Приложение
к приказу №_____
от «____» _____ 2025 г.

П О Л О Ж Е Н И Е
ПО ОРГАНИЗАЦИИ РАБОТЫ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ В ГБУК ЛО «МУЗЕЙНОЕ АГЕНТСТВО»

1. Общие положения

1.1. Настоящее положение разработано в соответствии с:

1.1.1. Федеральным законом РФ от 06 марта 2006 года № 35-ФЗ «О противодействии терроризму»;

1.1.2. Федеральным законом РФ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

1.1.3. Федеральным законом РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

1.1.4. Постановлением Правительства РФ от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

1.1.5. Постановлением Правительства РФ от 11 февраля 2017 года № 176 «Об утверждении требований к антитеррористической защищенности объектов (территорий) в сфере культуры и формы паспорта безопасности этих объектов (территорий)»;

1.1.6. С учетом положений 23 и 24 Конституции Российской Федерации

1.1.7. Иными нормативными актами Российской Федерации;

1.1.8. Уставом и иными локальными нормативными актами ГБУК ЛО «Музейное агентство» (далее – Учреждение).

1.2. Под видеонаблюдением понимается осуществление визуального контроля (наблюдения) посредством использования видеокамер и специального оборудования, объединённого в систему видеонаблюдения (систему охранного телевидения), для получения видеоинформации о территориях, объектах, помещениях, действий находящихся на их территории людей, а также запись полученного изображения и его хранение для последующего использования.

1.3. Система открытого видеонаблюдения в Учреждении является **элементом общей системы безопасности**, направленной на обеспечение безопасности работников и посетителей, поддержание порядка, сохранения имущества, предупреждение возникновения чрезвычайных ситуаций и обеспечение объективности расследования в случаях их возникновения.

1.4. Система видеонаблюдения не может быть направлена на сбор информации о конкретном человеке.

1.5. Видеокамеры устанавливаются в местах, открытых для общего доступа (территория, входы в здание, коридоры, выставочные залы), а также в помещениях ограниченного доступа, где осуществляется хранение музейных предметов (фондохранилище) и материальных ценностей Учреждения (служебные помещения, рабочие кабинеты).

1.6. Установка видеокамер не допускается в туалетных комнатах, комнатах для переодевания (раздевалках) и в иных местах, связанных с осуществлением личных нужд работников и посетителей.

1.7. Посетители и работники объекта и иные лица информируются о системе видеонаблюдения путем размещения специальных объявлений и общепринятых знаков о ведении видеонаблюдения.

1.8. Информация, полученная посредством видеонаблюдения, предоставляется в соответствующие службы и государственные органы только по письменным запросам в случаях, предусмотренных действующим законодательством РФ.

2. Цели и задачи организации видеонаблюдения

2.1. **Целью** системы видеонаблюдения является создание условий для обеспечения безопасности жизни и здоровья работников Учреждения, сохранности имущества Учреждения в ходе процесса хранения, изучения и популяризации объектов культурного наследия, музейных предметов и музейных коллекций, своевременного реагирования при возникновении чрезвычайных ситуаций, принятия необходимых мер по оказанию помощи персоналу и посетителей, как участников данного процесса.

2.2. Система видеонаблюдения призвана выполнять следующие **задачи**:

2.2.1. Контроль за обстановкой в помещениях и на территории Учреждения (включая его филиалы), охрана порядка и безопасности людей, обеспечение пропускного и внутриобъектового режима, предотвращение несанкционированного проникновения посторонних лиц и транспортных средств на территорию и в здание Учреждения;

2.2.2. Антитеррористическая защита, своевременное реагирование при возникновении опасных и чрезвычайных ситуаций, в том числе вызванных террористическими актами на территории и на объекты Учреждения;

2.2.3. Охрана жизни и здоровья людей, предупреждение и минимизация рисков травматизма на территории и на объектах Учреждения;

2.2.4. Установление достоверности фактов при расследовании несчастных случаев (запись события, регистрация времени, места и участников, причин получения травмы);

