Проверки Роскомнадзора: что проверят инспекторы в клинике, как накажут за нарушения и как оспорить санкции

‹актион› МЦФЭР

Система Главный врач

Содержание

Автор-составитель

Роскомнадзор проверяет, как клиники защищают персональные данные пациентов и работников. Главврач должен быть уверен, что сотрудники выполняют все правила и верно оформляют документы. Наша книга поможет подготовиться к проверке и пройти ее без штрафов.

Светлана Сергеевна СУВОРОВА, кандидат медицинских наук, независимый эксперт по организации здравоохранения и управлению персоналом медорганизаций

Какие бывают проверки

Проверки Роскомнадзора бывают плановыми и внеплановыми, документарными и выездными.

Основанием для плановой проверки станет уведомление о начале обработки персональных данных, которое медорганизация направила в Роскомнадзор. Образец уведомления – в конце главы.

Затем инспекторы будут проверять клинику не чаще одного раза в три года. Чтобы узнать, придут ли к вам инспекторы в текущем году, нужно посмотреть план проверок на сайте Роскомнадзора или Генпрокуратуры.

> **Пример. Что может стать причиной плановой проверки**
> Врач-терапевт пожаловался в Роскомнадзор, что его персональные данные стали известны сотрудникам, которые не имеют к ним доступ. При этом врач не хочет, чтобы инспекторы проводили проверку по его персонифицированной жалобе. Роскомнадзор может включить медорганизацию в план проверок.

Роскомнадзор уведомит о проверке за три рабочих дня до ее начала.

Под внеплановую проверку медорганизация может попасть в четырех случаях.

1. У предписания, которое выдали сотрудники Роскомнадзора по итогам прошлой проверки, истек срок.
2. В ведомство поступила информация, что действия медорганизации причинили вред жизни или здоровью людей либо есть подобная угроза.
3. В Роскомнадзор поступило обращение от граждан или организаций.
4. Руководитель Роскомнадзора назначил внеплановую проверку по поручению Президента, Правительства или требованию прокурора.

Роскомнадзор уведомит о внеплановой проверке за 24 часа до ее начала.

Документарную проверку инспекторы проводят по документам, которые медорганизация представила по запросу Роскомнадзора. Срок, в течение которого нужно представить документы, 10 календарных дней с момента, как клиника получила уведомление. Если инспекторы выявят противоречия или несоответствия, могут запросить дополнительные сведения. Медорганизация предоставляет их в течение 10 календарных дней после того, как получит запрос.

Если при документарной проверке у инспектора возникли вопросы, главврачу и ответственным сотрудникам нужно постараться дать исчерпывающие пояснения и достоверные подтверждения. Это поможет избежать выездной ревизии.

Роскомнадзор уведомит о проверке за три рабочих дня до ее начала.

Выездную проверку контролеры назначат в трех случаях.

1. Медорганизация не представила документы в срок.
2. Ведомство по результатам документарной проверки выявило, что сведения недостоверны или предоставлены не полностью.
3. Инспекторы не могут оценить по представленным документам, правильно ли клиника организовала работу с персональными данными.

Продолжительность ревизии – не более 20 рабочих дней. Контролеры могут продлить срок выездной проверки, если есть обоснованная причина, например требуется экспертиза. Максимальный срок продления – 20 рабочих дней.

Если при проверке сотрудник Роскомнадзора узнает о нарушении, которое не входит в его компетенцию,

он вправе передать информацию в другое ведомство. Оно проведет свою внеплановую проверку. В итоге медорганизацию проверят два ведомства и выдадут два различных предписания. Избежать совместных проверок поможет памятка.

КАК ИЗБЕЖАТЬ СОВМЕСТНОЙ ПРОВЕРКИ РОСКОМНАДЗОРА И ДРУГОГО НАДЗОРНОГО ВЕДОМСТВА

1. При документарной проверке не нужно передавать в Роскомнадзор лишнюю информацию. Лучше представлять документы строго по запросу. Если инспектору понадобятся уточнения, он их запросит.

2. При выездной проверке главврачу нужно сделать так, чтобы работники минимально контактировали с ревизорами. Можно отвести инспектору изолированное помещение, поставить охрану. Главврач и другие представители администрации вправе присутствовать при беседе с работником. Не передавайте требуемый документ в папке, в которой он хранится. Извлеките его для инспектора.

3. Своевременно уничтожайте документы и персональные данные, срок хранения которых истек, составляйте акты об уничтожении.

