**Муниципальное бюджетное учреждение**
**«Краеведческий музей городского округа Сызрань»**

# ПРИКАЗ

«04» августа 2014 г. № ____дсп

Сызрань

***Об утверждении***
***положения об обеспечении безопасности персональных данных***
***в информационных системах МБУ «Краеведческий музей г. о. Сызрань»***

Во исполнение требований Федерального закона №152-ФЗ от 27.07.2006 г. «О персональных данных», а также прочих нормативных документов по защите информации,

## ПРИКАЗЫВАЮ:

1. Утвердить «Положение об обеспечении безопасности персональных данных в информационных системах Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань»» (Приложение 1).
2. Требования настоящего приказа довести до заинтересованных лиц.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор М. В. Питьёва

**Приложение 1**
к Приказу
от «04» августа 2014 г. № 54-1

**УТВЕРЖДАЮ**

Директор МБУ «Краеведческий музей г. о. Сызрань»

_____ Питьёва М.В.

«04» августа 2014 г.

# ПОЛОЖЕНИЕ
## об обеспечении безопасности персональных данных в информационных системах Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань»

Сызрань
2014

**Содержание:**

# ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники.

**Автоматизированное рабочее место (АРМ)** — программно-технический комплекс автоматизированной системы, предназначенный для автоматизации деятельности определенного вида.

**Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

**Инцидент информационной безопасности** – событие, в результате наступления которого произошло разглашение конфиденциальной информации, нарушение работоспособности ИСПДн, внесение несанкционированных изменений, утечка или разглашение персональных данных клиентов и прочих событий, ведущих к нарушению прав и свобод граждан РФ.

**Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Конфиденциальность персональных данных** - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных или наличия иного законного основания.

**Контролируемая зона** - это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

**Обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

**Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или)

осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

**Персональные данные (ПДн)** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных**).**

**Предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

**Распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

**Система защиты персональных данных (СЗПДн)** – система защиты персональных данных включает в себя организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

**Средства криптографической защит информации (СКЗИ)** – к СКЗИ относятся аппаратные, программно-аппаратные и программные средства, реализующие криптографические алгоритмы преобразования информации с целью защиты информации при ее обработке, хранении и передаче по каналам связи.

**Трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

**Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

# I. ОБЩИЕ ПОЛОЖЕНИЯ

## 1. Введение

1.1 Положение об обеспечении безопасности персональных данных в информационных системах (далее - Положение) Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань» (далее – Организация или МБУ «Краеведческий музей г. о. Сызрань») разработано в соответствии с законодательством Российской Федерации о ПДн и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ПДн при их обработке в ИСПДн.

1.2 Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение являются:

- Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.
- Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
- «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008 г. № 512.
- Нормативно-методические документы Федеральной службы по техническому и эксперт-ному контролю Российской Федерации по обеспечению безопасности ПДн при их обработке в ИСПДн.

1.4 Настоящее Положение вступает в силу с момента его утверждения директором МБУ «Краеведческий музей г. о. Сызрань» и действует бессрочно, до замены его новым Положением.

1.5 Все изменения в Положение вносятся приказом директора МБУ «Краеведческий музей г. о. Сызрань».

1.6 Все сотрудники Организации допущенные к обработке ПД должны быть ознакомлены с настоящим Положением под роспись.

## 2. Область применения и цель положения

2.1 Настоящее положение принято в целях определения основных принципов построения системы защиты ПДн при их обработке в информационных системах ПДн, представляющих собой совокупность ПДн, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации.

2.2 Под техническими средствами, позволяющими осуществлять обработку ПДн, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн, программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

## 3. Методы и способы защиты персональных данных

3.1 Методы и способы защиты персональных данных определяются в соответствии нормативными документами по защите информации (Федеральный Закон № 152-ФЗ «О персональных данных», Постановления Правительства, Приказы ФСТЭК и ФСБ России).

3.2 Система защиты персональных данных должна соответствовать требованиям нормативных и руководящих документов ФСТЭК и ФСБ России.

## 4. Цели и принципы обеспечения безопасности

4.1 Целью обеспечения безопасности являются:

- организация непрерывного и защищенного процесса обработки, хранения, передачи информации, содержащей ПДн;
- защита прав и свобод граждан РФ, предоставляющих Организации свои ПДн для обработки и хранения.

4.2 Принципы обеспечения безопасности:

- основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов;
- обеспечивается комплексом правовых, организационных и технических мер (программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики информационной системы);
- должны обеспечиваться на всех этапах обработки информации и во всех режимах функционирования;
- должны предусматривать контроль эффективности средств защиты.

