



МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РЕСПУБЛИКИ ДАГЕСТАН
ГБУ РД «РЕСПУБЛИКАНСКАЯ КЛИНИЧЕСКАЯ БОЛЬНИЦА
СКОРОЙ МЕДИЦИНСКОЙ ПОМОЩИ» (ГБУ РД «РКБСМП»)

367003 РД г. Махачкала, пр. Пирогова, 3, тел.62-06-64 E-mail: rb2rd@mail.ru ОГРН 1080562000474 ИНН 0562070341

«15» 05 2025 г

ПРИКАЗ

№ 34-0

г. Махачкала

Об утверждении положения о видеонаблюдении
в ГБУ РД «РКБСМП»

В целях обеспечения антитеррористических мероприятий, безопасности персонала, пациентов и сохранности имущества ГБУ РД «РКБСМП», в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства РФ от 13 января 2017г. № 8 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства здравоохранения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства здравоохранения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)»,

ПРИКАЗЫВАЮ:

1. Организовать работу систем видеонаблюдения в ГБУ РД «РКБСМП».
2. Утвердить Положение о видеонаблюдении в ГБУ РД «РКБСМП» (Приложение №1).
3. Утвердить образец заявления о предоставлении доступа к системе видеонаблюдения (приложение №2).
4. Назначить уполномоченного специалиста по обеспечению контроля за бесперебойной работой оборудования системы видеонаблюдения.
5. Назначить ответственным за соблюдение правил эксплуатации системы видеонаблюдения ответственного специалиста.
6. Начальнику отдела ПОиИБ Муслимовой З.М. разместить Положение о видеонаблюдении в ГБУ РД «РКБСМП» на официальном сайте лечебного учреждения.
7. Начальнику отдела кадров внести соответствующие изменения в трудовые договоры.
9. Контроль над выполнением настоящего распоряжения оставляю за собой.

Главный врач

М.Р. Иманалиев

ПОЛОЖЕНИЕ **о системе видеонаблюдения в ГБУ РД «РКБСМП»**

1. Общие положения

1.1. Настоящее положение разработано в соответствии Федеральным законом РФ «О персональных данных» от 27 июля 2006 г. № 152-ФЗ, Постановлением Правительства РФ от 17 ноября 2007 г. № 781 "Об утверждении Положения о данных при их обработке в информационных системах персональных данных", ч. 13 ст. 30 Федерального закона от 30.12.2009 г. № 384 «Технический регламент о безопасности зданий и сооружений», п. 16 Постановления Правительства РФ от 13 января 2017 г. № 8 "Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства здравоохранения Российской Федерации и объектов деятельности Министерства здравоохранения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)».

1.2. Под видеонаблюдением понимается непосредственное осуществление видеонаблюдения посредством использования видеокамер для получения видеоинформации об объектах и помещениях, а также запись полученного изображения и его хранение для последующего использования.

1.3. Система открытого видеонаблюдения в ГБУ РД «РКБСМП» (далее по тексту – «Лечебное учреждение», «организация», «больница») является элементом общей системы безопасности лечебного учреждения, направленной на обеспечение безопасности при оказании медицинских услуг, поддержание трудовой дисциплины и порядка, предупреждение возникновения чрезвычайных ситуаций и обеспечение объективности расследования в случаях их возникновения.

1.4. Система видеонаблюдения является открытой, ведется с целью обеспечения безопасности работников организации и не может быть направлена на сбор информации о конкретном человеке.

2. Основные термины и определения

Видеонаблюдение - процесс, осуществляемый с применением оптико-электронных устройств, предназначенных для визуального контроля.

Видеоинформация (видеоизображение, видеоматериалы) - информация, регистрируемая камерами наблюдения.

Видеорегистратор, видеосервер — электронное устройство, предназначенное для приёма и хранения видеоизображения с камер наблюдения, а также

удаленного воспроизведения или ретрансляции видеоизображения с помощью специального сетевого программного обеспечения.

Камера наблюдения - оптико-электронное устройство, предназначенное для визуального контроля.

