



УТВЕРЖДЕНО

Приказом и. о. главного врача
ГБУ РО «СИБ» в г. Новочеркасске
от 07.2025 № 28-1

ПОЛОЖЕНИЕ

О СИСТЕМЕ ВИДЕОНАБЛЮДЕНИЯ

Государственного бюджетного учреждения Ростовской области
«Специализированная инфекционная больница» в г. Новочеркасске

1. Общее положение

1.1. Настоящее положение разработано в соответствии с Федеральным законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации, Трудового кодекса Российской Федерации от 30.12.2001 № 197-ФЗ, Постановлением 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)», Федеральным законом РФ «О персональных данных» от 27 июля 2006 г. № 152-ФЗ, Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных 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», Федерального закона от 21.11.2011 г. № 323-ФЗ (ред. От 26.03.2022) «Об основах охраны здоровья граждан в Российской Федерации».

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

1.3. Система открытого видеонаблюдения ГБУ РО «СИБ» в г. Новочеркасске (далее – Учреждение) является элементом общей системы безопасности 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, предупреждение противоправных действий на объектах.

1.4. Система видеонаблюдения является открытой, ведется в целях повышения эффективности режима безопасности Учреждения, обеспечения личной безопасности работников и пациентов, минимизации рисков материальных потерь, соблюдения пропускного и внутриобъектового режима, осуществления контроля сохранности имущества работников, осуществления контроля доступа к помещениям хранения наркотических средств и психотропных веществ.

2. Основные термины и определения

Видеонаблюдение — процесс, осуществляемый с применением оптикоэлектронных 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 в себя:

- 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 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.

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 Учреждения.

3.4. Отображение процесса видеозаписи камер в режиме реального времени производится на экране, компьютера секретаря - машинистки.

3.5. Хранение видеозаписей осуществляется на видеорегистраторах, входящих в состав установленной в Учреждении системы видеонаблюдения.

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 и опечатаны.

3.8. Программное обеспечение на видеорегистраторах и компьютерах, позволяющее просматривать видеозаписи с видеорегистраторов, должно быть защищено паролями доступа. Данные пароли задает назначенный руководителем ответственный за информационную безопасность Учреждения.

3.9. Пароли доступа могут заменяться при смене организации, осуществляющей техническое обслуживание системы видеонаблюдения, а также по решению ответственного за информационную безопасность Учреждения.

3.10. Ответственный за информационную безопасность Учреждения может передать пароль доступа к отдельной подсистеме видеонаблюдения при заключении договора с организацией на её обслуживание, по заявлению руководителя организации (Приложение №2). Данные заявления хранятся у ответственного за информационную безопасность.

4. Порядок организации системы видеонаблюдения

4.1. Установление видеонаблюдения осуществляется в соответствии с действующим законодательством Российской Федерации и настоящим положением. Решение об установке системы видеонаблюдения и местах размещения видеокамер принимается главным врачом Учреждения.

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

4.3. 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, чтение государственного регистрационного номера автомобиля.

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

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

4.6. 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 ответственный за систему видеонаблюдения, назначенный приказом руководителя Учреждения.

4.7. При вводе в эксплуатацию новых объектов, изменении количества или места расположения камер видеонаблюдения в настоящее Положение вносятся изменения.

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 сохранности товарно-материальных ценностей Учреждения, личного имущества персонала.

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

5.1.4. Своевременное информирование и оповещения работников Учреждения об угрозе возникновения кризисных ситуаций.

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

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 соответствующее 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 не будет считаться обработкой персональных данных, съемка рабочего процесса не является раскрытием персональных данных работника и не подпадает под действие главы 14 ТК РФ, а также не нарушает конституционные права работника на неприкосновенность частной жизни, поскольку осуществляется в целях, связанных с трудовой деятельностью работника, а не для того, чтобы установить обстоятельства его частной жизни либо личную или семейную тайну.

Согласие работников на осуществление их съемки и включение соответствующих условий в трудовой договор не требуется.

