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

## 12. Передача персональных данных

12.1. Персональные данные в соответствии с нормами действующего законодательства могут передаваться в государственные и негосударственные органы и учреждения, в частности:

- налоговые органы;
- органы социального страхования;
- органы государственной власти в сфере занятости населения;
- военкоматы;
- банк, в который перечисляется заработная плата в соответствии с заявлением работника;
- правоохранительные и судебные органы;
- профсоюзные органы.

12.2. Передача персональных данных третьим лицам осуществляется только с письменного согласия субъекта, за исключением случаев, установленных федеральными законами.

12.3. Персональные данные передаются с обязательным уведомлением лица, получающего их, об обязанности использования полученной конфиденциальной информации лишь в целях, для которых она сообщена, и с предупреждением об ответственности за незаконное использование данной информации в соответствии с федеральными законами.