УТВЕРЖДЕНО

приказом АУ Республики Марий Эл «Дирекция МФЦ»

от «29» июня 2020г. № 169-ОД

**П о л о ж е н и е**

**о системе видеонаблюдения**

**в АУ Республики Марий Эл «Дирекция МФЦ»**

**1.** **Общие положения**

* 1. Настоящее положение разработано в соответствии с требованиями Федерального закона от 06 марта 2006 г. № 35-ФЗ «О противодействии терроризму», Федерального закона от 27 июля 2006 г. № 152-ФЗ   
     «О персональных данных», Постановления Правительства от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных   
     при их обработке в информационных системах персональных данных».
  2. Под видеонаблюдением понимается непосредственное осуществление видеонаблюдения посредством использования видеокамер   
     для получения видеоинформации об объектах и помещениях, а также запись полученного изображения и его хранение для последующего использования.
  3. Система открытого видеонаблюдения в АУ Республики Марий Эл «Дирекция МФЦ» (далее по тексту - Учреждение) является элементом общей системы безопасности учреждения, направленной на обеспечение безопасности получателей государственных и муниципальных услуг   
     и работников, поддержание трудовой дисциплины и порядка, предупреждение возникновения чрезвычайных ситуаций и обеспечение объективности расследования в случаях их возникновения.
  4. Система видеонаблюдения является открытой, ведется с целью обеспечения безопасности получателей государственных и муниципальных услуг и работников Учреждения.

**2. Порядок организации системы видеонаблюдения**

* 1. Решение об установке системы видеонаблюдения принимается директором Учреждения при наличии необходимых финансовых средств, специального оборудования, нормативного обеспечения.
  2. Схема установки видеокамер разрабатывается руководством учреждения и согласовывается с Департаментом [информатизации и связи Республики Марий Эл](https://yandex.ru/maps/org/departament_informatizatsii_i_svyazi_respubliki_mariy_el/1719626237/).
  3. Система видеонаблюдения Учреждения является открытой   
     и включает в себя ряд устройств: камеры, мониторы, записывающие устройства.
  4. Установка системы видеонаблюдения осуществляется   
     в соответствии с ее целями и задачами согласно проектной документации   
     и технического задания на её монтаж (внутренние помещения, внешний периметр, в местах возможного несанкционированного проникновения посторонних лиц, проявления актов вандализма).
  5. Запрещается использование устройств, предназначенных   
     для негласного получения информации (например, скрытых камер).
  6. Запрещается установка системы видеонаблюдения в туалетах, помещениях дневного пребывания и в иных местах, связанных   
     с осуществлением личных нужд работников и получателей государственных и муниципальных услуг.
  7. Работники учреждения информируются под подпись о ведущемся   
     в Учреждении видеонаблюдении с момента установки камер видеонаблюдения, а принятые на работу после введения настоящего положения – с момента приема на работу. Также, в помещениях, где ведется видеонаблюдение, должны быть размещены в местах, доступных   
     для посетителей, информационные таблички.
  8. Функции по обеспечению бесперебойной работы элементов системы видеонаблюдения, проведение регулярного технического контроля, профилактическое обслуживание системы, работы по ремонту, модернизации и расширению системы, обеспечению отказоустойчивости на программном   
     и аппаратном уровнях, осуществляют сотрудники Учреждения (сектора информационных технологий), либо сторонняя организация в рамках договора на обслуживание (обеспечение работоспособности) технических средств видеонаблюдения.

**3. Цели и задачи системы видеонаблюдения**

* 1. Система видеонаблюдения призвана выполнять следующие задачи:
* обеспечение антитеррористической защиты граждан, охрана порядка и безопасности;
* пресечение противоправных действий;
* установления личности лица, совершившего противоправное действие;
* обеспечение противопожарной защиты здания и помещений;
* повышение эффективности действий при возникновении нештатных и чрезвычайных ситуаций;
* защита получателей государственных и муниципальных услуг,   
  их прав и интересов от противоправных действий работников Учреждения;
* совершенствование системы информирования и оповещения получателей государственных и муниципальных услуг и работников Учреждения об угрозе возникновения чрезвычайных ситуаций;
* предупреждение и минимизация рисков травматизма получателей государственных и муниципальных услуг и работников Учреждения;
* предупреждение, устранение причин (последствий) деятельности, приводящей к порче имущества Учреждения;
* осуществление контроля за ненадлежащим выполнением работниками своих должностных обязанностей.
  1. Видеонаблюдение осуществляется с целью документальной фиксации возможных противоправных действий, которые могут нанести вред работникам Учреждения, получателям государственных и муниципальных услуг и имуществу. В случае необходимости материалы видеозаписей, полученных камерами видеонаблюдения, могут быть использованы в качестве доказательств в судопроизводстве или переданы установленным порядком правоохранительным органам или другим органам в рамках действующего законодательства Российской Федерации.

