Приложение 1
к приказу ГБУК "Музей истории ГУЛАГа"
от "15" марта 2024 г. № 36/ОД

Положение
о системе видеонаблюдения в ГБУК "Музей истории ГУЛАГа"

1. Общие положения

1.1. Положение о системе видеонаблюдения в ГБУК "Музей истории ГУЛАГа" (далее – Положение) определяет порядок использования видеоаппаратуры и организации системы видеонаблюдения в ГБУК "Музей истории ГУЛАГа" (далее - Учреждение).

1.2. Настоящее положение разработано в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ "О персональных данных" (далее – Федеральный закон "О персональных данных"), Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

1.3. 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.

1.4. Система видеонаблюдения в Учреждении является открытой и не может быть направлена на сбор информации о конкретном человеке.

1.5. Настоящее Положение обязательно к соблюдению работниками и посетителями Учреждения. Работники Учреждения должны быть ознакомлены с Положением под роспись. Положение подлежит размещению на информационных стендах для посетителей, а также на официальном сайте Учреждения в информационно – телекоммуникационной сети "Интернет".

1.6. Локальные нормативные акты Учреждения и условия трудовых договоров с работниками, регламентирующие видеонаблюдение, в обязательном порядке согласовываются с директором Учреждения, заместителем директора по общим вопросам.

2. Порядок организации видеонаблюдения

2.1. Решение об установке системы видеонаблюдения принимается директором Учреждения.

2.2. Видеонаблюдение в Учреждении ведется в постоянном режиме.

2.3. Система видеонаблюдения Учреждения входит в систему контроля доступа и включает в себя ряд устройств: камеры, мониторы, записывающие устройства.

2.4. Запись камер видеонаблюдения происходит в режиме циклической записи, срок хранения - не менее 20 (двадцати) и не более 60 (шестидесяти) последних дней. Уничтожение происходит за счёт встроенных средств видеорегистрации в автоматическом режиме.

2.5. Предусмотрены меры защиты – пароль доступа к ресурсу видеонаблюдения.

2.6. Список ответственных лиц, имеющих доступ к системе видеонаблюдения, утверждается приказом Учреждения.

2.7. Просмотр записанных изображений осуществляется ответственными лицами, имеющими доступ к системе видеонаблюдения, в зоне ограниченного доступа.

2.8. О ведении видеонаблюдения работники и посетители Учреждения оповещаются с использованием:

- информационных знаков "Внимание! Ведется видеонаблюдение", размещенных в зонах видимости камер;
- информационных стендов, расположенных на территории Учреждения;
- официальной страницы Учреждения в информационно – телекоммуникационной сети "Интернет".

2.9. Работникам и посетителям Учреждения запрещено загораживать, закрывать камеры или иным способом препятствовать производству видеонаблюдения.

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

3. Цели и задачи видеонаблюдения, параметры контроля

3.1. Видеонаблюдение осуществляется с целью реализации профилактических мероприятий по противодействию терроризму, осуществления контроля за соблюдением норм пожарной и санитарной безопасности, трудовой дисциплины, пресечения противоправных действий со стороны работников и посетителей Учреждения, предотвращения конфликтных ситуаций, актов вандализма.

3.2. Система видеонаблюдения призвана выполнять следующие задачи:

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

3.2.2. Обеспечение противопожарной защиты зданий и сооружений.

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

3.2.4. Обеспечение защиты прав работников и посетителей Учреждения.

3.2.5. Совершенствование системы информирования и оповещения работников и посетителей Учреждения об угрозе возникновения чрезвычайных ситуаций.

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

3.3. Система видеонаблюдения должна обеспечивать контроль следующих основных дестабилизирующих факторов (параметры контроля):

- незаконного проникновения посторонних лиц, животных или чужеродных предметов, аппаратов на территорию и в помещения Учреждения;
- возникновения пожара;
- нарушения в системе теплоснабжения, отопления, подачи горячей и холодной воды;
- нарушения в подаче электроэнергии;
- несанкционированного проникновения в служебные помещения Учреждения
- отклонений от нормативных параметров технологических процессов, способных привести к возникновению чрезвычайных ситуаций;
- изменения состояния основания, строительных (инженерно-технических) конструкций зданий и сооружений;
- нарушения работоспособности систем противоаварийной защиты, безопасности и противопожарной защиты;
- сооружений инженерной защиты.

4. Меры по обеспечению безопасности персональных данных

4.1. В тех случаях, когда система видеонаблюдения позволяет отслеживать деятельность работников на рабочем месте или в иных помещениях, закрытых для общего доступа, такое наблюдение будет считаться обработкой персональных данных.

4.2. 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.

4.3. 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.

4.4. 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.

5. Ответственность за нарушения правил обработки персональных данных

5.1. Лица, виновные в нарушении требований Федерального закона "О персональных данных", несут предусмотренную законодательством Российской Федерации ответственность.

5.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом "О персональных данных", 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.