

Утверждаю
Главный врач
ГАОУЗ РКИБ
А.В.Багаутдинов
«__» ____ 20__ г



ПОЛОЖЕНИЕ
о системе видеонаблюдения в
Государственном автономном учреждении здравоохранения
«Республиканская клиническая инфекционная больница имени проф.
А.Ф.Агафонова»
Министерства здравоохранения Республики Татарстан
(ГАОУЗ «РКИБ»)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее положение разработано в соответствии с Федеральным законом РФ "О персональных данных" от 27.07.2006 № 152-ФЗ, Постановлением Правительства РФ от 17.11.2007 N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", федеральным законом от 06.03.2006 г. №35 «О противодействии терроризму», федеральным законом от 21.11.2011 г. № 323-ФЗ «Об основах здоровья граждан РФ», Постановлением правительства РФ от 13.01.2017 №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)".

1.2. Под видеонаблюдением понимается непосредственное осуществление видеонаблюдения, а также осуществление видеонаблюдения с функцией аудиозаписи посредством использования видеокамер для получения видео и аудиоинформации об объектах и помещениях, а также запись полученных данных и хранение для последующего использования.

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

1.4. Система открытого видеонаблюдения в Государственном автономном учреждении здравоохранения «Республиканская клиническая инфекционная больница имени проф. А.Ф.Агафонова» (далее по тексту - Организация) является элементом общей системы безопасности Организации, направленной на обеспечение безопасности, контроля качества оказания медицинских услуг, защиты персонала, пациентов и посетителей от угроз терроризма и противоправных действий, несанкционированного вторжения, поддержание дисциплины и порядка в Организации, предупреждение возникновения чрезвычайных ситуаций и обеспечение сохранности имущества.

1.5. Настоящее Положение обязательно для работников, пациентов и (или) посетителей Организации. Настоящее Положение подлежит размещению на официальном сайте Организации и находится в свободном доступе для работников и посетителей.

1.6. С целью противодействия терроризму и совершению противоправных действий, Организация обязана вести наблюдение за состоянием обстановки на всей территории, архивировать и хранить данные не менее 30 дней (постановление Правительства от 13.01.2019 г. № 8). Система видеонаблюдения в медицинской организации необходима для защиты посетителей, пациентов и персонала от угроз терроризма, и противоправных действий, несанкционированного вторжения (ч.13 ст. 30 Федерального закона от 30.12.2009г. № 384 «Технический регламент о безопасности зданий и

сооружений»), а также контроля качества оказываемых в организации медицинских услуг.

2. ПОРЯДОК ОРГАНИЗАЦИИ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

2.1. Сотрудники Организации выражают свое согласие на проведение видеоконтроля путем подписания формы согласия на обработку персональных данных.

2.2. Посетители организации информируются о системе видеоконтроля путем размещения специальных информационных табличек в зонах видимости видеокамер.

2.3. Система видеонаблюдения Организации входит в систему контроля доступа и включает в себя ряд устройств: камеры, микрофоны, мониторы, записывающие устройства, коммутационное оборудование.

2.4 Система видеонаблюдения организации выполняет следующие функции: запись видеопотока, запись аудио потока, хранение, передача, воспроизведение информации.

2.5. Места установки видеокамер в Организации определяются по мере необходимости в соответствии с конкретными задачами.

2.6. Установка системы видеонаблюдения осуществляется в соответствии с ее целями и задачами в Организации.

2.7. Видеокамеры устанавливаются в местах, открытых для общего доступа (территория, въезды, входы в здание, коридоры, парковки), а также в помещениях, где оказываются медицинские услуги (палаты, боксы, процедурный кабинет, кабинеты врачей и т.п).

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

3. ЦЕЛИ И ЗАДАЧИ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

3.1. Целью системы видеонаблюдения является создание условий для антитеррористической защищенности в Организации, безопасности персонала, посетителей и пациентов, сохранности имущества, своевременного реагирования при возникновении чрезвычайных ситуаций, контроля доступа на территорию, осуществление внутреннего контроля качества и безопасности медицинской деятельности, контроля качества оказываемых в организации медицинских услуг.