Участники лечебного процесса - сотрудники, пациенты, посетители.

3. Описание системы видеонаблюдения

3.1 Система представляет собой программно-аппаратный комплекс, не входящий в перечень специальных технических средств, предназначенных для негласного получения информации, включающий:

- камеры видеонаблюдения;
- видеомониторы;
- источники бесперебойного питания;
- видеорегистраторы и видеосерверы;
- сетевую (кабельную) инфраструктуру;
- средства хранения видеоинформации;
- программное обеспечение для просмотра изображений.

3.2 Зоны установки камер наблюдения:

- в местах возможного несанкционированного проникновения посторонних лиц (центральных входах, запасных выходах), по периметру зданий лечебного учреждения;
- в коридорах;
- на лестничных пролетах;
- на входных группах и на этажах зданий;
- в помещениях для проведения досуговых мероприятий;
- в фойе;
- в помещениях постоянного хранения материальных ценностей;
- в зонах контроля кассовых узлов;
- в других помещениях по решению главного врача;
- в актовом залах.

3.3. Режим видеонаблюдения:

- система функционирует 24 часа в сутки, 7 дней в неделю, в том числе в выходные и праздничные дни;
- режим видеонаблюдения отдельных объектов, места размещения, перечень, вид и тип устанавливаемых видеокамер утверждается отдельными нормативными актами лечебного учреждения.

3.4. Отображение процесса видеозаписи камер в режиме реального времени производится на экране, установленном на рабочем месте уполномоченного специалиста, назначенным главным врачом больницы, в зоне доступного наблюдения с целью своевременного реагирования на возникновение признаков и причин опасных ситуаций.

3.5. В процессе видеонаблюдения производится запись видеоинформации на материальные носители (жёсткие диски) специализированных видеосерверов и видеорегистраторов.

3.6. Срок хранения записей составляет не более 30 дней, после этого срока записи автоматически уничтожаются. Если камеры видеонаблюдения зафиксировали конфликтную (нестандартную) ситуацию, то для таких записей по указанию главного врача устанавливается специальный срок хранения до 3 лет. Их хранение осуществляется на компьютере уполномоченного специалиста.

3.7. Хранение видеозаписей осуществляется на видеорегистраторах, входящих в состав установленной в лечебном учреждении системы видеонаблюдения. Места нахождения видеорегистраторов определяются главным врачом.

Для помещений либо мест нахождения видеорегистраторов организуется режим обеспечения безопасности.

В этих целях должна исключаться возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц либо места нахождения регистраторов должны быть закрыты на ключ.

3.8. Программное обеспечение на видеорегистраторах и компьютерах, позволяющее просматривать видеозаписи с видеорегистраторов, должно быть защищено паролями доступа. Данные пароли задает уполномоченный специалист и передает специалистам организации, осуществляющей техническое обслуживание системы видеонаблюдения, для установки на видеорегистраторы.

3.9. Пароли доступа подлежат замене при смене организации, осуществляющей техническое обслуживание системы видеонаблюдения, а также по решению уполномоченного специалиста или главного врача.

3.10. Уполномоченный специалист по решению главного врача может передать пароль доступа к отдельной подсистеме видеонаблюдения назначенным сотрудникам по их личному заявлению (приложение №1). Данные заявления хранятся у уполномоченного специалиста.

4. Порядок организации системы видеонаблюдения

4.1. Решение об установке системы видеонаблюдения и местах размещения видеокамер принимается главным врачом лечебного учреждения.

4.2. Работники медицинской организации, работающие в помещениях, в которых установлена система видеонаблюдения, а также при установке дополнительных подсистем видеонаблюдения, должны в письменной форме выразить свое согласие или письменно обозначить свое несогласие на введение данной системы (подписание соглашения об изменении условий труда). Если работник не согласен на изменение условий трудового договора, то после выполнения процедур, предусмотренных Трудовым кодексом РФ (письменное уведомление о предстоящих изменениях, предложение другой работы) трудовой договор с ним может быть расторгнут по пункту 7 статьи 77 ТК РФ. Кроме того, ответственные лица, имеющие доступ к системе видеонаблюдения: уполномоченный специалист, сотрудники специалисты

организации, осуществляющей техническое обслуживание системы видеонаблюдения, сотрудники охранной организации должны дать письменное обязательство о неразглашении служебной информации ограниченного доступа и персональных данных в соответствии с п. 7 ст.86 ТК РФ, ст. 7 Закона № 152-ФЗ «О персональных данных».

