

## **ПОЛИТИКА ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СПБ ГБУЗ «ГОРОДСКАЯ ПОЛИКЛИНИКА №46»**

### **1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) составлена в соответствии с пунктом 2 статьи 18.1 Закона № 152-ФЗ от 27 июля 2006 г. «О персональных данных» и является основополагающим внутренним документом СПб ГБУЗ «Городская поликлиника №46 (далее Организация), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее – ПДн). Организация является оператором персональных данных и зарегистрирована в реестре Роскомнадзора.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав граждан при обработке ПДн в Организации, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Организацией как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Обработка ПДн в Организации осуществляется в связи с выполнением Организацией функций, предусмотренных ее учредительными документами и определяемых:

- Законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации»;
- постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- иными нормативными правовыми актами Российской Федерации.

Кроме того, обработка ПДн в Организации осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Организация выступает в качестве работодателя (гл. 14 ТК РФ), в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

1.5. Организация имеет право вносить изменения в настоящую Политику.

## 2. ТЕРМИНЫ И ПРИНЯТЫЕ СОКРАЩЕНИЯ

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

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

**Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

**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 ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

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

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

**Автоматизированная обработка персональных данных** – обработка ПДн с помощью средств вычислительной техники.

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

**Трансграничная передача персональных данных** - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

**Субъект персональных данных** - физическое лицо, данные которого обрабатываются;

**Конфиденциальность персональных данных** - обязательное для оператора и иных лиц, получивших доступ к ПДн, требование не раскрывать третьим лицам и не распространять ПДн без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

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

**Медицинская деятельность** – профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) ее компонентов в медицинских целях.

**Лечащий врач** – врач, на которого возложены функции по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения.

### 3. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

3.2. Для обеспечения безопасности ПДн Организация руководствуется следующими принципами:

– законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

– системность: обработка ПДн в Организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

– комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Организации и других имеющихся в Организации систем и средств защиты;

– непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

– своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

– преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Организации с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;

– персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

– минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;

– гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования ИСПДн Оператора, а также объема и состава обрабатываемых ПДн;

– специализация и профессионализм: реализация мер по обеспечению безопасности ПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;

– эффективность процедур отбора кадров: кадровая политика Организации предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн;

– наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

– непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

3.3. В СПб ГБУЗ «Городская поликлиника №46» не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн, в том числе при достижении целей их обработки или утраты

необходимости в достижении этих целей, обрабатывавшиеся Оператором ПДн уничтожаются или обезличиваются.

3.4. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости – и актуальность по отношению к целям обработки. Организация принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

#### **4. ЦЕЛИ СБОРА ПЕРСОНАЛЬНЫХ ДАННЫХ**

4.1. Оператор обрабатывает персональные данные в целях:

- оформления трудовых отношений, ведения кадрового делопроизводства, содействия в трудоустройстве, обучении, повышении по службе, пользовании различными льготами и гарантиями, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и сохранности имущества;
- осуществление трудовых отношений;
- заключения, исполнения и прекращения гражданско-правовых договоров;
- осуществление гражданско-правовых отношений;
- оказание медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с законами от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств» и от 29 ноября 2010 г. № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными постановлением Правительства РФ от 4 октября 2012 г. № 1006;
- оказания медицинских услуг, в том числе идентификации пациентов, отражения информации в медицинской документации, предоставления сведений страховым компаниям, предоставления установленной законодательством отчетности в отношении оказанных медицинских услуг;
- выполнения требований действующего законодательства;
- в иных случаях, установленных в законодательством РФ.

4.2. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

4.3. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

4.4. Обработке подлежат только ПДн, которые отвечают целям их обработки.

4.5. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

## **5. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

5.1. Правовым основанием обработки ПДн является совокупность правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку ПДн.

5.2. Оператор обрабатывает ПДн на основании:

- Трудового кодекса Российской Федерации;
- Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» и принятых на его основе нормативно-правовых актов, регулирующих отношения, связанные с оказанием медицинских услуг;
- иных федеральных законов и прочих нормативных правовых актов;
- устава Оператора;
- договоров, заключаемых между Оператором и субъектами ПДн;
- согласий на обработку ПДн.

