Государственное автономное учреждение здравоохранения
«Прокопьевская городская больница»

ПРИКАЗ

от «06» 02 2024г. № 175

г. Прокопьевск

Об утверждении положения
о видеонаблюдении в ГАУЗ ПГБ

В целях обеспечения антитеррористических мероприятий, безопасности персонала, пациентов и сохранности имущества ГАУЗ ПГБ, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Организовать работу систем видеонаблюдения на объектах ГАУЗ ПГБ.
2. Утвердить Положение о видеонаблюдении в ГАУЗ ПГБ и ввести его в действие с 15 февраля 2024г. согласно приложению №1.
3. Назначить лицом, ответственным за установку и эксплуатацию оборудования системы видеонаблюдения, системного администратора (Анискин И.Б.).
4. Назначить лицом, ответственным за предоставление доступа к месту хранения записей видеонаблюдения, начальника отдела информационных технологий (Дюбин А.Н., Анискин И.Б.).
5. Специалисту по связям с общественностью разместить Положение о видеонаблюдении в ГАУЗ ПГБ на официальном сайте в срок до 26 февраля 2024г.
6. Руководителям структурных подразделений ознакомить работников с Положением о видеонаблюдении в ГАУЗ ПГБ под роспись.
7. Заместителю главного врача по кадрам (Тимершина О.Н.) внести изменения в Правила внутреннего трудового распорядка, включив информацию о внедрении в ГАУЗ ПГБ системы видеоконтроля и ее функционирование.
8. Контроль за исполнением настоящего приказа возложить на заместителя главного врача по АХЧ (Кульков С.А.).

Главный врач ГАУЗ ПГБ М.В. Шмулевич

Приложение № 1
к Приказу ГАУЗ ПГБ
«06» 02 2024 года № 175

Положение
о системе видеонаблюдении в Государственном автономном учреждении здравоохранения «Прокопьевская городская больница»

I.Общие положения

1.1. Настоящее положение разработано в соответствии со статьей 21 Трудового Кодекса РФ, Федеральными законами № 35-ФЗ от 06.03.2006 «О противодействии терроризму» (ред. от 06.07.16), № 114-ФЗ от 25.07.2002 «О противодействии экстремистской деятельности» (ред. от 23.11.2015), № 152 – ФЗ от 27.07.2006 «О персональных данных», Указом Президента Российской Федерации от 15.02.2006 года №116 «О мерах по противодействию терроризму».
1.2. Система открытого видеонаблюдения в Государственном автономном учреждении здравоохранения «Прокопьевская городская больница» (далее – ГАУЗ ПГБ, Учреждение) является элементом общей системы безопасности, действующей совместно с системами охранно-пожарной и тревожной сигнализации и направленной на обеспечение безопасности функционирования рабочего процесса сотрудников Учреждения, пациентов и посетителей ГАУЗ ПГБ, профилактики возникновения предпосылок террористических актов, случаев экстремистских проявлений, предупреждения аварий, происшествий, чрезвычайных ситуаций и обеспечение объективности расследования в случаях их возникновения, а также поддержания дисциплины и порядка в Учреждении.
1.3. Система видеонаблюдения является открытой, ведется с целью обеспечения безопасности пациентов, а также сотрудников и их трудового процесса и не может быть направлена на сбор информации о конкретном человеке.
1.4. Фото и видео, аудио съемка сотрудниками Учреждения на территории Учреждения запрещена!
1.5. Любая иная фото, видео и аудио съемка сотрудников и их трудового процесса на территории Учреждения допустима только на основании согласия главного врача по письменному запросу.
1.6. Настоящее Положение обязательно для работников и посетителей ГАУЗ ПГБ. Каждый сотрудник подлежит ознакомлению с настоящим Положением под роспись.

II. Основные понятия и сокращения

В настоящем Положении применяются следующие основные понятия и сокращения:
2.1. Система охранная телевизионная (СОТ) - система видеонаблюдения, представляющая собой телевизионную систему замкнутого типа, предназначенную для противокриминальной защиты объекта.
2.2. Аналоговая система охранная телевизионная - система, в которой видеосигнал от видеокамер до видеомонитора и/или видеорегистратора передается в аналоговом виде, не подвергаясь аналого-цифровому преобразованию.
2.3. Несанкционированные действия (НСД) - действия в отношении технического средства (ТС), не предусмотренные нормативными (НД) и (или) эксплуатационными документами на ТС конкретного вида (например, несанкционированный доступ, несанкционированный просмотр).

