

ПОЛОЖЕНИЕ о системе видеонаблюдения в ГБУЗ «СКПБ № 1»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. В соответствии с требованиями Федерального закона от 06.03.2006 г. №35 «О противодействии терроризму», Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных», Федерального закона от 21.11.2011 г. №323-ФЗ «Об основах здоровья граждан РФ», Федерального закона от 02.07.2021 г. №311-ФЗ «О внесении изменений в Трудовой кодекс Российской Федерации...», Постановления Правительства РФ от 17.11.2007 №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и 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)».

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

1.3. С целью противодействия терроризму и совершению противоправных действий, больница обязана вести видеонаблюдение за состоянием обстановки в режиме реального времени на всех территориях, помещениях и в отдельных палатах, архивировать и хранить данные в течение 30 суток (постановление Правительства РФ от 13.01.2019 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 (далее – СВН) в больнице необходима для защиты (безопасности) персонала, пациентов и посетителей от угроз терроризма и противоправных действий, несанкционированного вторжения (ч.13 ст. 30 Федерального закона от 30.12.2009 г. №384 «Технический регламент о безопасности зданий и сооружений»), а также внутреннего контроля качества и безопасности медицинской помощи.

1.4. СВН является открытой и не может быть направлена на сбор информации о конкретном человеке, направлена на контроль дисциплины сотрудников и порядка в больнице, предупреждения возникновения чрезвычайных ситуаций и обеспечения сохранности имущества.

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

2. ПОРЯДОК ОРГАНИЗАЦИИ СВН

2.1. Решение об установке СВН принимается главным врачом больницы, видеоконтроль вводится соответствующим приказом.

2.2. Сотрудники, вновь принимаемые на работу, выражают свое согласие на проведение видеоконтроля путем заполнения формы согласия на обработку персональных данных.

2.3. Лица, являющиеся сотрудниками больницы на момент введения СВН, должны в письменной форме выразить свое согласие или несогласие на введение данной системы (заполнение согласия на обработку персональных данных). Если работник не согласен на изменение условий трудового договора, то после выполнения процедур, предусмотренных Трудовым кодексом РФ трудовой договор с ним может быть расторгнут по пункту 7 статьи 77 ТК РФ.

2.4. Посетители организации информируются о СВН путем размещения специальных информационных табличек в зонах видимости видеокамер.

2.5. СВН больницы входит в систему контроля доступа и включает в себя ряд устройств: камеры, мониторы, записывающие устройства (видеорегистраторы).

2.6. Места установки видеокамер в больнице определяются по мере необходимости в соответствии с конкретными задачами решением главного врача.

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

2.8. Установка видеокамер не допускается в туалетных, душевых комнатах для пациентов и работников больницы и в комнатах для переодевания работников.

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

2.10. СВН должна иметь резервный АРМ для дублирования и хранения записываемой информации.

2.11. Лица, ответственные за эксплуатацию, работоспособность и защиту информации в СВН назначаются приказом главного врача.

3. ЦЕЛИ И ЗАДАЧИ СВН

3.1. Целью СВН является создание условий для антитеррористической защищенности в больнице, безопасности персонала и пациентов, сохранности имущества, своевременного реагирования при возникновении чрезвычайных ситуаций, осуществление внутреннего контроля качества и безопасности медицинской деятельности.

3.2. Задачами организации видеонаблюдения являются:

- контроль за обстановкой на территориях и в помещениях больницы, обеспечение защиты от несанкционированного проникновения на территории, в здания и в помещения посторонних лиц и транспортных средств;

- своевременное реагирование при возникновении опасных и чрезвычайных ситуаций, в т.ч. вызванных террористическими актами на территории больницы;

- охрана жизни, предупреждение и минимизация рисков травматизма работников больницы и посетителей;

- установление достоверности фактов при расследовании несчастных случаев (запись события, регистрация времени, места и участников, причин получения травмы работником, пациентом, посетителем);

- 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, пациентов и

посетителей больницы;

- охрана имущества, предупреждение и устранение причин (последствий) деятельности, приводящей к порче имущества, а так же предупреждение случаев хищения имущества больницы и/или работников/посетителей;

- отслеживание, фиксация, своевременная передача изображений и данных об объектах видеонаблюдения;

- информационное обеспечение принятия решений главным врачом;

- предоставление информации по запросам соответствующих служб и государственных органов в случаях, предусмотренных действующим законодательством.