## **6. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ**

### **6.1. Получение ПДн**

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

6.1.2. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения ПДн, характере подлежащих получению ПДн, перечне действий с ПДн, сроке, в течение которого действует согласие, и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

6.1.3. Документы, содержащие ПДн, создаются путем:

- а) копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и т. д.);
- б) внесения сведений в учетные формы;
- в) получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и т. д.).

Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Оператором, определяется в соответствии с законодательством и определяется внутренними регулятивными документами Организации.

### **6.2. Обработка ПДн**

6.2.1 Обработка персональных данных осуществляется:

- с согласия субъекта ПДн на обработку его ПДн;
- в случаях, когда обработка ПДн необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;
- в случаях, когда осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн.

Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Организации.

Допущенные к обработке ПДн Работники под подпись знакомятся с документами организации, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных Работников.

Организацией производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

### 6.2.2. Категории субъектов персональных данных

В Организации обрабатываются ПДн следующих субъектов:

- физические лица, состоящие с учреждением в трудовых отношениях;
- физические лица, являющие близкими родственниками сотрудников учреждения;
- физические лица, уволившиеся из учреждения;
- физические лица, являющиеся кандидатами на работу;
- физические лица, состоящие с учреждением в гражданско-правовых отношениях;
- физические лица, обратившиеся в учреждение за медицинской помощью.

### 6.2.3. ПДн, обрабатываемые Организацией:

- полученные при осуществлении трудовых отношений;
- полученные для осуществления отбора кандидатов на работу в организацию;
- полученные при осуществлении гражданско-правовых отношений;
- полученные при оказании медицинской помощи.

Полный список ПДн представлен в перечне ПДн, утвержденном главным врачом Организации.

### 6.2.4. Обработка персональных данных ведется:

- неавтоматизированная обработка ПДн;
- автоматизированная обработка ПДн с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;
- смешанная обработка ПДн.

## 6.3. Хранение ПДн

6.3.1. ПДн субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

6.3.2. ПДн, зафиксированные на бумажных носителях, хранятся в запираемых шкафах либо в запираемых помещениях с ограниченным правом доступа (регистратура).

6.3.3. ПДн субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в каталогах ИСПДн в различных форматах.

6.3.4. Не допускается хранение и размещение документов, содержащих ПДн, в открытых электронных каталогах (файлообменниках) в ИСПДн.

6.3.5. Хранение ПДн в форме, позволяющей определить субъекта ПДн, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

## 6.4. Уничтожение ПДн

6.4.1. Уничтожение документов (носителей), содержащих ПДн, производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

6.4.2. ПДн на электронных носителях уничтожаются путем стирания или форматирования носителя.

6.4.3. Уничтожение производится комиссией. Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

## 6.5. Передача ПДн

6.5.1. Организация передает ПДн третьим лицам в следующих случаях:

- субъект выразил свое согласие на такие действия;
- передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

6.5.2. Перечень третьих лиц, которым передаются ПДн:

- Пенсионный фонд РФ для учета (на законных основаниях);
- Налоговые органы РФ (на законных основаниях);
- Фонд социального страхования (на законных основаниях);
- Территориальный фонд обязательного медицинского страхования (на законных основаниях);
- страховые медицинские организации по обязательному и добровольному медицинскому страхованию (на законных основаниях);
- банки для начисления заработной платы (на основании договора);
- судебные и правоохранительные органы в случаях, установленных законодательством;
- бюро кредитных историй (с согласия субъекта);
- юридические компании, работающие в рамках законодательства РФ, при неисполнении обязательств по договору займа (с согласия субъекта).

## **6.6. Порядок и условия обработки ПДн**

6.6.1. Обработка ПДн осуществляется после принятия необходимых мер по защите ПДн.

6.6.2. Оператор не вправе обрабатывать ПДн субъекта ПДн без его письменного согласия, за исключением случаев, предусмотренных статьей 6 Федерального закона «О персональных данных».