2.2.5. Обеспечение безопасности посетителей объектов (музеев) Учреждения, выявление случаев грубого обращения, установление причин конфликта между посетителями музея и работниками Учреждения;

2.2.6. Защита прав и интересов работников Учреждения;

2.2.7. Пресечение правонарушений, раннее выявление причин и признаков опасных ситуаций, их предотвращение и устранение;

2.2.8. Охрана имущества, предупреждение и устранение причин (последствий) деятельности, приводящей к порче имущества Учреждения;

2.2.9. Предупреждение случаев хищения имущества Учреждения, хищения личного имущества работников или посетителей музея;

2.2.10. Отслеживание, документальная фиксация, своевременный сбор данных о соблюдения режима внутреннего трудового распорядка работниками Учреждения, контроль за поддержанием установленных внутренних правил посещения объектов Учреждения, контроль трудовой дисциплины и обеспечение объективности при проведении служебных проверок и вынесении дисциплинарных взысканий;

2.2.11. Информационное обеспечение принятия решений руководством Учреждения;

2.2.12. Предоставление информации по запросам соответствующих служб и государственных органов осуществляется без письменного согласия субъекта персональных данных с целью противодействия терроризму, противодействия коррупции, защиты правопорядка и т.п., то есть в случаях, предусмотренных частью 2 статьи 11 Федерального закона РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных». Передача материалов видеозаписи осуществляется в соответствии с порядком, установленным для передачи сведений, содержащих персональные данные.

3. Порядок организации системы видеонаблюдения

3.1. В Учреждении имеется объектовая (локальная) открытая система видеонаблюдения в филиалах и помещениях Дирекции. В силу технических причин объектовые системы видеонаблюдения филиалов в единую сеть видеонаблюдения Учреждения не объединены.

3.2. Объектовая система видеонаблюдения включает в себя ряд устройств: камеры, мониторы, устройства коммутации видеосигнала, записывающие устройства, жесткий диск видеорегистратора для хранения архива видеоданных, программное обеспечение системы видеонаблюдения, компьютерное оборудование.

3.3. Запрещается использование устройств для негласного получения информации

(скрытых камер, микрофонов и т.п.).

3.4. Видеонаблюдение на объектах Учреждения ведется непрерывно с записью информации с видеокамер на жесткий диск видеорегистратора.

3.5. В некоторых филиалах Учреждения система видеонаблюдения может осуществляет передачу видеоизображения в режиме реального времени на монитор поста физической охраны, в некоторых филиалах (из-за отсутствия поста физической охраны) система видеонаблюдения записывает видеоизображение в архив на жесткий диск видеорегистратора, доступ к которому имеет ограниченных круг лиц.

3.6. Система видеонаблюдения должна обеспечивать:

3.6.1. Видеофиксацию текущего состояния объекта видеонаблюдения;

3.6.2. Сохранение архива видеозаписей для последующего анализа сроком не менее 30 дней;

3.6.3. Воспроизведение ранее записанной информации;

3.6.4. Оперативный доступ к архиву видеозаписей за конкретный период времени.

3.7. Работникам Учреждения **запрещается** загораживать, накрывать камеры видеонаблюдения посторонними предметами или иным способом ограничивать нормальное функционирование системы видеонаблюдения на объектах Учреждения.

3.8. **Посетители** объектов Учреждения, которые потенциально могут попасть или попадают в зону видеонаблюдения, **информируются о ведении видеонаблюдения посредством размещения специальных объявлений и общепринятых знаков**, иными способами, позволяющими гражданину принять решение о том, готов ли он стать объектом видеонаблюдения.

3.9. При оформлении на работу на вакантную должность в Учреждении соискатель предупреждается о наличии на объектах Учреждения открытой системы видеонаблюдения и о необходимости получения от него **письменного согласия** на обработку его биометрических (фото – видео изображение) персональных данных (Приложение №1 к Положению). При несогласии предоставить Учреждению, как оператору персональных данных, такое согласие письменно, соискатель не может претендовать на вакантную должность в Учреждение[1].