4.3 Информационная безопасность персональных данных должна основываться на следующих принципах:

- *Принцип системности* - системный подход к защите компьютерных систем предполагает необходимость взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов при всех видах информационной деятельности и информационного проявления. При обеспечении информационной безопасности информационных систем необходимо учитывать все слабые и наиболее уязвимые места системы, а также характер, возможные объекты и направления атак на систему со стороны нарушителя, пути проникновения распределенной системы и НСД к информации.

- *Принцип комплексности* - для обеспечения защиты имеется широкий спектр мер, методов и средств защиты компьютерных систем. Комплексное их использование предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающие все существующие каналы угроз и не содержащие слабых мест на стыках отдельных её компонентов.

- *Принцип непрерывности защиты* – защита информации - это не разовое мероприятие и не конкретная совокупность проведенных мероприятий и установленных средств защиты, а непрерывный направленный процесс предполагающий принятие соответствующих мер на всех этапах существования информационной системы. Разработка системы защиты должна вестись параллельно обработке самой защищаемой системы.

- *Разумная достаточность* - важно правильно выбрать тот уровень защиты при котором затраты, риск и размер возможного ущерба были бы приемлемы и не создавали неудобств пользователю.

- *Гибкость системы защиты* - часто приходится создавать систему защиты в условиях большой неопределенности, поэтому принятые меры и средства защиты особенно в начальный период их эксплуатации могут оказывать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения уровня варьирования защищенности средство защиты должно обладать определенной гибкостью, особенно если средство необходимо установить на работающую систему, не нарушая процесса её нормального функционирования.

- *Принцип простоты применения средств защиты* - механизмы защиты должны быть интуитивно понятны и просты в применении. Применение средств защиты не должно быть связано со знанием каких либо языков или требовать дополнительных затрат на её применение, а также не должно требовать выполнения рутинных малопонятных операций.

# II. ОРГАНИЗАЦИЯ РАБОТ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

## 5. Определение перечня персональных данных

5.1 На начальном этапе внедрения ИСПДн определяется перечень обрабатываемых ПДн. Каждый элемент перечня обрабатываемых ПДн должен быть элементарным (то есть не должен быть получен объединением других элементов, например, элемент «ФИО и паспорт» на самом деле состоит из двух элементов списка: ФИО, паспорт), с указанием цели обработки.

5.2 Перечень обрабатываемых ПДн утверждается директором МБУ «Краеведческий музей г. о. Сызрань».

## 6. Согласие субъекта персональных данных на обработку

6.1 На основании перечня обрабатываемых ПДн определяется требование согласия субъекта на обработку его ПДн, за исключением случаев указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152-ФЗ «О персональных данных».

6.2 Форма «Согласия на обработку персональных данных» (Приложение 1) должна содержать следующие данные:

- фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн);
- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта ПДн;
- цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие субъекта ПДн;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка будет поручена такому лицу;
- перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;

- срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено Федеральным законом;
- подпись субъекта ПДн.

## 7. Уведомление о начале обработки персональных данных

7.1 С помощью перечня обрабатываемых ПДн определяется необходимость отправки уведомления в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор России).

7.2 Отправка не требуется в случаях, указанных в части 2 статьи 22 Федерального закона № 152-ФЗ «О персональных данных». В иных случаях через Портал персональных данных Роскомнадзора России оформляется уведомление в электронном виде.

## 8. Определение политики в отношении обработки персональных данных

8.1 Политика в отношении обработки ПДн в Организации является официальным документом, в котором определены общие принципы, условия и цели обработки ПДн и сведения о реализуемых требованиях к защите ПДн.

8.2 Политика в отношении обработки ПДн распространяется на всех сотрудников оператора, включая сотрудников, работающих по договору подряда, а также на сотрудников сторонних организаций, взаимодействующих с оператором на основании соответствующих нормативных, правовых и организационно-распорядительных документов.

8.3 Все сотрудники Организации должны быть ознакомлены с политикой в отношении обработки ПДн.

8.4 Политика в отношении обработки ПДн должна быть опубликована в общедоступных источниках информации.

8.5 Политика в отношении обработки ПДн утверждается директором МБУ «Краеведческий музей г. о. Сызрань».

## 9. Определение политики в отношении обработки персональных данных сотрудников организации

9.1 Положение об обработке персональных данных сотрудников в Организации, является официальным документом, в котором определен порядок обработки и защиты ПДн сотрудников.

9.2 Все сотрудники Организации должны быть ознакомлены с Положением об обработке ПДн сотрудников в Организации, а также со всеми дополнениями и изменениями

к нему, под роспись. При приеме на работу ознакомление производится до подписания трудового договора.