Уведомление об обработке персональных данных

Уведомление об обработке (о намерении осуществлять обработку) персональных данных

Общество с ограниченной ответственностью «Медицина», ООО «Медицина», 7708123436, 1234567890123

(полное и сокращенное наименования (ИНН, ОГРН), фамилия, имя, отчество (при наличии) Оператора)

Адрес местонахождения: Москва, ул. Борисовская, д. 7. Почтовый адрес: 111111, Москва, ул. Пролетарская, д. 31

(адрес местонахождения и почтовый адрес Оператора)

руководствуясь:

Трудовым кодексом, Налоговым кодексом, Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», Гражданским кодексом, федеральными законами от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», от 08.01.1998 № 3-ФЗ «О наркотических средствах и психотропных веществах», от 17.09.1998 № 157-ФЗ «Об иммунопрофилактике инфекционных болезней», от 30.03.1999 № 52-ФЗ «О санитарно-эпидемиологическом благополучии населения», Законом РФ от 02.07.1992 № 3185-1 «О психиатрической помощи и гарантиях прав граждан при ее оказании», лицензией на осуществление медицинской деятельности от 11.11.2011 № 12345678910, согласием субъекта персональных данных на обработку персональных данных, уставом (утв. 11.11.2011)

(правовое основание обработки персональных данных)

с целью:

регистрации сведений физических лиц (субъектов персональных данных), необходимых для осуществления деятельности больничной организации, предусмотренной уставом, персональных данных работников, сведений об их профессиональной служебной деятельности в соответствии с Трудовым кодексом РФ, ведения бухгалтерского учета в соответствии с другими федеральными законами, определяющими случаи и особенности обработки персональных данных,

(цель обработки персональных данных)

осуществляет обработку:

фамилии, имени, отчества; года рождения; месяца рождения; даты рождения; места рождения; адреса; образования; профессии; доходов; СНИЛС, ИНН, стажа, данных документа, удостоверяющего личность,

(категории персональных данных)

принадлежащих:

работникам, их детям и родственникам.

(категории субъектов, персональные данные которых обрабатываются)

Обработка вышеуказанных персональных данных будет осуществляться путем:

сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи, удаления.

(перечень действий с персональными данными, общее описание используемых Оператором способов обработки персональных данных)

Для обеспечения безопасности персональных данных принимаются следующие меры:

Разработано и утверждено Положение об обработке персональных данных в «Медицине». Приказом от 01.08.2018 № 1 назначено лицо, ответственное за организацию обработки персональных данных – Сергеев С.А. (тел. 8-495-913-03-03). Опубликован и размещен на стенде организации документ, определяющий политику в отношении обработки персональных данных.

Разработаны локальные акты по вопросам обработки персональных данных. Осуществляется внутренний контроль соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных.

Работники, непосредственно осуществляющие обработку персональных данных, ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

Разработана модель угроз безопасности в информационной системе. Обеспечивается учет машинных носителей персональных данных.

Обеспечивается восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Разработаны правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечивается регистрация и учет всех действий, совершаемых с персональными данными в информационной системе персональных данных.

(описание мер, предусмотренных ст. 18.1 и 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств; фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты)

Сведения о наличии или об отсутствии трансграничной передачи персональных данных:

не осуществляется

(при наличии трансграничной передачи персональных данных в процессе их обработки указывается перечень иностранных государств, на территорию которых осуществляется трансграничная передача персональных данных)

Сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации:

Россия, Москва, ул. Борисовская, д. 7

(страна, адрес местонахождения базы данных,

собственный ЦОД

наименование информационной системы (базы данных))

Сведения об обеспечении безопасности персональных данных:

Определены места хранения персональных данных (материальных носителей). Определен перечень лиц, осуществляющих обработку персональных данных и имеющих к ним доступ. Обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. Обеспечен учет материальных носителей. Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, учтены в соответствующих журналах.

Исключена возможность неконтролируемого проникновения или пребывания посторонних лиц в помещениях, где ведется работа с персональными данными. Обеспечена сохранность носителей персональных данных и средств защиты информации. Лица, осуществляющие обработку ПДн без использования средств автоматизации, проинформированы о факте обработки ими персональных данных, а также об особенностях и правилах осуществления такой обработки.

(сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации)

Дата начала обработки персональных данных

1 августа 2018 года

(число, месяц, год)

Срок или условие прекращения обработки персональных данных:

ликвидация организации

(число, месяц, год или основание (условие), наступление которого повлечет прекращение обработки персональных данных)

Главный врач (должность) — (подпись) — Иванов А.В. (расшифровка подписи)

«1» августа 2018 г.

Что проверят

В ходе аудита сотрудники Роскомнадзора проверят:

- документы, которые содержат персональные данные, условия их хранения, формы согласий на обработку;
- локальные нормативные акты по работе с персональными данными;
- системы обработки персональных данных – на бумажных и электронных носителях, информационные технологии и технические средства защиты;
- информационные таблички о видеонаблюдении, если клиника его ведет.