3.10. Функции по обеспечению бесперебойного функционирования объектовой системы видеонаблюдения возлагается в порядке, указанном в Федеральном законе «О контрактной системе в сфере закупок товаров, работ или услуг для обеспечения государственных или муниципальных нужд» от 05.04.2013 № 44 (с изменениями и дополнениями), на сотрудников сторонних организаций, имеющих соответствующий опыт и навык работы с такими системами.

3.11. При заключении договоров со сторонними организациями, которые могут получить доступ к системе видеонаблюдения Учреждения в рамках выполнения своих полномочий (охранные услуги, техническое обслуживание системы охранного видеонаблюдения) предусмотреть обязательства работников этих организации соблюдать конфиденциальность в рамках исполнения таких договоров и не разглашать третьим лицам информацию, полученную при просмотре видеоинформации с объектовой системы видеонаблюдения Учреждения. Копия настоящего Положения передается руководителю охранной организации с целью контроля исполнения изложенных в нем требований работниками данной охранной организации при осуществлении возложенных на них обязанностей.

4. Порядок доступа к записям системы видеонаблюдения. Просмотр, хранение, порядок уничтожения, передача третьим лицам.

4.1. Запись информации с камер видеонаблюдения осуществляется непрерывно (24 часа в сутки) и подлежит хранению в течение не менее 30 дней.

Информация, полученная с камер видеонаблюдения локальной системы, не подлежит длительному хранению и автоматически уничтожается через 30 дней по мере заполнения

[1] ч.1 ст. 7 ФЗ-152 от 27.07.2006 «О персональных данных»

памяти жесткого диска видеорегистратора путем наложения новой записи с камер видеонаблюдения на архивную запись.

Информация, после записи с камер видеонаблюдения, является конфиденциальной, не подлежит перезаписи с жесткого диска видеорегистратора, редактированию, передаче третьим лицам, кроме особых случаев, предусмотренных действующим законодательством РФ.

4.2. Если по запросу правоохранительных органов или в ходе внутренней проверке через систему видеонаблюдения на объекте был выявлен факт совершения правонарушения или преступления, часть архивной записи с данным фактом может храниться в течение срока исковой давности (не менее 3 лет – не более 10 лет)[2], на отдельном носителе.

4.3. На объектах Учреждения, где имеется пост физической охраны, изображение с камер видеонаблюдения выводится круглосуточно в режиме онлайн на монитор поста охраны с целью своевременного реагирования охраны на возникшие чрезвычайные ситуации на охраняемом Объекте.

4.4. На объектах Учреждения, где нет поста физической охраны, изображение с камер видеонаблюдения записывается в архив на жесткий диск видеорегистратора.

4.5. Видеорегистратор должен иметь возможность технического подключения монитора к нему для контроля и настройки объектовой системы видеонаблюдения Объекта.

4.6. Доступ к просмотру архива записей видеонаблюдения, хранящимся на жестком диске видеорегистратора, имеют:

– директор Учреждения;

– заместитель директора по административной и правовой работе;

– заместитель директора по безопасности;

– работники отдела безопасности;

– работники юридического отдела;

– заведующий филиалом, где установлена объектовая система видеонаблюдения;

– иные лица, назначенные приказом директора Учреждения.

4.7. С должностных лиц, указанных в п.4.6. данного Положения, берется обязательство о неразглашении персональных данных, ставших им известным по роду своей деятельности[3] (Приложение №2 к Положению).

4.8. Доступ к просмотру камер видеонаблюдения, а также к архиву видеозаписей, хранящемуся на жестком диске видеорегистратора локальной системы видеонаблюдения, так же имеют:

– сотрудники охраны (при наличии на объекте договора с Учреждением);

– сотрудники организации, осуществляющие обслуживание системы видеонаблюдения на Объекте (по договору с Учреждением).

4.9. При заключении договорных отношений со сторонними организациями, которые получают доступ к локальной системе видеонаблюдения Учреждения, в текст договора в обязательном порядке необходимо вносить условие о неразглашении потенциальным контрагентом (его работниками) конфиденциальной информации (в том числе сведений, содержащих персональные данные), полученной при исполнении договорных обязательств с Учреждением.