4.3. Сотрудники, вновь принимаемые на работу, выражают свое согласие на проведение видеоконтроля путем заполнения формы согласия на обработку персональных данных и подписания трудового договора, включающего условие о видеонаблюдении на рабочем месте.

4.4. Пациенты и посетители больницы, которые потенциально могут попасть в зону видеокамер, информируются о наличии видеонаблюдения путем размещения специальных объявлений или информационный знаков (табличек) перед входом на территорию (здание) лечебного учреждения или в помещениях, где ведется видеонаблюдение.

4.5. Система видеонаблюдения входит в систему контроля доступа и включает в себя ряд устройств: камеры, мониторы, записывающие устройства. Выполняет различные функции: опознавание знакомого человека, опознавание незнакомого человека, сотрудников организации, чтение государственного регистрационного номера автомобиля, опознавание медицинского оборудования и лиц, работающих с ней.

4.6. Запрещается использование устройств, предназначенных для негласного получения информации (скрытых камер).

4.7. Запрещается установка системы видеонаблюдения в туалетных и ваннных (душевых) комнатах, других помещениях и в иных местах, связанных с осуществлением личных нужд работников и пациентов.

4.8. Функции по обеспечению контроля бесперебойной работы элементов системы видеонаблюдения, проведение регулярного технического контроля, профилактическое обслуживание системы, работы по ремонту, модернизации и расширению системы, обеспечению отказоустойчивости на программном и аппаратном уровнях, размещению предупреждающих табличек о ведении видеонаблюдения, нормативному обеспечению системы видеонаблюдения осуществляет уполномоченный специалист, либо лицо, временно его замещающее (с помощью специалистов организации, осуществляющей техническое обслуживание системы видеонаблюдения).

5. Цели и задачи системы видеонаблюдения

5.1. Система видеонаблюдения призвана выполнять следующие задачи:

5.1.1. Повышение эффективности действий при возникновении нештатных и чрезвычайных ситуаций.

5.1.2. Обеспечение противопожарной защиты зданий и сооружений.

5.1.3. Обеспечение антитеррористической защиты работников и территории Учреждения, охраны порядка и безопасности.

5.1.4. Совершенствование системы информирования и оповещения работников Учреждения об угрозе возникновения кризисных ситуаций.

5.1.5. Пресечение противоправных действий со стороны работников Учреждения и пациентов.

5.1.6. Контроль качества и безопасности оказания медицинской помощи.

5.1.7. Контроль соблюдения работниками трудовой дисциплины.

5.2. Видеонаблюдение осуществляется с целью документальной фиксации возможных противоправных действий, которые могут нанести вред имуществу. В случае необходимости материалы видеозаписей, полученных камерами видеонаблюдения, могут быть использованы в качестве доказательства в уголовном или гражданском судопроизводстве для доказывания факта совершения противоправного действия, а также для установления личности лица, совершившего противоправное действие.

6. Меры по обеспечению безопасности персональных данных, хранение данных видеонаблюдения и передача третьим лицам

6.1. В тех случаях, когда система видеонаблюдения позволяет отслеживать деятельность сотрудников на рабочем месте или в иных помещениях, закрытых для общего доступа, такое наблюдение будет считаться обработкой персональных данных.

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

6.3. Обработка персональных данных должна осуществляться на законной основе и ограничиваться достижением конкретных, заранее определенных и законных целей.

Не допускается обработка персональных данных, не совместимая с целями сбора персональных данных.