2.4. СОТ - система охранная телевизионная. В Учреждения используются следующие СОТ:
- аналоговые, - цифровые, - комбинированные.
2.5. Детектор движения - устройство или функция СОТ, формирующие сигнал извещения о тревоге при обнаружении движения в поле зрения видеокамеры.
2.6. Противокриминальная защита сотрудников, посетителей, объектов и имущества - деятельность, осуществляемая с целью обеспечения криминальной безопасности Учреждения.

II.Цель и задачи

2.1. Цель системы видеонаблюдения: создание условий для обеспечения безопасности трудового процесса, своевременного реагирования при возникновении предпосылок террористических актов, случаев экстремистских проявлений, предупреждения аварий, происшествий, чрезвычайных ситуаций и обеспечение объективности расследования в случаях их возникновения, а также поддержания дисциплины и порядка в ГАУЗ ПГБ, принятие необходимых мер по оказанию помощи и защите участников трудового процесса в случае возникновения чрезвычайного происшествия.
2.2. Задачи мероприятий по обеспечению безопасности Учреждения путем установки систем видеонаблюдения:
- защита сотрудников, пациентов их прав и интересов, имущества от неблагоприятных воздействий;
- раннее выявление причин и признаков опасных ситуаций, их предотвращение и устранение;
- предупреждение и минимизация рисков травматизма сотрудников;
- предупреждение, устранение причин (последствий) деятельности, приводящей к порче имущества.

III. Порядок организации системы видеонаблюдения

3.1. Решение об установке видеонаблюдения может быть принято главным врачом ГАУЗ ПГБ в соответствии с Федеральными Законами.
3.2. СОТ устанавливается в следующих зонах, позволяющих с учетом количества устанавливаемых камер и мест их размещения, обеспечивать непрерывное видеонаблюдение:
- в местах возможного несанкционированного проникновения посторонних лиц;
- в местах повышенного риска возникновения травмоопасных ситуаций;
3.2.1. Видеоконтроль в Учреждении ведется круглосуточно.
3.3. Сотрудники Учреждения, которые потенциально могут попасть в зону видеонаблюдения, информируются о дате начала видеонаблюдения. Для оповещения могут быть использованы следующие формы:
- размещение специальных объявлений перед входом на территорию, на которой ведется видеонаблюдение;
- информирование сотрудников на общих собраниях, структурных совещаниях.
3.4. Посетители Учреждения информируются о системе видеоконтроля путем размещения специальных информационных табличек в зонах видимости видеокамер.

IV. Просмотр, хранение данных видеонаблюдения и передача данных третьим лицам

4.1. Система видеонаблюдения предполагает запись информации на жесткий диск видеорегистратора, которая не подлежит длительному хранению, уничтожается

автоматически по мере заполнения памяти жесткого диска в течение 30 дней с момента записи.

4.2. Запись информации видеонаблюдения является конфиденциальной, не подлежит перезаписи с жесткого диска, редактированию, передачи третьим лицам (исключительно, в случае совершения правонарушения перезапись и передача информации для расследования допускается только по решению главного врача).

4.3. Доступ к просмотру записей видеонаблюдения, сохраняющимся установленный период на жестком диске, производится с письменного разрешения главного врача ГАУЗ ПГБ.

4.4. Доступ к просмотру записей видеонаблюдения, хранящимся установленный период на жестком диске, имеют:

- главный врач ГАУЗ ПГБ (неограниченно по времени);
- заместитель главного врача по АХЧ (неограниченно по времени);
- системный администратор видеонаблюдения Учреждения (неограниченно по времени);
- начальник отдела информационных технологий (неограниченно по времени);
- специалист по ГО и ЧС Учреждения (в случае возникновения ЧС);
- начальник юридического отдела (при поступлении запроса правоохранительных органов).

Обеспечением конфиденциальности является пароль доступа к информации, хранящийся у перечисленных лиц.

Срок хранения записи видеонаблюдения составляет 5 рабочих дней, в дальнейшем данные файлы будут удалены лицами, имеющими доступ или системным администратором видеонаблюдения Учреждения.

4.6. Для защиты публичных интересов (т.е. выявления фактов опасных явлений и совершения правонарушения) в просмотре могут участвовать лица, изображенные на записи, сотрудники полиции и специальных служб (при наличии оснований, установленных Федеральными законами), а также законные представители лиц, изображенных на записи.

4.7. Если камеры зафиксировали конфликтную ситуацию между посетителем и сотрудником ГАУЗ ПГБ, то такие записи подлежат хранению в течение срока исковой давности, т.е. в течение трех лет.