9.3 Положение об обработке ПДн сотрудников в Организации утверждается директором МБУ «Краеведческий музей г. о. Сызрань»

## 10. Определение ответственных за обработку и обеспечение защиты персональных данных

10.1 За вопросы безопасности в Организации несут ответственность:

- директор МБУ «Краеведческий музей г. о. Сызрань»;
- ответственный за организацию обработки ПДн;
- ответственный за обеспечение безопасности ПДн;
- ответственный за технические средства обработки ПДн;
- сотрудники, допущенные к ПДн в связи со служебной необходимостью.

10.2 Лица, ответственные за организацию обработки, обеспечение безопасности и технические средства обработки ПДн, назначаются из состава сотрудников Организации.

10.3 Ответственные могут быть выделены либо как штатные единицы, либо выполнять функции назначенные приказами директора МБУ «Краеведческий музей г. о. Сызрань»:

- приказ о назначении ответственного за организацию обработки ПДн;
- приказ о назначении ответственного за обеспечение безопасности ПДн;
- приказ о назначении ответственного за технические средства обработки ПДн.

10.4 Ответственный за организацию обработки ПДн - лицо, отвечающее за организацию и состояние процесса обработки ПДн.

10.5 Ответственный за обеспечение безопасности ПДн – лицо, отвечающее за правильность использования и нормальное функционирование установленной системы защиты информации, реализующей меры по обеспечению безопасности ПДн.

10.6 Ответственный за технические средства обработки ПДн - лицо, отвечающее за правильность использования и бесперебойное, стабильное функционирование установленных систем обработки ПДн.

10.7 Ответственные в своей работе должны руководствоваться утвержденными директором МБУ «Краеведческий музей г. о. Сызрань» инструкциями, определяющими их функции, права и обязанности.

10.8 Лица, ответственные за организацию обработки, обеспечение безопасности и технические средства обработки ПДн несут ответственность за неразглашение и

корректность обработки ПДн в соответствии с административным и уголовным Кодексами Российской Федерации.

## 11. Создание комиссии по организации работ по защите персональных данных

11.1 Для организации работ по защите информации создается комиссия по организации работ по защите ПДн.

11.2 Состав лиц комиссии по организации работ по защите ПДн и ее создание оформляется приказом директора МБУ «Краеведческий музей г. о. Сызрань».

11.3 Функциональные обязанности комиссии по организации работ по защите ПДн изложены в утвержденном директором МБУ «Краеведческий музей г. о. Сызрань» «Положении о комиссии для организации работ по защите персональных данных».

## 12. Определение контролируемой зоны и помещений обработки персональных данных

12.1 Контролируемая зона может ограничиваться периметром охраняемой территории частично, охраняемой территорией, охватывающей здания и сооружения, в которых проводятся закрытые мероприятия, частью зданий, комнатой, кабинетом, в которых проводятся закрытые мероприятия. Контролируемая зона может устанавливаться размером больше, чем охраняемая территория, при этом она должна обеспечивать постоянный контроль за неохраняемой частью территории.

12.2 Территория контролируемой зоны определяется приказом директора МБУ «Краеведческий музей г. о. Сызрань».

12.3 Территория контролируемой зоны должна включать в себя помещения Организации, в которых содержатся:

- системы обработки ПДн;
- системы хранения данных, содержащих ПДн;
- системы резервного копирования систем обработки и хранения ПДн;
- системы защиты информации;
- станции ввода, обработки, просмотра ПДн.

12.4 Перечень помещений, в которых ведется обработка ПДн, утверждается директором МБУ «Краеведческий музей г. о. Сызрань».

## 13. Определение списка лиц, имеющих доступ к обработке персональных данных

13.1 Лица, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим ПДн на основании «Списка должностных лиц для предоставления доступа к персональным данным», утвержденного директором МБУ «Краеведческий музей г. о. Сызрань».

13.2 Операторы и иные лица, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта ПДн, если иное не предусмотрено Федеральным законом.

13.3 Круг лиц, имеющих доступ к ПДн, должен быть достаточным для выполнения непрерывной и бессбойной обработки ПДн, и при этом быть максимально ограниченным для снижения рисков утечки информации.

13.4 «Список должностных лиц для предоставления доступа к персональным данным» может представлять собой перечень структурных подразделений непосредственно собирающих и обрабатывающих ПДн.

## 14. Определение прав доступа лиц, имеющих доступ к обработке персональных данных

14.1 Права доступа лиц, имеющих доступ к обработке ПДн, определяются в необходимом и достаточном объеме для осуществления обработки.

14.2 Предоставление прав реализуется ответственным за обеспечение безопасности ПДн. Объем необходимых прав определяется по согласованию с руководителем подразделения, осуществляющего обработку ПДн.