6.4. Хранение персональных данных должно осуществляться не дольше, чем этого требуют цели обработки персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей. Лечебное учреждение относится к местам свободного посещения, и для обеспечения необходимой степени антитеррористической защищенности ГБУ РД «РКБСМП» обязана иметь систему видеонаблюдения, позволяющую с учетом количества устанавливаемых камер и мест их размещения обеспечивать непрерывное видеонаблюдение потенциально опасных участков и критических элементов объекта (территории), архивирование и хранение данных не менее 1 месяца (п. 16 Постановления Правительства РФ от 13 января 2017 г. № 8 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства здравоохранения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства здравоохранения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)»). Система видеонаблюдения предполагает запись информации на жесткий диск видеорегистратора, которая не подлежит

несанкционированной перезаписи на другие носители и длительному хранению, передаче третьим лицам, уничтожается автоматически по мере заполнения памяти жесткого диска. Минимальный срок хранения видеозаписей составляет 1 месяц, после этого срока запись подлежит уничтожению путем циклической перезаписи жесткого диска.

6.5. Отображение процесса видеозаписи камер в режиме реального времени производится на экране, установленном на рабочем месте в кабинете уполномоченного специалиста (главного врача по необходимости) в зоне доступного наблюдения с целью своевременного реагирования на возникновение признаков и причин опасных ситуаций.

6.6. Права полного доступа («администратор») к системе видеонаблюдения, имеет главный врач и уполномоченный специалист. Обеспечением конфиденциальности являются пароли доступа к информации видеорегистраторов, хранящиеся у уполномоченного специалиста.

6.7. Просмотр записанных изображений может осуществляться с разрешения главного врача ответственными лицами. В целях реализации задач обозначенных в п 5.1, приказом главного врача, дополнительно могут быть назначены лица из числа сотрудников учреждения, для осуществления контрольных проверок видеозаписей системы видеонаблюдения, на наличие обозначенных приказом нарушений, с ограничением объектов наблюдения в рамках выделенных полномочий и правами доступа к системе «только просмотр». Для защиты публичных интересов (т.е. выявления факта совершения правонарушения) в просмотре могут участвовать лица, изображенные на записи, сотрудники правоохранительных органов и органов следствия (при наличии заявления о совершении противоправных действий).

6.8. Для обеспечения объективности расследования в случаях возникновения чрезвычайных ситуаций и (или) происшествий и служебного расследования, нарушений Правил внутреннего трудового распорядка, нарушений порядков оказания медицинской помощи, противоправных действий со стороны работников Учреждения или иных лиц на территории и в помещениях ГБУ РД «РКБСМП», соответствующие видеофрагменты могут быть сохранены уполномоченным специалистом, либо лицом, временно его замещающим (с помощью специалистов организации, осуществляющей техническое обслуживание системы видеонаблюдения) с диска видеорегистратора на внешний носитель с соблюдением необходимых мер защиты конфиденциальной информации, срока, необходимого для выполнения целей обработки, либо с увольнением соответствующего работника, сохраненные видеофрагменты уничтожаются (за исключением случаев необходимости использования данных в судебном разбирательстве).

6.9. В целях обеспечения защиты персональных данных третьих лиц, в соответствии со ст. 89 ТК РФ по требованию работника ему предоставляются только те записи, которые не содержат изображений других работников или иных граждан.

6.10. Передача информации о видеонаблюдении в соответствующие службы и государственные органы производится только по их письменным запросам в случаях, предусмотренных действующим законодательством.

6.11. Использование изображения лиц, зафиксированных видеокамерой, без их согласия возможно только в следующих случаях:

- если изображение используется в государственных, общественных или публичных интересах;
- если изображение получено при съемке, которая проводится в местах, открытых для свободного посещения или на публичных мероприятиях (съездах, конференциях, совещаниях), за исключением случаев, когда такое изображение является основным объектом использования.

7. Порядок доступа к видеоматериалам и передача третьим лицам

7.1. Информация, записываемая системой видеонаблюдения, является конфиденциальной, не подлежит перезаписи с жестких дисков специализированных видеосерверов, редактированию и передаче третьим лицам.

7.2. Вся записываемая видеoinформация может быть использована только в соответствии с действующим законодательством Российской Федерации и настоящим Положением.