3.3. СВН должна обеспечивать:

- видео фиксацию текущего состояния объекта 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, могут быть использованы в качестве доказательства в уголовном, гражданском или административном судопроизводстве для доказывания факта совершения противоправного действия, а также для установления личности лица, совершившего соответствующее противоправное действие.

4. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПОСТРАНЕНИЯ (СЛУЖЕБНОЙ ИНФОРМАЦИИ)

4.1. СВН позволяет отслеживать деятельность сотрудников на рабочем месте или в иных помещениях, закрытых для общего доступа, такое наблюдение будет считаться обработкой служебной информации.

4.2. Больница обязуется принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, в части касающейся предусмотренных Федеральным законом №152-ФЗ от 27.07.2007 года «О персональных данных», и принятыми в соответствии с ним нормативными правовыми актами.

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

5.1. СВН предполагает запись информации в режиме реального времени на жесткий диск видеорегистратора и резервного автоматизированного рабочего места (далее – АРМ), которая не подлежит перезаписи и длительному хранению:

- для видеокамер, установленных для обеспечения антитеррористической защищенности больницы, уничтожается автоматически по мере заполнения памяти жесткого диска не менее, чем через 30 суток;

- для видеокамер, установленных для осуществления внутреннего, контроля качества и безопасности оказания медицинских услуг, уничтожается автоматически по мере заполнения памяти жесткого диска до 14 суток.

5.2. Запись информации видеонаблюдения является конфиденциальной, не подлежит перезаписи с жестких дисков видеорегистраторов и резервного АРМ, редактированию.

Исключение составляют случаи официального письменного обращения с разрешения главного врача больницы.

5.3. Отображение процесса видеозаписи в режиме реального времени производится на экраны, установленные:

- в кабинете главного врача с целью своевременного реагирования на возникновение признаков и причин опасных ситуаций;
- в помещениях контрольно-пропускных пунктов, в которых оборудованы посты охраны на территориях больницы (ул. Красная, 1 и ул. 16 Полевой участок, 7), с целью своевременного реагирования на возникновение признаков и причин опасных ситуаций;
- на посту охраны холл здания литер Ж, с целью своевременного реагирования на возникновение признаков и причин опасных ситуаций;
- в кабинете начальника отдела ГО и МР на резервном АРМ;
- заместителя главного врача по медицинской части, с целью своевременного реагирования на возникновение признаков и причин опасных ситуаций;
- заместителя главного врача по клинико-экспертной работе, с целью своевременного реагирования на возникновение признаков и причин опасных ситуаций;
- заместителя главного врача по амбулаторно-поликлиническому разделу работы, с целью своевременного реагирования на возникновение признаков и причин опасных ситуаций;
- в кабинетах заведующих отделений, с целью своевременного реагирования на возникновение признаков и причин опасных ситуаций;
- в помещениях отделений больницы с круглосуточным пребыванием медицинского персонала, с целью своевременного реагирования на возникновение признаков и причин опасных ситуаций.

5.4. Разрешение доступа к просмотру записей видеонаблюдения, хранящихся установленный период на жестком диске видеорегистратора и резервного АРМ, осуществляется:

- для просмотров записей в отделениях с разрешения заместителя главного врача по медицинской части;
- для просмотров записей в отделении клинико-экспертной работе с разрешения заместителя главного врача по клинико-экспертной работе;
- для просмотров записей в диспансерном отделении с разрешения заместителя главного врача по амбулаторно-поликлиническому разделу работы;
- для просмотров записей установленных для антитеррористической защищенности больницы с разрешения главного врача.

На основании письменного разрешения главного врача больницы другие работники больницы могут быть допущены к просмотру записей видеонаблюдения, при условии принятия ими на себя обязательств о неразглашении персональных данных третьих лиц только в присутствии ответственного за организацию работы СВН или лица, его замещающего.

5.5. Обеспечением конфиденциальности является пароль доступа к информации видеорегистратора, который известен лицам, имеющим право на просмотр согласно пункту 5.4.

Генерация и выдача паролей доступа осуществляется ответственным за организацию работы СВН, назначенным приказом главного врача больницы посредством ведения «Журнала генерации, учета и выдачи паролей доступа» под личную роспись (образец – приложение № 4). Смена пароля или его продление осуществляется не реже одного раза в шесть месяцев (либо при увольнении этих должностных лиц).

5.6. Просмотр записанных изображений может осуществляться исключительно при личном участии должностных лиц имеющих право на просмотр указанных в пункте 5.4., а по (при отсутствии посторонних лиц).