14.3 Права доступа сотрудников к информационным ресурсам, содержащим ПДн регламентированы «Матрицей доступа сотрудников к защищаемым информационным ресурсам ИСПДн», утвержденной директором МБУ «Краеведческий музей г. о. Сызрань».

## 15. Определение прав доступа лиц, имеющих доступ к сопровождению систем защиты и обработки персональных данных

15.1 Права доступа лиц, имеющих доступ к сопровождению систем защиты и обработки ПДн, определяются из соображений разделения ролей обеспечения безопасности ПДн и обеспечения работы систем обработки ПДн.

15.2 Роль обеспечения безопасности должна реализовывать следующие функции:

- аудит доступа (организационный и инструментальный);
- назначение прав доступа;
- установка и удаление из системы средств защиты информации;
- управление настройками средств защиты информации.

15.3 Роль обеспечения работы систем обработки ПДн должна реализовывать следующие функции:

- установка и удаление средств обработки ПДн;
- управление настройками средств обработки ПДн;
- установка и удаление вспомогательных средств обработки ПДн и не связанных с обработкой систем;
- управление настройками вспомогательных средств обработки ПДн и не связанных с обработкой систем.

15.4 Права доступа сотрудников к информационным ресурсам, содержащим ПДн регламентированы «Матрицей доступа сотрудников к защищаемым информационным ресурсам ИСПДн», утвержденной директором МБУ «Краеведческий музей г. о. Сызрань».

## 16. Проектирование системы защиты персональных данных

16.1 Проектирование системы защиты ПДн состоит из нескольких этапов:

- определение актуальных угроз безопасности ИСПДн;
- определение уровня защищенности ИСПДн;
- определение мер по обеспечению безопасности ПДн;
- выполнение необходимых мер по обеспечению безопасности ПДн.

16.2 Комиссия по организации работ по защите ПДн, путем экспертной оценки определяет актуальные угрозы безопасности ИСПДн.

16.2.1 Модель угроз безопасности ИСПДн разрабатывается в соответствии с РД «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России.

16.2.2 Ответственный за обеспечение безопасности ПДн оформляет результаты определения актуальных угроз безопасности ИСПДн в виде «Модели угроз безопасности ПДн при их обработке в ИСПДн» (далее - Модель угроз безопасности ИСПДн).

16.3 Комиссией по организации работ по защите ПДн оформляется результат определения уровня защищенности ИСПДн в виде «Акта определения уровня защищенности (классификации) ИСПДн».

16.3.1 Уровень защищенности ИСПДн определяется на основании результата анализа исходных данных и модели угроз безопасности ИСПДн, в соответствии с постановлением

Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

16.4 Комиссией по организации работ по защите ПДн формируется набор требований к обеспечению безопасности ПДн.

16.4.1 На основании результатов определения актуальных угроз безопасности ИСПДн и определения уровня защищенности ИСПДн, в соответствии с приказом ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» формируется набор требований к обеспечению безопасности ПДн.

16.4.2 Ответственный за обеспечение безопасности ПДн оформляет окончательный набор требований к обеспечению безопасности ПДн в виде «Технических требований к системе защиты в ИСПДн» и «Описания системы защиты информации в ИСПДн …».

16.5 Ответственный за обеспечение безопасности ПДн оформляет результаты выполнения необходимых мер по обеспечению безопасности ПДн в виде «Формуляра ИСПДн».

## 17. Оценка соответствия внедренной системы защиты персональных данных

17.1 Оценка соответствия внедренной системы защиты проводится с использованием сертифицированных в системе сертификации ФСТЭК России инструментальных средств с оформлением заключения о готовности системы защиты или проведении аттестационных испытаний с привлечением лицензиата ФСТЭК России.

17.2 В случае аттестации, при успешных испытаниях выдается «Аттестат соответствия ИСПДн требованиям по безопасности информации».

## 18. Квалификация персонала

18.1 Сотрудники, участвующие в обработке ПДн, должны иметь соответствующее образование и квалификацию, позволяющие им корректно работать со средствами обработки информации.

18.2 Не разрешается допуск лиц, не прошедших собеседование с руководителем подразделения на предмет проверки знаний по работе с средствами обработки.

# III. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

## 19. Порядок предоставления доступа к информационным ресурсам, содержащим персональные данные

19.1 Доступ сотрудника к персональным данным осуществляется в соответствии с занимаемой должностью и в объеме, необходимом для выполнения должностных обязанностей

19.2 На каждую ИСПДн должна быть разработана «Матрица доступа сотрудников к защищаемым информационным ресурсам ИСПДн», в которой для каждого информационного ресурса содержащего ПДн регламентирован перечень допущенных сотрудников.