6.6.3. равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

6.6.4. Письменное согласие субъекта ПДн должно включать:

- фамилию, имя, отчество;
- адрес субъекта ПДн;
- номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес Оператора;
- цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие субъекта ПДн;
- перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых Оператором способов обработки ПДн;
- срок, в течение которого действует согласие;
- способ его отзыва;
- подпись субъекта ПДн.

6.6.5. Оператор организует обработку ПДн в следующем порядке:

- 1) назначает ответственного за организацию обработки ПДн, устанавливает перечень лиц, имеющих доступ к ПДн;
- 2) разрабатывает и утверждает документы по вопросам обработки ПДн;
- 3) применяет правовые, организационные и технические меры по обеспечению безопасности ПДн;
- 4) осуществляет внутренний контроль соответствия обработки ПДн Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, настоящей Политике;
- 5) осуществляет оценку вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона «О персональных данных», определяет соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных данным Федеральным законом;
- 6) знакомит работников Оператора, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе с

требованиями к защите ПДн, настоящей Политики, документами по вопросам обработки ПДн.

6.6.6. Оператор при обработке ПДн принимает необходимые правовые, организационные и технические меры, в том числе:

- 1) определяет угрозы безопасности персональных данных при их обработке в ИСПДн;
- 2) применяет организационные и технические меры по обеспечению безопасности ПДн при их обработке ИСПДн, необходимые для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;
- 3) применяет прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации;
- 4) оценивает эффективность принимаемых мер по обеспечению безопасности ПДн до при эксплуатации ИСПДн;
- 5) учитывает машинные носители персональных данных;
- 6) обнаруживает факты несанкционированного доступа к ПДн и принимает меры;
- 7) восстанавливает ПДн, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;
- 8) устанавливает правила доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечивает регистрацию и учет всех действий, совершаемых с ПДн в ИСПДн.

6.6.7. При обработке ПДн Оператор выполняет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

6.6.8. В целях обеспечения сохранности и конфиденциальности ПДн все операции с ПДн должны выполняться только работниками Оператора, осуществляющими данную работу в соответствии с трудовыми обязанностями.

6.6.9. Оператор получает ПДн непосредственно от субъектов ПДн или их представителей, наделенных соответствующими полномочиями. Согласия субъекта на получение его ПДн от третьих лиц не требуется в случаях, когда согласие субъекта на передачу его ПДн третьим лицам получено от него в письменном виде при заключении договора с Оператором, а так-же в случаях, установленных федеральным законом.

6.6.10. Запрещается хранение документов с ПДн и их копий на рабочих местах и в открытом доступе, оставлять шкафы открытыми в случае выхода работника из рабочего помещения.

6.6.11. В электронном виде документы, содержащие ПДн, разрешается хранить в специализированных базах данных или в специально отведенных для этого каталогах с ограничением и разграничением доступа. Копирование таких данных запрещено.

6.6.12. При увольнении работника, имеющего доступ к ПДн, прекращении доступа к ПДн, документы и иные носители, содержащие ПДн, сдаются работником своему непосредственному руководителю.

## **7. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИСПДН**

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

7.2. Обеспечение безопасности при обработке ПДн, содержащихся в информационных системах, 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 ПДн при их обработке в ИСПДн, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

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

7.4. Информация может вноситься как в автоматическом режиме при получении ПДн 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.

7.5. Обеспечение безопасности ПДн, обрабатываемых в информационных системах органов, достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн.

7.6. В случае выявления нарушений порядка обработки ПДн уполномоченными работниками незамедлительно принимаются меры по установлению причин нарушений и их устранению.

7.7. В состав мер по обеспечению безопасности ПДн, реализуемых в рамках системы защиты ПДн с учетом актуальных угроз безопасности ПДн 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 обрабатываются ПДн;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности ПДн;
- обеспечение целостности ИСПДн;
- обеспечение доступности ПДн;
- 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 ИСПДн и к возникновению угроз безопасности ПДн, и реагирование на них;
- управление конфигурацией информационной системы и системы защиты ПДн.