5.7. Для защиты публичных интересов (т.е. выявление факта совершения правонарушения) в просмотре могут участвовать лица, изображенные на записи и сотрудники полиции (и других правоохранительные органы РФ).

5.8. Передача записей камер видеонаблюдения третьей стороне допускается только в исключительных случаях (по письменному мотивированному запросу следственных и судебных органов, а также по письменному мотивированному запросу работников, изображенных на видеозаписи).

Решение о передаче записей принимает главный врач больницы.

6. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ ПРАВИЛ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Лица, виновные в нарушении требований Федерального закона №152-ФЗ от 27.07.2007 года «О персональных данных», несут предусмотренную законодательством Российской Федерации ответственность.

6.2. Моральный и материальный 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 больницы (кроме уполномоченных на то лиц) и охранной организации **ЗАПРЕЩАЕТСЯ:**

препятствовать работе СВН путем регулировки направления (обзора) камер видеонаблюдения, загромождать, закрывать камеры или каким-либо иным способом препятствовать производству видеонаблюдения, отключать электропитание камер СВН.

За причинение материального вреда и порчу камер СВН работники больницы и охранной организации несут ответственность в соответствии с действующим законодательством Российской Федерации.

7. ОРГАНИЗАЦИЯ ВСЕСТОРОННЕГО ОБЕСПЕЧЕНИЯ РАБОТЫ СВН

7.1. Ответственность за проведение технического обслуживания, в том числе проведения ремонтных работ для поддержания работоспособности СВН возлагается на начальника технического отдела.

7.2. Ответственность за работоспособность программно-аппаратного комплекса СВН, в том числе его модернизацию (обновление операционных систем, САВЗ, системы разграничения доступа и т.д.) возлагается на начальника медико-информационного отдела автоматизированных систем управления.

7.3. Выполнение работ, указанных в п.п. 7.1. и 7.2., в том числе в нерабочее время (выходные, нерабочие и праздничные дни) проводить только по согласованию с ответственным за организацию работы СВН с записью в журнале учета вскрытия помещений (приложение 2).

7.4. Ответственность за предотвращение неправомерного доступа к защищаемой информации, хранящейся на магнитных накопителях, контроль за ее использованием, возлагается на ответственного за организацию работы СВН по защите информации.

7.5. Организация информационной безопасности при эксплуатации СВН должна обеспечивать установленные сроки хранения, конфиденциальность и целостность информации и обеспечивается проведением следующих мероприятий:

– ограничением круга лиц, допущенных к информации с СВН, в соответствии с приказом главного врача;

– ограничением физического доступа к магнитным накопителям СВН путем опечатывания устройств, исключающих их вскрытие без нарушения оттиска печати ответственного за организацию работы СВН по ЗИ;

– обеспечением учета доступа в помещения, где используются магнитные накопители СВН с записью в журнале учета вскрытия помещения, приложение 2;

– обеспечением хранения и выдачи ключей от помещений, где используются магнитные накопители СВН с записью в журнале учета и выдачи ключей, приложение 3;

– учетом магнитных носителей информации используемых в СВН в «Журнале учета СКЗИ МИО АСУ».

7.6. Руководители структурных подразделений в случае нарушения работоспособности СВН представляют заявки на их ремонт в установленном порядке.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Настоящее Положение, изменения и дополнения к нему, утверждаются приказом главного врача больницы.

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

8.3. Один экземпляр настоящего положения выдается под роспись директору (руководителю) охранной организации (предприятия) с которой заключен действующий Контракт на оказание охранных услуг.

Заместитель главного врача по хозяйственным вопросам

М.Ф. Кизим

Ответственный за АТЗ

А.В. Бабин

Ответственный за организацию СВН по ЗИ

А.В. Павлов

Приложение 1
к Положению о системе видеонаблюдения

И.о.главного врача ГБУЗ «СКПБ №1»
Коноваловой О.Ю.

(должность, ФИО сотрудника)

Согласие работника на осуществление видеонаблюдения на рабочем месте

Настоящим подтверждаю, что осведомлен о внедрении СВН на территории и в помещениях ГБУЗ «СКПБ №1» (далее - работодатель) и выражаю свое согласие на использование работодателем СВН в целях обеспечения безопасности сторон трудового договора, контроля выполнения работниками Правил внутреннего трудового распорядка, обеспечения сохранности имущества, выявления нарушений законодательства Российской Федерации и локальных нормативных актов работодателя.

[подпись, инициалы, фамилия]

[число, месяц, год]