7.3. Доступ к видеoinформации, хранящейся на жестких дисках специализированных видеосерверов, может осуществляться только по локальной сети системы видеонаблюдения без передачи по сети Интернет.

7.4. Допуск к просмотру видеоматериалов, хранящихся на жестких дисках специализированных видеосерверов и видеорегистраторов, имеют главный врач и уполномоченный специалист.

7.5. Работники охранной организации, состоящей с Учреждением в договорных отношениях (далее работники охраны) с целью выполнения возложенных на них охранных услуг. Работники охраны имеют право просмотра видеoinформации только в режиме онлайн при исполнении возложенных на них обязанностей по охране лечебного учреждения в период своего рабочего времени (дежурства);

7.6. Просмотр необходимых видеоматериалов может осуществляться иными работниками, имеющими соответствующие права допуска, по указанию главного врача. К просмотру могут также привлекаться должностные лица больницы (в части их касающейся), а также работники лечебной организации, сотрудники охраны, имеющие отношение к событиям, зафиксированным системой видеонаблюдения. Для защиты публичных интересов (т.е. выявления факта совершения правонарушения) в просмотре могут участвовать лица, изображенные на записи, либо (законные представители) и сотрудники правоохранительных органов.

7.7. Передача видеоматериалов третьей стороне допускается только в исключительных случаях (по мотивированному запросу следственных или судебных органов, а также по запросу граждан, изображенных на записи). Вопрос о передаче материалов решает главный врач. Передача видеоматериалов осуществляется уполномоченным лицом, выполняющим функции администратора системы видеонаблюдения.

8. Ответственность за нарушения правил обработки персональных данных

8.1. Лица, виновные в нарушении требований Федерального закона «О персональных данных», несут предусмотренную законодательством Российской Федерации ответственность.

8.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом, а также требований к защите персональных данных подлежат возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

8.3. Работникам Учреждения запрещается: препятствовать работе системы видеонаблюдения путем регулировки направления (обзора) камер видеонаблюдения, загораживать, закрывать камеры или каким-либо иным способом препятствовать производству видеонаблюдения, отключать электропитание камер системы видеонаблюдения. За причинение материального вреда и порчу камер системы видеонаблюдения работники медицинской организации несут ответственность в соответствии с действующим законодательством Российской Федерации.

8.4. Просмотр и копирование видеозаписей на носители информации (для передачи главному врачу) с установленных видеорегистраторов осуществляется на компьютере, установленном на посту охраны представителями подрядной организации обслуживающих систему охранного видеонаблюдения. Лица, имеющие право доступа к просмотру видеозаписей, осуществляют их просмотр и обработку только в присутствии уполномоченного специалиста на основании соответствующего решения ответственного за видеонаблюдение либо главного врача.

8.5. В случае обнаружения несанкционированного доступа к видеорегистратору и (или) видеозаписи (взлом входной двери в помещение) специалист организации, осуществляющей техническое обслуживание системы видеонаблюдения, в кратчайшие сроки обязаны в письменной форме обязан доложить о случившемся для принятия соответствующих мер.

9. Порядок введения системы видеонаблюдения

9.1. Система видеонаблюдения вводится в Учреждении на основании приказа главного врача.

9.2. Ответственное лицо за внедрение, организацию работы и контроль за работой системы видеонаблюдения назначается приказом главного врача.

9.3. Главный врач с целью технического обслуживания и ремонта оборудования системы видеонаблюдения имеет право заключить договорные отношения со специализированной организацией. При заключении договорных отношений со сторонней организацией в проект договора необходимо вносить условие о неразглашении потенциальным контрагентом

(его работниками) конфиденциальной, служебной и технической информации (в том числе сведений, содержащих персональные данные), полученной при исполнении договорных обязательств, ответственности за соблюдение конфиденциальности информации, полученной с видеокамер.

10. Заключительные положения

10.1 Настоящее Положение, а также вносимые в него изменения и дополнения вступают в силу с момента его утверждения главным врачом лечебного учреждения.

Мухомов З.М. Мухомова