3.2. Задачами организации видеонаблюдения являются:

- контроль за обстановкой в помещениях и на территории Организации, обеспечение защиты от несанкционированного проникновения на территорию и в здание посторонних лиц и транспортных средств;
- своевременное реагирование при возникновении опасных и чрезвычайных ситуаций, в т.ч. вызванных террористическими актами на территории Организации;

- охрана жизни, предупреждение и минимизация рисков травматизма работников Организации и посетителей;
- установление достоверности фактов при расследовании несчастных случаев (запись события, регистрация времени, места и участников, причин получения травмы работником и посетителей);
- разрешения конфликтных ситуаций и споров и обеспечения объективности расследования в случаях их возникновения;
- обеспечение противопожарной защиты зданий и сооружений;
- повышение ответственности всех сотрудников за качество своей профессиональной деятельности и выполнение должностных обязанностей;
- раннее выявление причин и признаков опасных ситуаций, их предотвращение и устранение;
- пресечение противоправных действий со стороны работников Организации и посетителей;
- охрана имущества, предупреждение и устранение причин (последствий) деятельности, приводящей к порче имущества, а также предупреждение случаев хищения имущества организации и/или работников/посетителей;
- информационное обеспечение принятия решений;
- предоставление информации по запросам соответствующих служб и государственных органов в случаях, предусмотренных действующим законодательством.

3.3. Система видеонаблюдения должна обеспечивать:

- видео/аудио фиксацию текущего состояния объектов видеонаблюдения;
- сохранение архива видеозаписей для последующего анализа;
- воспроизведение ранее записанной информации;
- оперативный доступ к архиву видеозаписей за конкретный период времени и с определённых видеокамер.

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

4. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. 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.

4.2. Организация 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.

4.3. 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.

4.4. 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.

5. ПРОСМОТР, ХРАНЕНИЕ ДАННЫХ ВИДЕОНАБЛЮДЕНИЯ И ПЕРЕДАЧА ДАННЫХ ТРЕТЬИМ ЛИЦАМ

5.1. Запись камер видеонаблюдения осуществляется постоянно (24 часа в сутки) и подлежит хранению не менее 30 дней.

5.2. Система видеонаблюдения предполагает запись информации на жесткий диск видеорегистратора, которая не подлежит перезаписи и длительному хранению, удаляется автоматически по мере заполнения памяти жесткого диска.

При возникновении и фиксации конфликтных ситуаций, фактов правонарушений записи могут подлежать хранению в течении срока исковой давности.

5.3. Запись информации видеонаблюдения является конфиденциальной, не подлежит перезаписи с жесткого диска видеорегистратора, редактированию, передачи третьим лицам.

5.4. Отображение процесса видеонаблюдения в режиме реального времени производится на экраны, установленные:

- на постах отделений;
- на постах охраны въездной группы;
- в мониторинговой комнате.

5.5. Доступ к просмотру записей видеонаблюдения, хранящимся установленный период на жестком диске видеорегистратора, имеют Главный врач Организации, а также замещающие его лица в рамках установленных полномочий. На основании разрешения Главного врача Организации другие работники Организации могут быть допущены к просмотру записей видеонаблюдения, при условии принятия ими на себя обязательств о неразглашении персональных данных третьих лиц. Просмотр записей видеонаблюдения и прослушивание аудиофайлов производится с разрешения Главного врача Организации (по письменному запросу).

5.6. Обеспечением конфиденциальности является пароль доступа к информации видеорегистратора, а также разграничение полномочий Администраторов и пользователей системы видеонаблюдения

5.7. Для защиты публичных интересов (выявление факта совершения правонарушения) в просмотре могут участвовать лица, изображенные на записи, сотрудники полиции по письменному запросу.

5.8. Передача записей камер видеонаблюдения третьей стороне допускается только в исключительных случаях (по письменному запросу следственных и судебных органов, а также по письменному запросу работников, изображенных на видеозаписи). Вопрос о передаче записей решает Главный врач Организации.

5.9. Администрирование системы видеонаблюдения, мониторинг работоспособности, контроль записи, установку паролей, разграничение доступов, осуществляют сотрудники отдела АСУ.

6. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ ПРАВИЛ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Лица, виновные в нарушении требований Федерального закона "О персональных данных", несут предусмотренную законодательством Российской Федерации ответственность.

6.2. 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.

6.3. Работникам Организации 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 Организации несут ответственность в соответствии с действующим законодательством Российской Федерации.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Настоящее положение, изменения, дополнения к нему, утверждаются приказом главного врача Организации.

7.2. Ознакомление работников Организации с настоящим положением, изменениями и дополнениями к нему, проводится в обязательном порядке под роспись.