4.10. По требованию лица, изображенного на видеозаписи[4], ему свободный доступ к его персональным данным на видеозаписи не предоставляется, т.к. такой доступ нарушает права и законные интересы третьих лиц, изображение которых имеется на видеозаписи и письменное разрешение от них на это оператором персональных данных (Учреждение) не получено[5].

Просмотр видеозаписи субъектом персональных данных возможен только в случае отсутствия на запрашиваемом фрагменте видеозаписи изображения иных субъектов персональных данных либо в случаях, указанных в п.4.12 данного Положения.

4.11. Просмотр записанных изображений осуществляется должностными лицами,

---

[2] ст. 196 ГК РФ

[3] ст. 86 ТК РФ; ст.7 ФЗ-152 от 27.07.2006 «О персональных данных»

[4] ч.7 ст. 14 ФЗ-152 от 27.07.2006 «О персональных данных»

[5] п.4 ч.8 ст. 14 ФЗ-152 от 27.07.2006 «О персональных данных»

указанными в п.4.6. данного Положения, в условиях ограниченного доступа (при отсутствии посторонних лиц).

4.12. Для защиты личных и (или) публичных интересов (т.е. выявления факта конфликтной ситуации, совершенного правонарушения) в просмотре могут участвовать лица: изображенные на видеозаписи, их законные представители (родители, попечители и т.д.), а также работники юридического отдела Учреждения, работники отдела безопасности Учреждения, сотрудники правоохранительных органов (в соответствии с совершаемыми ими процессуальными действиями).

4.13. Лица, указанные в п.4.6. данного Положения, на основании и в соответствии с законодательством РФ, обязаны пропускать сотрудников правоохранительных органов при предъявлении ими своего служебного удостоверения (сотрудников полиции[6], следственного комитета России[7], ФСБ России[8], прокуратуры России[9]) к просмотру информации локальной системы видеонаблюдения Учреждения.

4.14. Передача копии части архива записей камер видеонаблюдения третьей стороне допускается только в исключительных случаях (по письменному запросу правоохранительных[10] и судебных органов[11]). Вопрос о передаче копий части архива видеозаписей решает директор Учреждения путем проставления резолюции на запросе правоохранительных или судебных органов, на докладной записке заведующего филиалом, начальника отдела безопасности или заместителя директора по безопасности Учреждения.

4.15. Контроль за обеспечением работоспособности локальной объектовой системы видеонаблюдения в филиале Учреждения, ответственность за организацию просмотра архива видеозаписей, копирование и подготовку к выдаче архивной видеоинформации осуществляет заведующий филиалом, в помещении Дирекции – начальник отдела безопасности Учреждения.

4.16. Ответственность за своевременное информирование лиц, указанных в п.4.15 данного Положения, о нарушении режима работы объектовой системы видеонаблюдения (при наличии поста физической охраны), возлагается на сотрудников охранной организации, осуществляющих физическую охрану Объекта по договору с Учреждением или на сотрудников обслуживающей организации, по договору с Учреждением осуществляющей её техническое обслуживание.

5. Ответственность за нарушение правил обработки персональных данных

5.1. Лицо, виновное в несоблюдении пунктов данного Положения, повлекшее причинении вреда путем распространения конфиденциальных записей объектовых системы видеонаблюдения Учреждения, несет ответственность в порядке, предусмотренном действующим законодательством РФ.

5.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, правил обработки персональных данных, установленных Законодательством, а также требований к защите персональных данных подлежат возмещению в соответствии с законодательством Российской Федерации.

6. Техническое сопровождение обеспечения видеонаблюдения.

6.1. Лицо, ответственное за обеспечение процесса видеонаблюдения на Объектах Учреждение, обязано своевременно принимать меры по устранению технических неполадок в работе соответствующего оборудования.

6.2. С целью технического обслуживания и ремонта оборудования локальных систем видеонаблюдения Учреждение привлекает специализированные организации на основании договорных отношений.

