

УТВЕРЖДАЮ

Главный врач ГБУЗ СО

«ВФД г. Нижний Тагил»

И.В. Панькова

« 1 » февраля 2018 года

ПОЛОЖЕНИЕ

о системе видеонаблюдения в ГБУЗ СО «ВФД г. Нижний Тагил»

1. Общие положения

1.1. Настоящее положение о системе видеонаблюдения в ГБУЗ СО «ВФД г. Нижний Тагил» (далее- Положение и Учреждение) разработано в соответствии с Федеральным законом РФ "О персональных данных" от 27 июля 2006 г. № 152-ФЗ, Постановлением Правительства РФ от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных".

1.2. Настоящее Положение устанавливает порядок проведения видеонаблюдения на в здании Учреждения по адресу: Свердловская область, г. Нижний Тагил, пр. Ленина, д.23/40, устанавливает цели и способы его осуществления, порядок доступа к записям, их хранения и уничтожения, а также привлечения к ответственности.

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

1.3. Система открытого видеонаблюдения в Учреждении является элементом общей системы безопасности Организации, направленной на обеспечение общественной безопасности, поддержание трудовой дисциплины и порядка, направленной на предупреждение возможных террористических, экстремистских акций и других противоправных проявлений в отношении сотрудников Учреждения, предупреждение возникновения чрезвычайных ситуаций и обеспечение объективности расследования в случаях их возникновения.

1.4. Система видеонаблюдения в Учреждении является открытой, ведется с целью обеспечения безопасности работников организации и не может быть направлена на сбор информации о конкретном человеке.

1.5. Видеонаблюдение осуществляется с целью документальной фиксации возможных противоправных действий, которые могут нанести вред имуществу. 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.

2. Цели и задачи системы видеонаблюдения

2.1. Система видеонаблюдения призвана выполнять следующие задачи:

2.1.1. Повышение эффективности действий при возникновении нештатных и чрезвычайных ситуаций.

2.1.2. Обеспечение противопожарной защиты зданий и сооружений.

2.1.3. Обеспечение антитеррористической защиты работников и территории Учреждения, охраны порядка и безопасности.

2.1.4. Совершенствование системы информирования и оповещения работников Учреждения об угрозе возникновения кризисных ситуаций.

2.1.5. Пресечение противоправных действий со стороны работников Учреждения и посетителей.

2.1.6. Контроль за выполнением со стороны работников Учреждения и посетителей Правил внутреннего трудового распорядка Учреждения.

2.2. Видеонаблюдение осуществляется с целью документальной фиксации возможных противоправных действий, которые могут нанести вред имуществу. 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.

2.3. Задачи мероприятий по обеспечению безопасности Учреждения путем установки системы видеонаблюдения:

2.3.1. Контроль за обстановкой, в том числе во внутренних помещениях и в пределах территории Учреждения, обеспечивающих защиту от несанкционированного проникновения в Учреждение посторонних лиц.

2.3.2. Защита сотрудников Учреждения, их прав и интересов, имущества от неблагоприятных воздействий.

2.3.3. Ранее выявление причин и признаков опасных ситуаций, их предотвращение и устранение.

2.3.4. Предупреждение и минимизация рисков материального ущерба в условиях действия дестабилизирующих факторов.

2.3.5. Предоставление информации по запросам соответствующих служб и государственных органов в случаях, предусмотренных действующим законодательством.

3. Порядок организации системы видеонаблюдения

3.1. Система видеонаблюдения в Учреждении является открытой.

Видеонаблюдение осуществляет передачу видеоизображения в режиме реального времени, синхронизацию событий с системой единого точного времени.

Система видеонаблюдения Учреждения входит в систему контроля доступа и включает в себя ряд устройств: камеры, монитор, записывающее устройство.

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

3.3. Видеокамеры установлены:

1. Входная группа Учреждения
2. Холл (у регистратуры)
3. Коридор (у запасного выхода)
4. Коридор (у кабинета главного врача)

3.4. Сотрудники и посетители Учреждения, которые потенциально могут попасть в зону видеонаблюдения, информируются про видеонаблюдение в Учреждении.

Для оповещения используются следующие формы:

- размещено специальное информационное объявление (табличка) перед входом в Учреждение о том, что ведется видеонаблюдение;
- информирование через официальный сайт Учреждения;
- размещение настоящего Положения на доске объявлений Учреждения.

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

4.1. Отображение процесса видеозаписи производится на мониторе, установленном в кабинете главного врача Учреждения.

Ответственное лицо, отвечающее за техническое состояние системы видеонаблюдения, назначено приказом главного врача по Учреждению.

4.2. Система видеонаблюдения предполагает запись информации на жесткий диск видеорегистратора, которая не подлжет перезаписи, уничтожается автоматически по мере заполнения памяти жесткого диска.

4.3. Запись информации видеонаблюдения является конфиденциальной, не подлжет перезаписи с жесткого диска видеорегистратора, редактированию, передаче третьим лицам.

4.4. Доступ к просмотру записи видеонаблюдения, хранящимся в установленный период на жестком диске видеорегистратора, имеет главный врач Учреждения, главная медицинская сестра, начальник хозяйственного отдела.

4.5. Просмотр записанных изображений может осуществляться исключительно при личном участии главного врача Учреждения, главной медицинской сестры и наачальника хозяйственного отдела Учреждения (при отсутствии посторонних лиц).

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

4.6. Если камеры видеонаблюдения зафиксировали конфликтную (нестандартную) ситуацию, то для таких записей устанавливается специальный срок хранения, в течение срока исковой давности, т.е. в течение трех лет.

4.7. Передача записей камер видеонаблюдения третьей стороне допускается только в исключительных случаях (по запросу следственных и судебных органов, а также по запросу граждан, изображенных на видеозаписи). Вопрос о передаче записей решает главный врач Учреждения.

4.8. Лицо, виновное в причинении вреда нарушением конфиденциальности записей камер, несет ответственность в порядке, предусмотренном действующим законодательством РФ.

5. Меры по обеспечению безопасности персональных данных

5.1. 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,

5.2. Обработка персональных данных должна осуществляться на законной основе и ограничиваться достижением конкретных, заранее определенных и законных целей.

Не допускается обработка персональных данных, несовместимых с целями сбора персональных данных.

5.3. 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.

6. Ответственность за нарушения правил обработки персональных данных.

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

6.2. Моральный вред, причиненный субъекту вследствие нарушения его прав, 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.