19.3 В общем виде порядок доступа новых сотрудников должен осуществляться по следующей схеме:

1) принимаемый сотрудник в соответствии с занимаемой должностью и в соответствии со «Списком лиц имеющих доступ к обработке ПДн» наделяется правом доступа к обработке ПДн;

2) ответственный за организацию обработки персональных данных инструктирует сотрудника и доводит до сведения следующие документы:

- перечень обрабатываемых ПДн;
- настоящее Положением;

3) принимаемый сотрудник в обязательном порядке, заполняет «Обязательство о неразглашении информации конфиденциального характера» (Приложение 2);

4) ответственный за организацию обработки персональных данных заводит в «Журнал учета лиц, имеющих доступ к обработке персональных данных» (Приложение 3) нового сотрудника.

5) ответственный за обеспечение безопасности персональных данных заводит в информационную систему нового пользователя, наделяет его необходимыми правами доступа к ресурсам.

6) ответственный за обеспечение безопасности персональных данных передает пользователю идентификационную информацию (логин/пароль).

## 20. Порядок прекращения доступа к информационным ресурсам, содержащим персональные данные

20.1 При прекращении доступа к ПДн, сотрудник (в связи с увольнением или иным причинам отсутствия необходимости обработки ПДн, используя конкретный информационный ресурс) должен расписаться в «Журнале учета лиц, имеющих доступ к обработке ПДн» (Приложение 3), указав дату прекращения доступа.

20.2 Ответственный за обеспечение безопасности вносит соответствующие изменения в информационную систему.

## 21. Порядок предоставления информации органам государственной власти и местного самоуправления, физическим и юридическим лицам

21.1 Оператор должен предоставлять информацию, содержащую ПДн субъекта, третьим лицам только с письменного согласия субъекта ПДн за исключением случаев, предусмотренных частью 2 статьи 9 Федерального закона № 152-ФЗ «О персональных данных».

21.2 Информация, содержащая ПДн субъекта и предоставляемая третьим лицам, должна быть достоверной и не избыточной, по отношению к целям, заявленным этими лицами, при сборе ПДн.

21.3 При передаче обработки ПДн другому лицу на основании договора, оператор должен зафиксировать в нем обязанность указанного лица в обеспечении конфиденциальности ПДн и безопасности данных при их обработке.

21.4 При трансграничной передаче ПДн оператор должен руководствоваться положениями статьи 12 Федерального закона № 152-ФЗ «О персональных данных».

## 22. Порядок работы с электронными журналами обращений пользователей информационной системы к персональным данным

22.1 Правила и порядок протоколирования и анализа (аудита) значимых событий в ИСПДн, направлены на превентивную фиксацию и изучение действий субъектов и объектов в ИСПДн.

22.2 Все события, происходящие в ОС, ИСПДн, других критических приложениях и средствах защиты должны протоколироваться в специальные электронные журналы аудита.

22.3 Аудит событий, зафиксированных в указанных электронных журналах, должен анализироваться в плановом порядке на постоянной основе.

22.4 Электронные журналы аудита должны записываться и вестись в автоматизированном режиме.

22.5 Настройки журналов аудита должны однозначно интерпретировать все значимые события ИСПДн.

22.6 Электронные журналы аудита не должны быть доступны на чтение, уничтожение и модификацию пользователям ИСПДн.

22.7 Электронные журналы аудита должны быть доступны на чтение и архивирование сотруднику, выполняющему функции ответственного за обеспечение безопасности ПДн.

22.8 Размер каждого электронного журнала должен составлять не менее 10 Мб. Затирание старых событий журнала происходит по необходимости по мере заполнения журнала.

22.9Контроль выполнения положений и требований порядка работы с электронными журналами обращений пользователей информационной системы к ПДн должен осуществлять ответственный за обеспечение безопасности ПДн.

## 23. Порядок регистрации инцидентов безопасности

23.1 Любые инциденты безопасности, в которые входят:

- факты попыток и успешной реализации несанкционированного доступа в системы обработки информации, в помещения обработки информации и к хранилищам информации;
- факты сбоя или некорректной работы систем обработки информации;
- факты сбоя или некорректной работы средств защиты информации;
- факты разглашения информации, содержащей ПДн;
- факты разглашения информации о методах и способах защиты и обработки информации, содержащей ПДн,

должны сообщаться сотрудниками Организации ответственному за обеспечение безопасности ПДн.

23.2 По каждому сообщению ответственный за обеспечение безопасности ПДн должен регистрировать инцидент в «Журнале учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств информационной системы ПДн» (Приложение 4), который в дальнейшем должен проходить процедуру расследования комиссией по организации работ по защите ПДн.