Список документов, которые затребуют инспекторы, – в таблице ниже.

Документы, которые запросит Роскомнадзор при документарной проверке

Документ	В каких случаях инспекторы запросят документ
Уведомление об обработке персональных данных	Если медорганизация была обязана отправить уведомление
Свидетельство о государственной регистрации Устав или положение о медицинской организации	В любом случае
Приказ о назначении ответственного за работу с персональными данными и о допуске к персональным данным Положение об обработке персональных данных Формы согласия на обработку персональных данных Инструкция по заполнению документов, которые содержат персональные данные Журналы учета доступа к персональным данным	В любом случае
Акт о проведении проверки	Если нужно подтвердить, что медорганизация устранила все выявленные нарушения в срок
Предписание об устранении нарушений Копия протокола об административном правонарушении Представление прокурора Решение суда Документы, которые подтверждают, что медорганизация устранила нарушение и заплатила штраф	Если по результатам предыдущих проверок контролеры возбудили дело

Уведомление об обработке персональных данных. Медицинская организация – оператор персональных данных. Она должна уведомить Роскомнадзор об обработке данных и получить номер в реестре операторов. Юрист или другой ответственный сотрудник составляет уведомление и направляет его в ведомство.

Уведомление – документ установленной формы. После того, как медорганизация уведомила Роскомнадзор, он включает клинику в реестр операторов персональных данных.

Коммерческие медорганизации, которые работают только по договорам оказания медуслуг и используют персональные данные для их исполнения, могут не направлять уведомление.

Основание – подпункт 2 части 2 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ).

Обработка персональных данных, которые предоставляют медработники при трудоустройстве, также не требует уведомления. Это следует из подпункта 1 части 2 статьи 22 Закона № 152-ФЗ.

Положение об обработке персональных данных. Это основной документ медорганизации. Положение включает:

1. Перечни должностных лиц с полным и ограниченным доступами к персональным данным. Для лиц, которым доступ ограничен, – цели, для которых они могут использовать данные.
2. Правила доступа к персональным данным работников медучреждения и представителей сторонних организаций.
3. Правила предоставления и передачи персональных данных третьим лицам – не субъектам и не операторам персональных данных.
4. Правила регистрации и учета всех действий с персональными данными в информационной систе-

ме, описание базы персональных данных и информационных технологий, которые обеспечивают их обработку.

5 Правила хранения документов, которые содержат персональные данные.

6 Угрозы безопасности при обработке персональных данных на бумажных и электронных носителях, меры по преодолению этих угроз.

7 Отдел кадров знакомит с положением всех сотрудников медорганизации.

Политика обработки персональных данных. Документ информирует третьих лиц о том, как медорганизация обрабатывает их персональные данные. Клиника обязана разместить политику в электронном виде на своем сайте, а также в бумажном виде на информационном стенде. Если этого не сделать, медорганизацию оштрафуют на 15 000 – 30 000 руб. Ниже – образец политики обработки персональных данных.

Инструкция по заполнению документов, которые содержат персональные данные. Документ разъясняет, как заполнять разделы персональных данных в каждой форме первичной медицинской документации.

Журналы учета. Медорганизация должна вести четыре журнала: учета доступа к персональным данным; учета выдачи организациям и государственным органам персональных данных работников; регистрации однократного допуска на территорию медорганизации; учета проверок.

Журнал регистрации однократного допуска можно вести в произвольной форме. Ее утверждает приказом руководитель медорганизации.

Журнал учета проверок ведут по утвержденной форме – приложение 4 к приказу Минэкономразвития от 30.04.2009 № 141.

Сертификаты на средства защиты информации. Контролеры проверят, есть ли в медорганизации сертификаты на антивирусные программы, системы видеонаблюдения, контроля и управления доступом (СКУД), криптографические системы, межсетевые экраны.

Формы согласия на обработку персональных данных и соглашений о неразглашении. Сотрудники Роскомнадзора проверят оформленные согласия на всех работников и пациентов, а также соискателей, чьи персональные данные хранятся в кадровой службе в электронном виде и в виде заполненных анкет и резюме.

Также ведомство проверяет соглашения о неразглашении персональных данных пациентов и работников. Медицинский персонал подписывает соглашение о неразглашении данных пациентов, кадровая служба – о неразглашении данных работников, администрация – оба соглашения.

Вы можете скачать формы согласий на обработку персональных данных.

Форма согласия на обработку биометрических данных. На обработку биометрических данных требуется отдельное согласие (ст. 11 Закона № 152-ФЗ), его можно включить в основную форму.

Если медорганизация не использует биометрические данные, согласие можно не брать. Но если инспектор проверит конкретные случаи и решит, что биометрические данные обрабатывались, медорганизации придется обосновывать цель обработки.