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

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

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

Определение типа угроз безопасности ПДн, 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».

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

7.9.1. Необходимость обеспечения первого уровня защищенности ПДн 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 ПДн, либо биометрические персональные данные, либо иные категории ПДн;
- б) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает специальные категории ПДн более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора.

7.9.2. Необходимость обеспечения второго уровня защищенности ПДн 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 ПДн;
- б) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает специальные категории ПДн сотрудников Оператора или специальные категории ПДн менее чем 100000 субъектов ПДн, не являющихся сотрудниками Оператора;
- в) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает биометрические ПДн;
- г) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает общедоступные ПДн более чем 100000 субъектов ПДн не являющихся сотрудниками Оператора;
- д) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает иные категории ПДн более чем 100000 субъектов ПДн, не являющихся сотрудниками Оператора;
- е) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает специальные категории ПДн более чем 100000 субъектов ПДн, не являющихся сотрудниками Оператора.

7.9.3. Необходимость обеспечения третьего уровня защищенности ПДн 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 ПДн сотрудников Оператора или общедоступные ПДн менее чем 100000 субъектов ПДн, не являющихся сотрудниками Оператора;
- б) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает иные категории сотрудников Оператора или иные категории ПДн менее чем 100000 субъектов ПДн, не являющихся сотрудниками Оператора;
- в) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает специальные категории ПДн данных сотрудников Оператора или специальные категории ПДн менее чем 100000 субъектов ПДн, не являющихся сотрудниками Оператора;

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

д) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает иные категории ПДн более чем 100000 субъектов персональных данных, не являющихся сотрудниками Оператора.

7.9.4. Необходимость обеспечения четвертого уровня защищенности ПДн 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 ПДн;

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

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

## **8. ПОРЯДОК ОТВЕТА НА ЗАПРОСЫ СУБЪЕКТОВ НА ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ**

8.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- 1) подтверждение факта обработки ПДн;
- 2) правовые основания и цели обработки ПДн;
- 3) цели и применяемые оператором способы обработки ПДн;
- 4) наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Оператором или на основании федерального закона;
- 5) обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки ПДн, в том числе сроки их хранения;
- 7) порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом «О персональных данных»;
- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Оператора, если обработка поручена или будет поручена такому лицу;
- 10) иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

8.2. Указанные выше сведения должны быть предоставлены субъекту ПДн Оператором в доступной форме и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

8.3. Сведения, указанные в пункте 8.1, предоставляются субъекту ПДн или его представителю Оператором при получении запроса субъекта ПДн или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение

и иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Оператором, подпись субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

8.4. В случае если сведения, указанные в пункте 8.1, а также обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 8.1, и ознакомления с такими ПДн не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом или принятым в соответствии с ним нормативным правовым актом.

8.5. Субъект ПДн вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 8.1, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в пункте 8.4, в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 8.1, должен содержать обоснование направления повторного запроса.

8.6. Оператор вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 8.4 и 8.5. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

8.7. Оператор обязан сообщить субъекту персональных данных или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя в течение 30 дней с даты получения запроса субъекта ПДн или его представителя.

8.8. Оператор обязан предоставить безвозмездно субъекту ПДн данных или его представителю возможность ознакомления с ПДн, относящимися к этому субъекту ПДн.

8.9. В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, Оператор обязан внести в них необходимые изменения.

8.10. В срок, не превышающий семи рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Оператор обязан уничтожить такие ПДн.

8.11. Оператор обязан уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принять меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

8.12. В случае выявления неправомерной обработки ПДн по запросу субъекта ПДн или его представителя, либо уполномоченного органа по защите прав субъектов ПДн Оператор обязан осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, с момента получения указанного запроса на период проверки.