---

[6] п.5 ч.1 ст.12 ФЗ-3 «О полиции»

[7] п.3 ч.1. ст.7 ФЗ-403 «О Следственном комитете Российской Федерации»

[8] п. «З» ч.1 ст.13 ФЗ-40 «О федеральной службе безопасности»

[9] п.1 ст.22 ФЗ-2202-1 «О прокуратуре Российской Федерации»

[10] п.4 ч.1 ст.12 ФЗ-3; п.3 ч.1. ст.7 ФЗ-403; п. «М» ч.1 ст.13 ФЗ-40; п.1 ст.22 ФЗ-2202-1.

[11] ст.13 ГПК РФ; ст. 16 АПК РФ; ст. 392 УПК РФ

6.3. При заключении договорных отношений со сторонней организацией в проект договора необходимо вносить условие о неразглашении потенциальным контрагентом (его работниками) конфиденциальной информации (в том числе сведений, содержащих персональные данные), полученной при исполнении договорных обязательств.

7. Заключительные положения.

7.1. Настоящее Положение вводится в действие с момента утверждения его приказом директора Учреждения.
7.2. Изменения и дополнения настоящего Положения вносятся приказом директора Учреждения.
7.3. Положение действует до момента утверждения и введения в действие нового Положения.

Подготовил:

Начальник отдела безопасности С.А. Макаренко

Приложение №1
к Положению по организации работы
системы видеонаблюдения

ОБРАЗЕЦ

Согласие
на обработку биометрических персональных данных
в ГБУК ЛО «Музейное агентство»

г. Санкт- Петербург «___» _____ 202__ г.

Я, _____
(ФИО полностью)

паспорт _____ выдан _____
_____,

адрес: _____

_____

в соответствии со ст.9 и 11 Федерального закона от 27.07.2006 №152 –ФЗ «О персональных данных» **даю по своей воле и в своих интересах свое согласие на обработку моих биометрических персональных данных** оператором ГБУК ЛО «Музейное агентство» (ИНН 7825414608) с целью оформления мне пропуска в помещения с ограниченным доступом на территории ГБУК ЛО «Музейное агентство», обеспечение контроля безопасности производства работ, сохранности моего имущества и имущества оператора.

Согласие относится к следующим биометрическим персональным данным: **фото-видеоизображения**.

Настоящее согласие предоставляется мною на осуществление действий в отношении моих биометрических персональных данных, которые необходимы для достижения указанной выше цели, включая (без ограничений) сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение) извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, а также осуществление любых иных действий, предусмотренных действующим законодательством Российской Федерации.

Я проинформирован, что оператор гарантирует обработку моих биометрических персональных данных в соответствии с действующим законодательством Российской Федерации как автоматизированным, так и неавтоматизированным способами.

Настоящее согласие **действительно** в течение действия моего трудового договора от «____» _____ 202__ года № _____ и может быть отозвано путем письменного заявления в произвольной форме.

_____ _____ /_____/
(должность) (подпись) (ФИО)

Приложение №2
к Положению по организации работы
системы видеонаблюдения

ОБРАЗЕЦ

Обязательство
о неразглашении персональных данных
в ГБУК ЛО «Музейное агентство»

г. Санкт- Петербург «___» _____ 202__ г.

Я, _____
(ФИО полностью)

паспорт _____ выдан _____
_____,

адрес: _____

_____

исполняющий (-ая) должностные обязанности в ГБУК ЛО «Музейное агентство» по должности _____

предупрежден (-а) о том, что на период исполнения должностных обязанностей в соответствии с должностной инструкцией мне будет предоставлен допуск к информации, содержащей персональные данные третьих лиц, обработку которых я буду осуществлять.

Настоящим **добровольно принимаю на себя обязательства**:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному руководителю.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. После прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я **предупрежден (-а)**, что в случае нарушения данного обязательства я буду привлечен к ответственности, предусмотренной трудовым, гражданским, административным и уголовным законодательством РФ.

С правилами обработки персональных данных ознакомлен (-а).

_____ _____ /_____/
(должность) (подпись) (ФИО)