



Министерство здравоохранения Челябинской области
Государственное автономное учреждение здравоохранения
«Городская клиническая больница № 11 г. Челябинск»
(ГАУЗ «ГКБ № 11 г. Челябинск»)

ПРИКАЗ

«12» 11 2025 г.

№ 320

г. Челябинск

О введении в действие «Положения о
системе видеонаблюдения в ГАУЗ «ГКБ
№ 11 г. Челябинск»

В соответствии с Постановлением Правительства Российской Федерации 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)» и в целях обеспечения антитеррористической защищенности объектов ГАУЗ «ГКБ № 11 г. Челябинск»

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие с 14.11.2025 г «Положение о системе видеонаблюдения в ГАУЗ «ГКБ № 11 г. Челябинск» (приложение № 1).
2. Заместителю главного врача по хозяйственным вопросам Милованцеву Е.Ю. организовать обеспечение зданий и территорий информационными знаками (табличками), где ведется видеонаблюдение.
3. Контроль исполнения настоящего приказа оставляю за собой.

Главный врач

Н. В. Горлова

УТВЕРЖДЕНО

приказом ГАУЗ «ГКБ № 11 г. Челябинск»

от 12.11.2025 № 320

ПОЛОЖЕНИЕ
о системе видеонаблюдения в ГАУЗ «ГКБ № 11 г. Челябинск»

1. Общие положения.

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)»;

- Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Федерального закона от 30.12.2009 г. № 384 «Технический регламент о безопасности зданий и сооружений» ч. 13 ст. 30;

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

1.2 Система видеонаблюдения в ГАУЗ «ГКБ № 11 г. Челябинск» (далее учреждение) является элементом общей системы безопасности учреждения, направленной на обеспечение безопасности при оказании медицинских услуг, на поддержание трудовой дисциплины и порядка, на прогнозирование и предупреждение возникновения чрезвычайных ситуаций и обеспечение объективности расследования в случаях их возникновения, на прогнозирование и предупреждение противоправных действий на объектах, аварийных ситуаций на объектах путём контроля за параметрами процессов обеспечения функционирования объектов и определения отклонений их текущих значений от нормативных.

1.3 Система видеонаблюдения является открытой, ведется в целях:

- повышения эффективности действий при возникновении нештатных и чрезвычайных ситуаций, а также оперативной ликвидации таких ситуаций, в т.ч. вызванных террористическими актами;
- повышения эффективности режима безопасности в учреждении;
- обеспечения личной безопасности работников и пациентов, минимизации рисков материальных потерь в учреждении, повышения эффективности обеспечения режима конфиденциальности и безопасности персональных данных, обрабатываемых в учреждении;
- осуществления контроля сохранности имущества работников и учреждения, осуществления контроля доступа к помещениям хранения наркотических средств и психотропных веществ;
- обеспечения противопожарной защиты зданий и сооружений, соблюдения порядка в помещениях, в том числе в ночное время и в нерабочие дни;
- усиления контроля трудовой дисциплины на территории и в помещениях учреждения;
- совершенствования системы информирования и оповещения работников, посетителей и пациентов об угрозе возникновения кризисных ситуаций.

2. Порядок организации, размещения и допуска к системам видеонаблюдения.

2.1 Установление видеонаблюдения в учреждении осуществляется в соответствии с настоящим положением.

2.2. Решение о местах установки камер системы видеонаблюдения принимается главным врачом по согласованию с начальником отдела по информационной безопасности и оформляется соответствующим приказом.

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

2.4. Система видеонаблюдения включает в себя ряд устройств: камеры, мониторы, записывающие устройства. Данная система выполняет различные функции: опознавание человека, чтение государственного регистрационного номера автомобиля.

2.5. При организации и размещении систем видеонаблюдения не используются устройства, предназначенные для негласного получения информации (скрытых камер). При организации и размещении систем видеонаблюдения не используется установка системы видеонаблюдения в туалетных и ваннных (душевых) комнатах, палатах, кабинетах и других помещениях, связанных с осуществлением личных нужд работников и пациентов.

3. Цели и задачи системы видеонаблюдения.

3.1 Система видеонаблюдения призвана выполнять следующие задачи:

- контроль исполнения обязанностей сотрудников согласно трудового договора;
- обеспечение сохранности товарно-материальных ценностей;
- обеспечение безопасности персонала на рабочих местах;
- контроль и организация безопасности в помещении.

3.2. Видео- аудио- наблюдение осуществляется с целью документальной фиксации возможных противоправных действий, которые могут нанести вред работникам учреждения, посетителям, пациентам, имуществу.

3.3. 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, хранение данных видеонаблюдения и передача третьим лицам.

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 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 включении соответствующих условий в трудовой договор не требуется.

4.2. Для обеспечения необходимой степени антитеррористической защищенности учреждение обязано:

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

4.2.2. 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)».

4.4. 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.

4.5. 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.

4.6. Право полного доступа («администратор») к системе видеонаблюдения, имеет: главный врач или лицо, его замещающее, начальник отдела по информационной безопасности.

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

4.8. 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 начальником отдела по информационной безопасности с диска видеорегистратора на внешний носитель с соблюдением необходимых мер защиты конфиденциальной информации.

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

5. Ответственность за нарушения правил обработки персональных данных.

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

5.2. 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,

5.3. За причинение материального вреда и порчу камер системы видеонаблюдения работники учреждения несут ответственность в соответствии с действующим законодательством Российской Федерации.

Заместитель главного врача по ГО и МР

 Е. В. Зеленко

Согласовано:

Начальник отдела по информационной безопасности

 А.А. Обручников