Согласие субъекта на трансграничную передачу данных. Данное согласие должно быть, если медорганизация передавала персональные данные в другие страны (ст. 12 Закона № 152-ФЗ). Также необходимы документы, которые подтверждают, что организация зашифровала эти данные и направила по защищенным каналам в соответствии с ГОСТ 28147-89.

Согласие не нужно, если клиника передала данные для защиты жизни, здоровья субъекта и при этом согласие в письменной форме получить было невозможно (подп. 5 п. 4 ст. 12 Закона № 152-ФЗ).

Документы по обработке специальных категорий персональных данных. Обработка таких данных, как расовая принадлежность, национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимная жизнь, не допускается.

Исключение – случаи, которые перечислены в пункте 2 статьи 10 Закона № 152-ФЗ.

Конкретные ситуации могут быть связаны с выделением социальной помощи или назначением пенсии; защитой жизни, здоровья или жизненно важных интересов субъекта персональных данных или лица, которое не может предоставить свои персональные данные самостоятельно; установлением и соблюдением прав субъекта персональных данных (третьих лиц) или в связи с осуществлением правосудия; усыновлением детей; предоставлением или лишением гражданства РФ.

Если медорганизации приходилось обрабатывать такие данные, нужно подготовить документы, которые подтверждают, почему это было необходимо. Также обязательны документы, которые доказывают, что обработку прекратили сразу же, как только необходимость в этом отпала. Например, после того как сотрудник получил российское гражданство, копию паспорта иностранного государства из личного дела можно убрать.

Согласие на обработку персональных данных

Я, нижеподписавшийся <Ф. И. О. полностью>, проживающий по адресу <по месту регистрации>, паспорт <серия и номер>, выдан <дата и название выдавшего органа>, в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» подтверждаю свое согласие на обработку <название и адрес медицинского учреждения> (далее – Оператор) моих персональных данных, включающих фамилию, имя, отчество, пол, дату рождения, адрес места жительства, контактный телефон(ы), реквизиты полиса ОМС (ДМС), страховой номер индивидуального лицевого счета в Пенсионном фонде РФ (СНИЛС), данные о состоянии моего здоровья, заболеваниях, случаях обращения за медицинской помощью в медико-профилактических целях, в целях установления медицинского диагноза и оказания медицинских услуг при условии, что их обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну. В процессе оказания Оператором мне медицинской помощи я предоставляю право медицинским работникам передавать мои персональные данные, содержащие сведения, составляющие врачебную тайну, другим должностным лицам Оператора в интересах моего обследования и лечения.

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение. Оператор вправе обрабатывать мои персональные данные посредством внесения их в электронную базу данных, включения в списки (реестры) и отчетные формы, предусмотренные документами, регламентирующими предоставление отчетных данных (документов) по ОМС (договором ДМС).

Оператор имеет право во исполнение своих обязательств по работе в системе ОМС (по договору ДМС) на обмен (прием и передачу) моими персональными данными со страховой медицинской организацией <название> и территориальным Фондом ОМС с использованием машинных носителей или по каналам связи с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа, при условии, что их прием и обработка будут осуществляться лицом, обязанным сохранять профессиональную тайну.

Срок хранения моих персональных данных соответствует сроку хранения первичных медицинских документов (медицинской карты) и составляет <25 лет>.

Передача моих персональных данных иным лицам или иное их разглашение может осуществляться только с моего письменного согласия.

Настоящее согласие дано мной <дата> и действует бессрочно.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

В случае получения моего письменного заявления об отзыве настоящего согласия на обработку персональных данных Оператор обязан прекратить их обработку в течение периода времени, необходимого для завершения взаиморасчетов по оплате оказанной мне до этого медицинской помощи.

Контактный телефон(ы) <...> и почтовый адрес <...>

Подпись субъекта персональных данных _____

Согласие на обработку персональных данных на сайте клиники

Согласие на обработку персональных данных

Регистрируясь (авторизуясь), оставляя заявки на «Бесплатную консультацию» и «Обратный звонок» на сайте Клиники _____ ООО «_____» _____
(домен сайта)

и в мобильном приложении «_____», Пользователь соглашается
(название клиники или юр. лица)

с настоящим Согласием на обработку персональных данных (далее – Согласие), составленным на основании Политики обработки персональных данных.

Действуя свободно, своей волей и в своем интересе, а также подтверждая свою дееспособность, Пользователь дает свое согласие _____ расположенному
(наименование, ИНН)

по адресу _____, на обработку своих персональных данных
(использующему домен)

со следующими условиями:

данное Согласие дается на обработку персональных данных как без использования средств автоматизации, так и с их использованием.

