

ПОЛОЖЕНИЕ**о системе видеонаблюдения в ГБУЗ «НПЦ спец.мед.помощи детям ДЗМ»****1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. В соответствии с требованиями Федерального закона от 06.03.2006 № 35 «О противодействии терроризму», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 21.11.2011 № 323-ФЗ «Об основах здоровья граждан в Российской Федерации» (далее – ФЗ от 21.11.2011 № 323-ФЗ), Федерального закона от 02.07.2021 № 311-ФЗ «О внесении изменений в Трудовой кодекс Российской Федерации», постановления Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и постановления Правительства Российской Федерации № 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)» (далее – ПП от 13.01.2017 № 8), приказ от 26.11.2024 № 1072 «О совершенствовании работы по обеспечению безопасности и антитеррористической защищенности организаций, учреждений и предприятий, подведомственных Департаменту здравоохранения города Москвы».

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, ГБУЗ «НПЦ спец.мед.помощи детям ДЗМ» (далее – Учреждение) обязано 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 (ПП от 13.01.2017 № 8).

Система видеонаблюдения (далее – СВН) в Учреждении 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 оказания медицинской помощи.

1.4. СВН является открытой и не может быть направлена на скрытый сбор информации о конкретном человеке, а направлена на контроль дисциплины сотрудников и порядка в Учреждении, предупреждения возникновения чрезвычайных ситуаций, обеспечения сохранности имущества и безопасности оказания медицинской деятельности.

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

2. ПОРЯДОК ОРГАНИЗАЦИИ СВН

2.1. Решение об установке СВН принимается директором Учреждения в соответствии со ст. 16 п.б. ПП от 13.01.2019 г. № 8 и должно позволять (с учетом количества устанавливаемых камер и места их размещения) обеспечивать непрерывное видеонаблюдение потенциально

опасных участков и критических элементов объектов (территории) Учреждения и хранение данных не менее 1 месяца.

2.2. Решение об установке СВН для внутреннего контроля качества и безопасности оказания медицинской помощи принимается директором Учреждения на основании ФЗ от 21.11.2011 № 323-ФЗ.

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

2.4. СВН позволяет отслеживать деятельность сотрудников на рабочем месте или иных помещениях закрытых для общего доступа и видеонаблюдение рабочего процесса не является раскрытием персональных данных работника, не подпадает под действия гл. 14 Трудового кодекса Российской Федерации, 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 видеосъемки и включения соответствующих условий в трудовой договор не требуется.

2.5. Посетители Учреждения информируются о СВН путем размещения специальных информационных табличек.

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

2.7. Места установки видеокамер в Учреждении определяются по мере необходимости в соответствии с конкретными задачами, решением директора.

2.8. Видеокамеры устанавливаются в местах открытых для общего доступа (территория, входы в здание, коридоры), а также в помещениях, где оказываются медицинские услуги (кабинеты врачей, и т.п).

2.9. Установка видеокамер не допускается в туалетных, душевых комнатах для пациентов и работников Учреждения и в комнатах для переодевания работников.

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

2.11. Ответственными за эксплуатацию, работоспособность и защиту информации в СВН являются сотрудники отдела по сопровождению информационных систем.

3. ЦЕЛИ И ЗАДАЧИ СВН

3.1. Целью СВН является создание условий для антитеррористической защищенности в Учреждении, 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 Учреждения, 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 Учреждения;
- охрана жизни, предупреждение и минимизация рисков травматизма работников Учреждения 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 Учреждения;
- охрана имущества, предупреждение и устранение причин (последствий) деятельности, приводящей к порче имущества, а так же предупреждение случаев хищения имущества Учреждения и/или работников/посетителей;
- отслеживание, фиксация, своевременная передача изображений и данных об объектах видеонаблюдения;
- информационное обеспечение принятия решений директором, а в его отсутствие главным врачом;
- предоставление информации по запросам соответствующих служб и государственных органов в случаях, предусмотренных действующим законодательством.

3.3. СВН должна обеспечивать:

- видеофиксацию 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.

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 считается обработкой служебной информации.

4.2. Учреждение обязуется принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, в части касающейся, предусмотренных Федеральным законом от 27.07.2007 № 152-ФЗ «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 Учреждения, запись 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, запись уничтожается автоматически по мере заполнения памяти жесткого диска не менее чем через 30 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 государственных органов с разрешения директора, а в его отсутствие - главного врача Учреждения.

5.3. Если камеры видеонаблюдения зафиксировали конфликтную нестандартную ситуацию, то данные переписываются на съемный носитель и для таких записей устанавливается специальный срок хранения 6 месяцев. При конфликтной ситуации между посетителями (представителем ребенка, пациента) и работником Учреждения, то такие записи подлежат хранению в течение срока исковой давности (3 года).

Если камеры зафиксировали административный проступок, то такие записи хранятся в течение всего срока производства по административному делу.

По надлежащему запросу правоохранительных органов или по постановлению о выемке данные материалы передаются правоохранительным органам. Съёмные носители с записями камер хранятся в сейфе у начальника отдела по сопровождению информационных систем.

5.4. Отображение процесса видеозаписи в режиме реального времени производится:

5.4.1. для обеспечения антитеррористической защищенности Учреждения;

– в комнате видеонаблюдения и контрольно - пропускном пункте;

5.4.2. для осуществления внутреннего контроля качества и безопасности оказания медицинских услуг:

- в кабинете главного врача;
- в кабинете заместителя главного врача по хирургической помощи;
- в кабинете главной медицинской сестры;
- в кабинете заведующего отделом эпидемиологии - врача-эпидемиолога.

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

– для просмотра записей с целью осуществления внутреннего контроля качества и безопасности оказания медицинских услуг в отделениях с разрешения директора или главного врача Учреждения;

– для просмотра записей установленных для антитеррористической защищенности Учреждения с разрешения специалиста по безопасности и режиму, специалисту по гражданской обороне;

– для просмотра записей в случае конфликтной (нестандартной) ситуации, происшествии и т.д. с разрешения специалиста по безопасности и режиму.

На основании разрешения директора или главного врача Учреждения, сотрудники, а в ряде конфликтных ситуаций, законные представители пациентов (посетители) могут быть

допущены к просмотру записей видеонаблюдения, при условии принятия ими на себя обязательств о неразглашении персональных данных третьих лиц только в присутствии специалистов по безопасности и режиму, по гражданской обороне, сотрудника отдела по сопровождению информационных систем и сотрудника ЧОП.

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

5.7. 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 директор, а при его отсутствии главный врач Учреждения.

5.8. Видеоматериалы не могут выкладываться в сеть интернет, локальную сеть или доводиться для всеобщего сведения без письменного согласия лиц, в отношении которых отснят видеоматериал.

6. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ ПРАВИЛ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Лица, виновные в нарушении требований Федерального закона от 27.07.2007 № 152-ФЗ «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 Учреждения (кроме уполномоченных на то лиц) и ЧОП **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 Учреждения и ЧОП несут ответственность в соответствии с действующим законодательством Российской Федерации.

7. ОРГАНИЗАЦИЯ ВСЕСТОРОННЕГО ОБЕСПЕЧЕНИЯ РАБОТЫ СВН

7.1. Ответственность за проведение технического обслуживания, работоспособность программно-аппаратного комплекса СВН, его модернизация, в том числе проведение ремонтных работ для поддержания работоспособности СВН возлагается на отдел по сопровождению информационных систем.

7.2. Ответственность за предотвращение неправомерного доступа к защищаемой информации, хранящейся на съемных накопителях, контроль за ее использованием, возлагается на начальника отдела по сопровождению информационных систем.