V. Структура и общие требования к системе видеонаблюдения

5.1. Требования к информационной безопасности:

5.1.1. Для Системы видеонаблюдения следует учитывать следующие виды угроз безопасности:

- конфиденциальности (несанкционированный доступ);
- целостности (случайное или преднамеренное искажение);
- подлинности (подмена данных);
- доступности.

5.1.2 Средства защиты информации системы видеозаписи должны обеспечивать защиту от всех видов угроз безопасности:

- конфигурационные данные;
- журнал событий;
- архив оцифрованных видеоданных;
- разграничение доступа к функциональным возможностям системы видеозаписи.

5.2. Требования устойчивости системы видеозаписи к внешним воздействующим факторам.

5.2.1. Требования устойчивости к воздействию климатических факторов устанавливают в стандартах и нормативными на технические средства и системы видеозаписи конкретных типов в соответствии с ГОСТ 15150-69 «Межгосударственный стандарт. Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды» (утв. Постановлением Госстандарта СССР от 29.12.1969 N 1394).
5.2.2. Оболочки технических средств при необходимости защиты от внешних воздействий должны иметь степени защиты по ГОСТ 14254-2015 (IEC 60529:2013) «Межгосударственный стандарт. Степени защиты, обеспечиваемые оболочками (Код 1Р)» (введен в действие Приказом Росстандарта от 10.06.2016 N 604-ст), которые следует устанавливать в нормативных документах на системы видеонаблюдения конкретных типов.
5.2.3. Технические средства и система видеонаблюдения должны обеспечивать соответствие требованиям к прочности и устойчивости при воздействии механических нагрузок, значения параметров которых следует устанавливать в нормативных документах на технические средства и систему видеонаблюдения конкретных типов.
5.3. Требования к электропитанию.
5.3.1. Основное электропитание технического средства и система видеозаписи должно осуществляться от электрической сети систем электроснабжения общего назначения переменного тока частотой 50 Гц номинальным напряжением не менее 220 В.
5.3.2. Техническое средства и система видеозаписи должны сохранять работоспособность при отклонениях напряжения электрической сети систем электроснабжения общего назначения в диапазоне от минус 20% до плюс 10% от номинального значения, а также отклонениях частоты переменного тока в диапазоне от 49 до 51 Гц.
5.3.3. Электропитание отдельных Технических средств допускается осуществлять от других источников с иными параметрами выходных напряжений, требования к которым устанавливают в НД на ТС конкретных типов.
5.3.4. Система видеозаписи в зависимости от группы по функциональным характеристикам должна иметь резервное электропитание, при пропадании напряжения основного источника питания. В качестве резервного источника электропитания может использоваться резервная сеть переменного тока или источники электропитания постоянного тока.
5.3.5. Номинальное напряжение резервного источника электропитания постоянного тока выбирают из ряда: 12; 24 В. Значения параметров должны быть установлены в нормативных документах или другой документации на систему видеонаблюдения конкретных типов.
5.3.6. При использовании в качестве источника резервного электропитания аккумуляторных батарей должен осуществляться их автоматический подзаряд.
5.3.7. Технические средства и система видеонаблюдения должны сохранять функциональные характеристики при допустимых отклонениях напряжения резервного источника электропитания от минус 15% до плюс 10% номинального значения.
5.3.8. Резервный источник электропитания должен обеспечивать выполнение основных функций СОТ при пропадании напряжения в сети на время не менее 0.5 ч при условии устранения неисправности основного электропитания в течение этого времени.
5.4. Требования к конструкции.
5.4.1. Конструкцией технического средства должна быть обеспечена взаимозаменяемость сменных однотипных составных частей и ремонтопригодность.

5.4.2. Конструкцией технического средства должны быть обеспечены:
- удобство технического обслуживания, эксплуатации;
- доступ ко всем элементам, узлам и блокам, требующим регулирования или замены в процессе эксплуатации.

5.4.3. Конструкционные, электроизоляционные материалы, покрытия и комплектующие технического средства должны обеспечивать:
- механическую прочность;
- требуемую надежность;
- выполнение требований по устойчивости к несанкционированному доступу по категориям и классам устойчивости;
- безопасную работу в заданных условиях эксплуатации.

VI. Меры по обеспечению безопасности персональных данных

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.

VII. Ответственность за нарушения правил обработки персональных данных

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

7.2. 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.

Разработал
Специалист по защите
информации ГАУЗ ПГБ — Солдатов Е.А.

Согласовано
Начальник юридического
отдела ГАУЗ ПГБ — Герасимова О.В.