## 24. Порядок расследования инцидентов информационной безопасности

24.1 Источником информации об инциденте информационной безопасности может служить:

1) сообщения сотрудников, клиентов Организации, направленные в Организацию в виде сообщений по электронной почте, служебных записок, писем, заявлений и т.д.;

2) уведомления/сообщения органов осуществляющих контроль или надзор за деятельностью Организации;

3) данные, полученные на основании анализа журналов СЗПДн.

24.2 Разбором инцидентов информационной безопасности занимается комиссия по организации работ по защите ПДн, согласно «Инструкции о порядке проведения служебного расследования, нарушений режима информационной безопасности».

## 25. Порядок предоставления информации по обращению субъекта персональных данных

25.1 Все обращения субъектов ПДн регистрируются ответственным за обработку ПДн в «Журнале регистрации обращений субъектов ПДн» (Приложение 5).

25.2 Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

1) подтверждение факта обработки ПДн оператором;

2) правовые основания и цели обработки ПДн;

3) цели и применяемые оператором способы обработки ПДн;

4) наименование и место нахождения оператора, сведения о лицах (за исключением сотрудников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании Федерального закона;

5) обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;

6) сроки обработки ПДн, в том числе сроки их хранения;

7) порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом № 152-ФЗ «О персональных данных»;

8) информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные Федеральным законом № 152-ФЗ «О персональных данных» или другими Федеральными законами.

## 26. Порядок организации безопасности носителей информации

26.1 Материальные носители информации должны храниться в сейфах или запираемых шкафах.

26.2 Все электронные носители информации должны быть промаркированы (возможно использование заводской маркировки) и перечислены в «Журнале учета машинных носителей информации, на которых хранятся и (или) обрабатываются ПДн» (Приложение 6).

26.3 Выдача и сдача электронных носителей осуществляется под роспись пользователя носителя.

26.4 Уничтожением носителей ПДн в электронном виде ПДн в Организации занимается комиссия по организации работ по защите ПДн, утверждённая директором МБУ «Краеведческий музей г. о. Сызрань».

26.5 К ПДн, хранимым в электронном виде относятся файлы, папки, электронные архивы на жестком диске компьютера и машиночитаемых носителях (компакт-дисках CD-R/RW или DVD-R/RW, дискетах 3,5, флеш-носителях).

26.6 Машиночитаемые носители по истечению сроков обработки и хранения на них ПДн, подлежат уничтожению, с целью невозможности восстановления и дальнейшего использования. Это достигается путем деформирования, нарушения единой целостности носителя или его сжигания.

26.7 Комиссия составляет и подписывает в двух экземплярах соответствующий «Акт об уничтожении машиночитаемых носителей и электронных файлов, содержащих персональные данные» (Приложение 7). В течение трех дней после составления «Акты об уничтожении машиночитаемых носителей и электронных файлов, содержащих персональные данные» направляются на утверждение директором МБУ «Краеведческий музей г. о. Сызрань». После утверждения один экземпляр акта остается у ответственного за обеспечение безопасности персональных данных, второй экземпляр передается в архив на хранение.

26.8 Подлежащие уничтожению файлы с ПДн, расположенные на жестком диске информационной системы ПДн, удаляются средствами операционной системы компьютера с последующим «очищением корзины».

26.9 В случае допустимости повторного использования машиночитаемого носителя применяется программное удаление («затирание») содержимого путём его форматирования с последующей записью новой информации на данный носитель.

26.10 Факт уничтожения носителя ПДн фиксируется ответственным за обеспечение безопасности персональных данных в «Журнале учета машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные» (Приложение 6). В графе журнала «Дата и номер акта уничтожения» заносятся соответствующие данные.

## 27. Порядок организации безопасности средств обработки персональных данных

27.1 Безопасность средств обработки ПДн обеспечивается организационными и техническими средствами.

27.2 Организационно осуществляется допуск сотрудников и третьих лиц (если того требует бизнес-процесс), при этом минимизируется круг лиц, имеющих доступ. Права доступа к информации назначаются исходя из их необходимости и достаточности.

27.3 Технически безопасность обеспечивается корректной настройкой средств обработки информации и установкой наложенных средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

27.4 Все средства защиты информации, эксплуатационная и техническая документация к ним, должны быть учтены и занесены ответственным за обеспечение безопасности ПДн в «Журнал учета средств защиты информации, эксплуатационной и технической документации к ним» (Приложение 8).

## 28. Порядок организации безопасности связи

28.1 Каналы передачи данных должны обеспечивать безопасное соединение узлов сети Организации.