**4. Меры по обеспечению безопасности**

**персональных данных, хранение данных видеонаблюдения**

**и передача третьим лицам**

* 1. Функции по обеспечению безопасности хранения, управления   
     и передачи видеоданных, настройке и изменению параметров системы, конфигурирование системы, управление параметрами архивирования, управление учетными записями доступа к системе видеонаблюдения (логины/пароли) и назначение прав доступа, осуществляют ответственные   
     за управление (администрирование) системой защиты информации информационных систем, назначаемый приказом директора Учреждения (далее - Ответственные). Любые работы с системой видеонаблюдения, осуществляемые Ответственным, в рамках установленного данным пунктом, осуществляются только по распоряжению директора.
  2. В тех случаях, когда система видеонаблюдения позволяет отслеживать деятельность работников Учреждения в помещениях, закрытых для общего доступа, такое наблюдение считается обработкой персональных данных.
  3. Учреждение обязуется принимать меры, необходимые   
     и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», и принятыми   
     в соответствии с ним локальными актами.
  4. 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.
  5. Система видеонаблюдения предполагает 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.
  6. Отображение процесса видеозаписи камер в режиме реального времени производится на экране, установленном на рабочем месте сотрудников охраны (пост охраны) в зоне доступного наблюдения с целью своевременного реагирования на возникновение признаков и причин опасных ситуаций.
  7. Правами полного доступа («администратор») к системе видеонаблюдения, имеет директор учреждения или лицо, его замещающее, заместитель директора (ответственный за организацию обработки персональных данных) и сотрудники Учреждения, назначенные   
     в соответствии с п. 4.1. настоящего Положения.
  8. Просмотр записанных видеоматериалов может осуществляться   
     при личном участии директора Учреждения или его заместителя, а также   
     по их распоряжению Ответственными. В целях реализации задач, обозначенных в п 3.1 настоящего Положения, по письменному распоряжению директора Учреждения дополнительно могут быть назначены лица из числа сотрудников Учреждения для осуществления контрольных проверок видеозаписей системы видеонаблюдения на наличие нарушений   
     с ограничением объектов наблюдения в рамках выделенных полномочий   
     и правами доступа к системе «только просмотр». Для защиты публичных интересов (т.е. выявления факта совершения правонарушения) в просмотре могут участвовать лица, являющиеся участниками на записи,   
     а также сотрудники правоохранительных органов, органов следствия и другие лица, предусмотренные действующим законодательством.
  9. Для обеспечения объективности расследования в случаях возникновения чрезвычайных ситуаций и (или) происшествий и служебных разбирательств, нарушений правил внутреннего трудового распорядка, противоправных действий со стороны работников Учреждения или иных лиц на территории и в помещениях Учреждения, соответствующие видеофрагменты по указанию директора Учреждения могут быть сохранены   
     с диска видеорегистратора на внешний носитель с соблюдением необходимых мер защиты конфиденциальной информации.
  10. Сохраненные видеофрагменты уничтожаются (стираются)   
      (за исключением случаев необходимости использования данных в судебном разбирательстве) после завершения срока, необходимого для выполнения целей обработки, либо с увольнением соответствующего работника.
  11. В целях обеспечения защиты персональных данных третьих лиц   
      по требованию работника ему предоставляются только те записи, которые   
      не содержат видеозаписей других работников или иных граждан.
  12. Передача информации о видеонаблюдении в соответствующие службы и государственные органы производится только по их письменным запросам в случаях, предусмотренных действующим законодательством.
  13. Использование изображения лиц, зафиксированных видеокамерой без их согласия возможно только в следующих случаях:
* если изображение используется в государственных, общественных или публичных интересах;
* если изображение получено при съемке, которая проводится   
  в местах, открытых для свободного посещения.

**5. Ответственность за нарушения**

**правил обработки персональных данных**

5.1. Лица, виновные в нарушении требований нормативных правовых актов Российской Федерации, настоящего Положения, несут предусмотренную действующим законодательством Российской Федерации ответственность.

5.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, правил обработки персональных данных, установленных федеральным законом, а также требований к защите персональных данных подлежат возмещению в соответствии с действующим законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда, понесенных субъектом персональных данных убытков.

5.3. Работникам Учреждения запрещается:

* препятствовать работе системы видеонаблюдения путем регулировки направления (обзора) камер видеонаблюдения;
* загораживать, закрывать камеры или каким-либо иным способом препятствовать производству видеонаблюдения;
* отключать электропитание камер системы видеонаблюдения.

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

**6. Заключительные положения**

* 1. Настоящее Положение, изменения, дополнения к нему, утверждаются приказом директора Учреждения.
  2. Ознакомление работников Учреждения с настоящим положением, изменениями и дополнениями к нему, проводится в обязательном порядке под подпись.
  3. Настоящее Положение, изменения и дополнения к нему, размещаются в доступном для ознакомления месте, на официальном сайте учреждения.