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

6.3. Территория Учреждения относится к местам свободного посещения.

Для обеспечения необходимой степени антитеррористической защищенности объектов Учреждения необходимо:

6.3.1. Иметь систему видеонаблюдения, позволяющую с учетом количества устанавливаемых камер и мест их размещения обеспечивать непрерывное видеонаблюдение потенциально опасных участков и критических элементов объекта (территории).

6.3.2. Осуществлять архивирование и хранение данных не менее месяца п. 16 Постановления Правительства РФ от 13 января 2017 г. № 8 «Об утверждении требований 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)».

6.4. В рамках системы видеонаблюдения осуществляется 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 (один) месяц, после этого срока запись подлежит уничтожению путем циклической перезаписи жесткого диска. В случае фиксации на видеокамерах нестандартной либо конфликтной ситуации на территории Учреждения видео и аудиофайлы подлежат хранению в течение не менее 3-х лет.

6.5. Отображение процесса видеозаписи камер в режиме реального времени производится на экране, установленном исключительно на рабочем месте ответственного лица в зоне доступного наблюдения с целью своевременного реагирования на возникновение признаков и причин опасных ситуаций.

6.6. Право полного доступа («администратор») к системе видеонаблюдения, имеет: главный врач или лицо, его замещающее, ответственный за информационную безопасность Учреждения, ответственный за соблюдение правила эксплуатации системы видеонаблюдения, её бесперебойной работы и профилактического обслуживания.

Просмотр видеозаписей посторонними лицами, не обладающими правами полного доступа к системе видеонаблюдения, запрещен.

7. Порядок доступа к видеоматериалам и передача третьим лицам

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

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

7.3. Просмотр необходимых видеоматериалов может осуществляться иными работниками, имеющими соответствующие права допуска, по указанию главного врача. К просмотру могут также привлекаться должностные лица Учреждения (в части их касающейся), а также работники Учреждения, 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.

7.4. Просмотр записанных изображений может осуществляться с письменного разрешения главного врача либо лица его замещающего. Для защиты публичных интересов (т.е. выявления факта совершения правонарушения) в просмотре могут участвовать лица, изображенные на записи, сотрудники правоохранительных органов, органов следствия и дознания (при наличии заявления о совершении противоправных деяний).

7.5. Для обеспечения объективности расследования в случаях возникновения чрезвычайных ситуаций и (или) происшествий и служебного расследования, нарушений Правил внутреннего трудового распорядка, противоправных действий со стороны работников Учреждения или иных лиц на территории и в помещениях Учреждения соответствующие видеофрагменты могут быть сохранены руководителем с диска видеорегистратора на внешний носитель с соблюдением необходимых мер защиты конфиденциальной информации.

7.6. В соответствии со ст. 5 Закона «О персональных данных» после завершения срока, необходимого для выполнения целей обработки, либо с увольнением соответствующего работника, сохраненные видеофрагменты уничтожаются (за исключением случаев необходимости использования данных в судебном разбирательстве).

7.7. 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.

7.8. 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.

7.9. 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.

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

8.3. 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.

8.4. Работникам Учреждения, а также иным любым лицам запрещается: препятствовать работе системы видеонаблюдения путем регулировки направления (обзора) камер видеонаблюдения, загромождать, закрывать камеры или каким-либо иным способом препятствовать производству видеонаблюдения, отключать электропитание камер системы видеонаблюдения.

8.5. За причинение материального вреда и порчу камер системы видеонаблюдения участники лечебного процесса несут ответственность в соответствии с действующим законодательством Российской Федерации.

9. Заключительные положения

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

9.2. Настоящее положение, изменения и дополнения к нему, доводится персоналу, размещается на сайте Учреждения.

Перечень мест установки камер видеонаблюдения

№	Структурное подразделение	Адрес	Общее количество видеокамер	Количество наружных видеокамер	Количество внутренних видеокамер
1.	Администрация, инфекционное отделение №1	г. Новочеркасск ул. Б. Хмельницкого, 3.	19	14	5