8.13. В случае выявления неточных ПДн по запросу субъекта ПДн или его представителя или по запросу уполномоченного органа по защите прав субъектов ПДн Оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту ПДн с момента получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

8.14. В случае подтверждения факта неточности ПДн Оператор на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов обязан уточнить ПДн

в течение семи рабочих дней со дня представления таких сведений и снять блокирование ПДн.

8.15. В случае выявления неправомерной обработки ПДн, осуществляемой Оператором, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПДн. В случае если обеспечить правомерность обработки ПДн невозможно, Оператор в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки, обязан уничтожить такие ПДн. Об устранении допущенных нарушений или об уничтожении ПДн Оператор обязан уведомить субъекта ПДн или его представителя.

8.16. В случае достижения цели обработки ПДн Оператор обязан прекратить обработку ПДн и уничтожить ПДн в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено соглашением между Оператором и субъектом ПДн либо если Оператор не вправе осуществлять уничтожение ПДн на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

8.17. В случае отзыва субъектом ПДн согласия на обработку его ПДн Оператор обязан прекратить их обработку и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн в срок, не превышающий 30 дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Оператором и субъектом персональных данных либо Федеральным законом «О персональных данных» или другими федеральными законами.

8.18. В случае отсутствия возможности уничтожения ПДн в течение указанных сроков Оператор осуществляет блокирование таких ПДн и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

## **9. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ**

9.1. В соответствии с требованиями нормативных документов Оператором создается система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

9.2. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

9.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками и сторонними лицами.

9.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПДн.

9.5. Основными мерами защиты ПДн, используемыми Организацией, являются:

9.5.1. Назначение лица ответственного за обработку ПДн, которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите ПДн.

9.5.2. Определение актуальных угроз безопасности ПДн при их обработке в ИСПДн и разработка мер и мероприятий по защите ПДн.

9.5.3. Разработка политики в отношении обработки персональных данных.

9.5.4. Установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечения регистрации и учета всех действий, совершаемых с ПДн в ИСПДн.

9.5.5. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями.

- 9.5.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей ПДн, обеспечение их сохранности.
- 9.5.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.
- 9.5.8. Сертифицированное программное средство защиты информации от несанкционированного доступа.
- 9.5.9. Сертифицированные межсетевой экран и средство обнаружения вторжения.
- 9.5.10. Соблюдение условий, обеспечивающих сохранность ПДн и исключающих несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн.
- 9.5.11. Установление правил доступа к обрабатываемым ПДн, обеспечение регистрации и учета действий, совершаемых с ПДн, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер.
- 9.5.12. Восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
- 9.5.13. Обучение работников Организации, непосредственно осуществляющих обработку ПДн, положениям законодательства Российской Федерации о ПДн, в том числе требованиям к защите ПДн, документам, определяющим политику Организации в отношении обработки персональных данных, локальным актам по вопросам обработки ПДн.
- 9.5.14. Осуществление внутреннего контроля.

## **10. ОСНОВНЫЕ ПРАВА СУБЪЕКТА ПДн**

- 10.1 Субъект ПДн вправе требовать от оператора уточнения его ПДн, 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. Обработка ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта ПДн.
- 10.3. Принятие на основании обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы разрешается только при наличии согласия в письменной форме субъекта ПДн или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта ПДн.
- 10.4. Если субъект ПДн считает, что Оператор осуществляет обработку его ПДн с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.
- 10.5. Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и компенсацию морального вреда в судебном порядке.

## **11. ОБЯЗАННОСТИ ОПЕРАТОРА ПДн**

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

11.2. Если предоставление ПДн является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн.

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

11.4. 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.

11.5. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к настоящей Политике, к сведениям о реализуемых требованиях к защите ПДн. Оператор в случае осуществления сбора ПДн с использованием информационных сетей обязан опубликовать в соответствующей информационной сети Политику и сведения о реализуемых требованиях к защите ПДн, а также обеспечить возможность доступа к указанному документу с использованием соответствующей информационной сети.

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

## **12. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

12.1. Политика является общедоступным документом.

12.2. Ответственность лиц, имеющих доступ к ПДн, определяется действующим законодательством Российской Федерации.