согласие дается на обработку следующих персональных данных, не являющихся специальными или биометрическими:

Ф. И. О.;

дата рождения;

номера контактных телефонов;

адреса электронной почты;

место работы, адрес места работы и занимаемая должность;

сведения о местоположении;

какие страницы открывает и на какие кнопки нажимает Пользователь;

ip-адрес.

3. Персональные данные не являются общедоступными.

4. Цель обработки персональных данных:

обработка входящих запросов физических лиц и (или) юридических лиц с целью оказания консультирования;

аналитика действий физического лица на веб-сайте и функционирования веб-сайта;

проведение рекламных и новостных рассылок.

5. Основаниями для обработки персональных данных являются:

статья 24 Конституции РФ;

статья 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

устав ООО «_____»;

настоящее согласие на обработку персональных данных.

6. В ходе обработки с персональными данными будут совершены следующие действия:

сбор;

запись;

систематизация;

накопление;

хранение;

уточнение (обновление, изменение);

извлечение;

использование;

блокирование;

удаление;

уничтожение.

7. Персональные данные обрабатываются до момента отзыва физическим лицом согласия на обработку персональных данных на домене _____.

8. Согласие может быть отозвано субъектом персональных данных или его представителем:

путем направления письменного заявления в _____ (наименование клиники или юр. лица) или его

представителю по адресу, указанному в начале данного Согласия;

путем направления электронного запроса на адрес _____.

9. В случае отзыва субъектом персональных данных или его представителем согласия на обработку персональных данных _____ (наименование клиники или юр. лица)

вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2–11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

10. Настоящее Согласие действует все время до момента прекращения обработки персональных данных, указанных в пунктах 7 и 8 данного Согласия.

Политика обработки и защиты персональных данных медицинской организации

УТВЕРЖДАЮ
Главный врач ГБУЗ «Больница»
И.И. Иванов
«17» ноября 2018 г.

Политика обработки и защиты персональных данных медицинской организации ГБУЗ «Больница»

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) составлена в соответствии с пунктом 2 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и является основополагающим внутренним регулятивным документом медицинской организации ГБУЗ «Больница» (далее – Организация или Оператор), определяющим ключевые направления ее деятельности в области обработки и защиты персональных данных (далее – ПДн), оператором которых является Организация.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его 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:

- Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановлением Правительства РФ от 01.11.2012 № 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), в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

1.5. Организация имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее размещения на сайте, если иное не предусмотрено новой редакцией Политики.

1.6. Действующая редакция хранится в месте нахождения Организации по адресу: г. Москва, ул. Новая Басманная, д. 22, электронная версия Политики – на сайте по адресу: gbuzbolnitsa.ru.

1.7. Персональные данные обрабатывают с использованием средств автоматизации или без них.

1.8. Организация до начала обработки персональных данных обязана уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных согласно частям 1 и 3 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.9. Приказом главного врача учреждения от 14.11.2018 № 22 ответственным лицом за организацию обработки персональных данных в соответствии с пунктом 1 статьи 18.1 Закона № 152-ФЗ назначен инженер по работе с персональными данными Григорьев Е.В.

2. Термины и принятые сокращения

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

2.2. 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.

2.3. 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.

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

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

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

2.7. 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.

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

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

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

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

2.12. 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.

2.13. 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 элемен-

тов, 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 информационных систем персональных данных Организации, 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 Организации не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в Организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Организацией ПНд 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. Обработка персональных данных

4.1. Получение ПДн

4.1.1. 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.

4.1.2. 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.

4.1.3. 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 Организацией, определяется в соответствии с законодательством и определяется внутренними регулятивными документами Организации.

4.2. Обработка ПДн

4.2.1. 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 Российской Федерации 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 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.

4.2.2. Цели обработки ПДн:
- обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12.04.2010 № 61-ФЗ «Об обращении лекарственных средств» и от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными постановлением Правительства РФ от 04.10.2012 № 1006;
- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений.

4.2.3. Категории субъектов персональных данных

В Организации обрабатываются ПДн следующих субъектов:
- физических лиц, состоящих с учреждением в трудовых отношениях;
- физических лиц, являющихся близкими родственниками сотрудников учреждения;
- физических лиц, уволившихся из учреждения;
- физических лиц, являющихся кандидатами на работу;
- физических лиц, состоящих с учреждением в гражданско-правовых отношениях;
- физических лиц, обратившихся в учреждение за медицинской помощью.

4.2.4. 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.

4.3. Обработка персональных данных ведется:
- с использованием средств автоматизации;
- без использования средств автоматизации.

4.4. Хранение ПДн

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

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

4.4.3. ПДн субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).

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

4.4.5. 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.

4.5. Уничтожение ПДн

4.5.1. 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.

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

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

4.6. Передача ПДн

4.6.1. Организация передает ПДн третьим лицам, если субъект выразил свое согласие на такие действия или передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

4.6.2. 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).

5. Защита персональных данных

5.1 Подсистемы защиты персональных данных

5.1.1. В соответствии с требованиями нормативных документов Организацией создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

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

5.1.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работе.

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

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

5.2.1. 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.

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

5.2.3. Разработка политики в отношении обработки персональных данных.

5.2.4. Установление правил доступа к ПДн, обрабатываемым в ИСПД, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПД.

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

5.2.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей ПДн, обеспечение их сохранности.

5.2.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

5.2.8. Сертифицированное программное средство защиты информации от несанкционированного доступа.

5.2.9. Сертифицированные межсетевой экран и средство обнаружения вторжения.

5.2.10. Соблюдение условий, обеспечивающих сохранность ПДн и исключающих несанкционированный доступ к ним, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн.

5.2.11. 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.

5.2.12. Восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

5.2.13. Обучение работников Организации, непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Организации в отноше-

нии обработки персональных данных, локальным актам по вопросам обработки персональных данных.

5.2.14. Осуществление внутреннего контроля и аудита.

5.2.15. Сотрудники Организации, непосредственно осуществляющие обработку персональных данных, должны быть ознакомлены под подпись до начала работы с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, настоящей Политикой, локальными актами по вопросам обработки персональных данных, с данным Положением и изменениями к нему.

6. Основные права субъекта ПДн и обязанности Организации

6.1. Основные права субъекта ПДн

6.1.1. Субъект ПДн имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Оператором способы обработки персональных данных;
- наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Законом № 152-ФЗ;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Законом № 152-ФЗ или другими федеральными законами.

6.1.2. Субъект ПДн 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.

6.2. Обязанности Организации

6.2.1. Организация обязана:
- при сборе ПДн предоставить информацию субъекту об обработке его ПДн;
- в случаях, если ПДн были получены не от субъекта ПДн, уведомить субъекта;

– при отказе в предоставлении ПДн субъекту разъясняются последствия такого отказа;
– опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;
– 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;
– давать ответы на запросы и обращения субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн;
– не сообщать персональные данные субъекта ПДн третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым кодексом РФ или иными федеральными законами;
– не сообщать персональные данные субъекта ПДн в коммерческих целях без его письменного согласия;
– предупреждать лиц, получающих персональные данные субъекта ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;
– разрешать доступ к персональным данным субъекта ПДн только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные субъекта ПДн, которые необходимы для выполнения конкретных функций.

7. Ответственность за нарушение норм, регулирующих обработку и защиту ПДн

7.1. Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных субъектов ПДн, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Какие документы должен предъявить инспектор

При выездной проверке инспектор предъявляет руководителю медорганизации или его уполномоченному представителю копию приказа о проверке и служебное удостоверение проверяющего.

В приказе сотрудники Роскомнадзора прописывают фамилии, имена, отчества, должности инспекторов, наименование медорганизации и ее адрес, цели, задачи, основания проверки, перечень документов для проверки, виды и объемы мероприятий по контролю, сроки и условия проверки. На приказе должна стоять печать территориального подразделения Роскомнадзора, которое проводит проверку.

Если в приказе есть ошибки, например, название медорганизации указано неверно, руководитель вправе не допускать инспектора в учреждение.

Проверяющим может быть только тот человек, чьи фамилия, имя и отчество указаны в приказе. В случае сомнений руководитель медорганизации или уполномоченный им сотрудник вправе потребовать у проверяющего паспорт. Если состав должностных лиц изменился, у инспектора должен быть приказ, который подтверждает изменения.

Если сомневаетесь в подлинности документов, которые предъявил инспектор, или подозреваете, что документы неправильно оформлены, обратитесь в территориальное подразделение Роскомнадзора.

Проверка без приказа Роскомнадзора – грубое нарушение закона (п. 4 ч. 2 ст. 20 Федерального закона от 26.12.2008 № 294-ФЗ). Результаты такой проверки недействительны. Чтобы их отменить, юристы клиники обращаются в вышестоящий орган госнадзора или в суд.

Какие права есть у главврача при проверке

Главный врач вправе присутствовать при проверке, знакомиться с ее результатами, указывать в акте проверки о своем ознакомлении, согласии или несогласии с результатами проверки и действиями инспекторов. Главврач может заявить о нарушении прав медорганизации при проверке, обжаловать действия инспекторов в административном или судебном порядке.

Если у главврача есть замечания, возражения или он обнаружил несоответствия, то вправе потребовать, чтобы инспектор внес их в акт или оформил как приложение к акту.

Руководитель медорганизации обязан предоставить инспектору в полном объеме информацию и документы, которые связаны с целями, задачами и предметом проверки; обеспечить доступ инспектора, а также привлеченных экспертов на территорию, в помещения, к оборудованию, где обрабатываются персональные данные; присутствовать при проверке лично или заблаговременно уполномочить на это кого-то из подчиненных; представить инспектору журнал учета проверок по типовой форме.

Какие права есть у инспектора при проверке

На что инспектор имеет право и чего он не должен делать во время проверки, представлено в таблице.

Что вправе и что не вправе делать инспектор Роскомнадзора во время проверки

Инспектор вправе	Инспектор не вправе
Проводить проверки в установленном порядке и при наличии документов беспрепятственно в любое время суток	Проверять то, что не относится к полномочиям Роскомнадзора
Запрашивать и безвозмездно получать от работодателей документы, объяснения, информацию, которые необходимы для проверки	Проводить выездную проверку в отсутствие руководителя или его уполномоченного представителя. Исключение — проверка по основанию «причинение вреда жизни или здоровью граждан»
Получать доступ к информационным системам персональных данных в режиме просмотра	Требовать документы, информацию, которые не относятся к предмету проверки, изымать оригиналы документов
Предъявлять предписания об устранении нарушений	Распространять информацию, которая составляет государственную, коммерческую, служебную, иную охраняемую законом тайну
Приостанавливать или прекращать обработку персональных данных, если медорганизация проводит ее с нарушением законодательства	Нарушать сроки проверки
Требовать уточнить, блокировать или уничтожить недостоверные или полученные незаконным путем персональные данные	Выдавать предписания или предложения о проведении проверок на коммерческой основе
Привлекать к проверке экспертов и экспертные организации	—

Как инспектор оформит результаты проверки

По результатам проверки инспектор составляет акт. Один из экземпляров акта он вручает руководителю медорганизации. Если инспектор не представил акт руководителю, то результаты проверки можно признать недействительными (п. 6 ч. 2 ст. 20 Закона № 294-ФЗ).

В акте проверки инспекторы указывают:

1. Установленные в ходе проверки факты соответствия или несоответствия методов обработки и способов хранения персональных данных законодательству в области работы с персональными данными.
2. Подробные сведения о нарушениях медорганизацией обязательных требований в сфере работы с персональными данными.
3. Случаи неповиновения законному распоряжению или требованию инспектора Роскомнадзора, а также случаи, когда инспектору не давали исполнять служебные обязанности (если такие случаи были).
4. Запись о том, что выявленное нарушение устранено, если это произошло в ходе проверки.

Если в результате проверки инспектор выявил нарушения, то вместе с актом он выдает руководителю предписание об устранении нарушений.

Если нарушения влекут административную или уголовную ответственность, инспектор вправе составить протокол и передать его в правоохранительные органы – прокуратуру или суд. Правоохранительные органы возбуждают административное или уголовное дело. По результатам рассмотрения этого дела в суде медорганизацию привлекают к ответственности.

Что грозит за нарушения по персональным данным

В таблице представлены виды нарушений в области персональных данных и санкции за них.

Как накажут клинику за нарушения в области персональных данных

Вид нарушения	Штраф для медорганизации, руб.	Примеры нарушений
Обработка персональных данных не соответствует заявленным целям	30 000—50 000	Медорганизации просят пациентов дать согласие на обработку данных о семейном, имущественном положении, образовании, профессии, доходах и т. д. Если пациент не подписывает документ, ему не оказывают помощь
Нет письменного согласия пациента на обработку персональных данных	15 000—75 000	Медорганизации не берут письменное согласие на обработку биометрических данных (ст. 11 Закона № 152-ФЗ). К ним относятся дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес, изображение человека. Рентгеновские и флюорографические снимки к биометрическим данным не относятся (разъяснения Роскомнадзора от 30.08.2013)
Медорганизация не разместила в открытом доступе документ, который определяет политику обработки персональных данных и требования к защите	15 000—30 000	Документ есть в медорганизации, но пациенты не имеют возможности с ним ознакомиться. Документ принят, но касается только работников медорганизации
Пациенту не предоставили информацию об обработке его персональных данных	20 000—40 000	Медорганизация не сообщает пациенту, кто именно обрабатывает его персональные данные, сколько они будут храниться в медорганизации
Медорганизация не выполнила требования пациента уточнить персональные данные	25 000—45 000	Медорганизация запросила у пациента сведения, которые не нужны для целей обработки, и не уничтожила их, когда пациент того потребовал
Медорганизация допустила несанкционированный доступ к персональным данным	25 000—50 000	Работник медорганизации случайно уничтожил персональные данные пациента, хотя не должен был иметь к ним доступа

Как оспорить результаты проверки

В каких случаях проверку можно аннулировать, как внести возражения в акт проверки, куда и в какой срок подать заявление – читайте далее.

Когда проверку признают недействительной. Результаты проверки можно аннулировать, если инспектор или другие сотрудники Роскомнадзора грубо нарушили закон (ст. 20 Закона № 294-ФЗ).

> **Ситуация. Когда инспектор вправе провести проверку без уведомления и в отсутствие руководителя**
>
> Если основание для внеплановой проверки — «вред жизни или здоровью граждан», Роскомнадзор не направляет уведомление в проверяемую организацию. Такую проверку он вправе проводить также в отсутствие руководителя или уполномоченного лица.

Как внести возражения в акт проверки. По результатам проверки инспектор составляет акт по форме, которую утвердил приказ Минэкономразвития от 30.04.2009 № 141. Руководитель медорганизации получает один экземпляр акта. При этом он расписывается, что ознакомился с актом или что отказывается ознакомиться.

Если у главврача есть возражения и замечания, инспектор обязан внести их в акт проверки или оформить как приложение. Возражения повысят шанс оспорить отдельные факты, выявленные в результате проверки, и избежать ответственности за них. Оспорить саму проверку на основании возражений к акту нельзя.

Инспектор должен внести замечания главврача до того, как он подпишет акт, – после подписи вносить изменения в документ запрещено. Инспектор не вправе отказаться вносить замечания в акт. Если он все же отказался, главврачу не следует подписывать акт.

Если инспектор внес возражения в акт проверки, за клиникой сохраняется право на обжалование действий и решений инспектора Роскомнадзора в установленном законом порядке. Если не внес, хотя и был обязан, акт тоже можно обжаловать.

Как обжаловать результаты проверки. Если инспектор или Роскомнадзор грубо нарушили закон, клиника может подать жалобу в вышестоящий орган госнадзора письменно или на личном приеме. Жалобу на инспектора территориального отделения Роскомнадзора направляют руководителю этого отделения, на руководителя территориального отделения – руководителю Роскомнадзора, на руководителя Роскомнадзора – министру связи и массовых коммуникаций.

Ведомства рассмотрят заявление в течение 30 дней. В случаях, предусмотренных законодательством РФ, срок рассмотрения обращения могут продлить, но максимум на 30 дней – об этом уведомляют заявителя. В уведомлении о продлении будет указано, на основании какого положения законодательства продлевается проверка.

Госорган может полностью или частично удовлетворить заявленные претензии медорганизации. Он отменит или изменит принятые по результатам проверки решения либо вынесет новое решение. Также медорганизация может получить отказ в удовлетворении жалобы.

Чтобы оспорить акт проверки или предписание об устранении нарушений, медорганизация направляет заявление руководителю территориального отделения Роскомнадзора. Срок для этого – 15 дней с момента, когда пришел акт. К заявлению следует приложить документы, которые подтвердят, что возражения обоснованны (ч. 12 ст. 16 Закона № 294-ФЗ).

Роскомнадзор рассмотрит возражения за 10 рабочих дней. Затем в течение трех дней сообщит решение в письменной форме.

Если досудебное обжалование не принесло результата, клиника вправе оспорить решение в суде. Юристы подают заявление в течение трех месяцев со дня получения решения Роскомнадзора. Они представляют результаты досудебного обжалования, а также документы, которые доказывают нарушения при проверке или опровергают факты, на которые инспектор указал в акте.

Если в досудебном или судебном порядке будет доказано, что неправомерные действия инспектора нанесли вред или материальный ущерб медорганизации, то убытки, в том числе упущенная выгода, восполнят за счет средств регионального бюджета.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ НАРУШЕНИЙ ИНСПЕКТОРОВ

1. Плановую проверку не включили в ежегодный план проверок Роскомнадзора.
2. Для проверки нет оснований или они недостаточны. Это решает руководитель территориального отделения Роскомнадзора или вышестоящих отделений, когда рассматривает поступившую жалобу.
3. Роскомнадзор не уведомил медорганизацию о начале проверки или нарушил сроки, в которые необходимо уведомить. Для плановой проверки срок уведомления составляет три дня, для внеплановой — 24 часа.
4. У инспектора нет приказа о проверке, служебного удостоверения или данные документы оформлены с ошибками.
5. Инспектор не указан в приказе о проверке и нет приказа о замене инспектора.
6. В проверке участвуют эксперты, которые не прошли аккредитацию или работают по трудовому или гражданско-правовому договору в проверяемой медорганизации.
7. Руководителя или уполномоченного лица не было в медорганизации во время проверки.
8. Ведомство нарушило сроки проверки.
9. Инспектор не представил акт проверки.
10. Инспектор проверял то, что не относится к полномочиям Роскомнадзора или предмету проверки.
11. Инспектор нарушил регламент проверки.