28.2 Безопасность может обеспечиваться следующими мерами:

- сегментация сети на зоны обработки ПДн и демилитаризированные зоны посредством физического разделения или с помощью VLAN технологий;
- создание виртуальных защищенных сетей (VPN-технологии) с использованием шифрования на алгоритмах ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001;

- максимальное ограничение доступа и набора протоколов и портов зоны обработки ПДн к сетям общего пользования и сетям международного обмена посредством средств межсетевого экранирования;
- обеспечение сетей обработки ПДн, имеющих подключение к сетям общего пользования и сетям международного обмена, средствами обнаружения и предотвращения вторжений;
- систематический контроль состояния системы защиты средствами активного аудита;
- при прохождении каналов связи вне контролируемой зоны необходимо обеспечивать шифрование передаваемой информации на таких участках.

28.3 Все средства защиты (средства обнаружения и предотвращения вторжений, средства межсетевого экранирования, СКЗИ) должны пройти процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

28.4 При организации обработки и передачи ПДн по каналам связи с использованием сертифицированных ФСБ СКЗИ, ответственным за СКЗИ назначается ответственный за обеспечение безопасности ПДн.

28.5 Ответственный за СКЗИ в своей работе руководствуется приказом ФАПСИ № 152 от 13.06.2001 г. «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

28.6 Все СКЗИ, эксплуатационная и техническая документация к ним должны быть учтены и занесены ответственным за СКЗИ в «Журнал учета средств криптографической защиты информации, эксплуатационной и технической документации к ним» (Приложение 9).

## 29. Порядок организации физической безопасности

29.1 Физическая безопасность организуется следующими средствами:

- организация разрешительной системы доступа в помещения хранения и обработки ПДн;
- использование систем контроля и управления доступом (СКУД);
- учет ключей, электронных ключей доступа (proximity card, touch memory);
- использование физической охраны;
- использование видеонаблюдения;

- конструктивное усиление окон, дверей, стен и иных преград для несанкционированного доступа;
- виброакустическое, визуальное, электромагнитное экранирование средств обработки ПДн и помещений.

## 30. Правила обеспечения безопасности обработки персональных данных

30.1 Сотрудники организации, доступ которых к ПДн необходим для выполнения служебных (трудовых) обязанностей, обязаны руководствоваться следующими инструкциями и правилами:

- инструкция пользователя по работе в информационных системах персональных данных (Приложение 10);
- инструкция по организации парольной защиты в информационных системах персональных данных (Приложение 11);
- инструкция по организации антивирусной защиты в информационных системах персональных данных (Приложение 12).

30.2 Ответственный за организацию обработки ПДн обязан руководствоваться следующими инструкциями и правилами:

- инструкция пользователя по работе в информационных системах персональных данных (Приложение 10);
- инструкция по организации парольной защиты в информационных системах персональных данных (Приложение 11);
- инструкция по организации антивирусной защиты в информационных системах персональных данных (Приложение 12);
- инструкция о порядке проведения служебного расследования, нарушений режима информационной безопасности (Приложение 15).

30.3 Ответственный за обеспечение безопасности ПДн обязан руководствоваться следующими инструкциями и правилами:

- инструкция пользователя по работе в информационных системах персональных данных (Приложение 10);
- инструкция по организации парольной защиты в информационных системах персональных данных (Приложение 11);
- инструкция по организации антивирусной защиты в информационных системах персональных данных (Приложение 12);

- инструкция о порядке проведения служебного расследования, нарушений режима информационной безопасности (Приложение 15).

30.4 Ответственный за технические средства обработки ПДн обязан руководствоваться следующими инструкциями и правилами:

- инструкция пользователя по работе в информационных системах персональных данных (Приложение 10);
- инструкция по организации парольной защиты в информационных системах персональных данных (Приложение 11);
- инструкция по организации антивирусной защиты в информационных системах персональных данных (Приложение 12);
- инструкция по организации обновления общесистемного и прикладного программного обеспечения информационных системах персональных данных (Приложение 13);
- инструкция по организации резервирования и восстановления программного обеспечения и баз данных информационных систем персональных данных (Приложение 14);
- инструкция о порядке проведения служебного расследования, нарушений режима информационной безопасности (Приложение 15).

**Приложение 1**

к Положению об обеспечении безопасности персональных данных в информационных системах Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань» от «___» _____ 2014 г.

# СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

**г. Сызрань** **«___» _____ 20___ г.**

Я,_____
(Фамилия, Имя, Отчество)

_____серия _____№_____ выдан_____
(вид основного документа, удостоверяющий личность)

_____,
(кем и когда)

проживающий(ая) по адресу _____

_____.

В лице представителя субъекта персональных данных (заполняется в случае получения согласия от представителя субъекта персональных данных),

_____
(Фамилия, Имя, Отчество)

_____серия _____№_____ выдан_____
(вид основного документа, удостоверяющий личность)

_____
(кем и когда)

проживающий(ая) по адресу _____
_____.

действующий от имени субъекта персональных данных на основании _____

(реквизиты доверенности или иного документа, подтверждающего полномочия представителя)

принимаю решение о предоставлении персональных данных Муниципальному бюджетному учреждению «Краеведческий музей городского округа Сызрань» (именуемому далее – «Оператор»), расположенному по адресу: 446001, Самарская область, г. Сызрань, пер. Достоевского, 34 и даю согласие на их обработку, как с использованием средств автоматизации, так и без использования таких средств, т.е. на совершение с ними следующих действий:

- сбор;
- систематизацию;
- накопление;
- хранение;

- уточнение (обновление, изменение);
- использование;
- обезличивание;
- блокирование;
- уничтожение;
- передачу персональных данных субъекта третьим лицам в случаях, установленных законодательством РФ;
- получение информации и документов от третьих лиц в случаях, установленных законодательством РФ.

Со следующей целью обработки персональных данных:

_____

_____

_____

Перечень персональных данных, на обработку которых дается согласие субъекта персональных данных (представителя субъекта персональных данных):

| № п/п | Перечень персональных данных |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Персональные данные субъекта подлежат хранению в течении сроков, установленных законодательством РФ, после чего подлежат уничтожению.

Срок, в течение которого действует настоящее согласие _____.

Субъект может отозвать настоящее согласие путем направления письменного заявления об отзыве Оператору. В этом случае Оператор прекращает обработку персональных данных Субъекта, а его персональные данные подлежат уничтожению, если отсутствуют иные правовые основания для обработки, установленные законодательством РФ.

«___» _____ 20__г. _____ _____

(подпись) (Ф.И.О.)

**Приложение 2**

к Положению об обеспечении безопасности персональных данных в информационных системах Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань» от «___» _____ 2014 г.

# ОБЯЗАТЕЛЬСТВО О НЕРАЗГЛАШЕНИИ ИНФОРМАЦИИ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА

**г. Сызрань** **«___» _____ 20___ г.**

Я, _____,

(Фамилия, Имя, Отчество)

заключив трудовой договор (контракт) № _____ от "__" _____ года на работу в Муниципальное бюджетное учреждение «Краеведческий музей городского округа Сызрань» (МБУ «Краеведческий музей г. о. Сызрань») в качестве _____,

(наименование должности)

предупрежден (а), что на период исполнения должностных обязанностей, в соответствии с должностной инструкцией (должностным регламентом) мне будет предоставлен допуск к информации конфиденциального характера. Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

2. Не передавать и не раскрывать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

3. В случае попытки третьих лиц получить от меня конфиденциальные сведения, сообщать непосредственному начальнику.

4. Не использовать конфиденциальные сведения с целью получения выгоды.

5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальных сведений.

6. В течение года после прекращения права на допуск к конфиденциальным сведениям не разглашать и не передавать третьим лицам известные мне конфиденциальные сведения.

Я предупрежден (а), что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

«___» _____ 20__г. _____ _____
(подпись) (Ф.И.О.)

**Приложение 3**

к Положению об обеспечении безопасности персональных данных в информационных системах Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань»
от «___» _____ 2014 г.

# ЖУРНАЛ
## учета лиц, имеющих доступ к обработке персональных данных
## инв. № _____

Начат: «___» _____ 20__г.

Окончен: «___» _____ 20__г.

На _____ листах

| № п/п | Ф.И.О. | Должность | Сведения о допуске к персональным данным | | | | Сведения о прекращении допуска к персональным данным | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | наименование ИСПД/ неавтоматизированная обработка | дата утверждения «Списка…» или дата приказа о назначении на должность | дата и подпись допускаемого лица | дата и подпись ответственного лица | дата утверждения «Списка…» или дата приказа об увольнении | номер приказа об увольнении | дата и подпись лица об ознакомлении с документом, прекращающим допуск к ПДн | дата и подпись ответственного лица |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

**Приложение 4**

к Положению об обеспечении безопасности персональных данных в информационных системах Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань»
от «___» _____ 2014 г.

# ЖУРНАЛ
## учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств информационной системы персональных данных
## инв. № _____

Начат: «____» _____ 20___ г.

Окончен: «____» _____ 20___ г.

На _____ листах

| № п/п | Дата | Краткое описание выполненной работы (нештатной ситуации) | Наименование ИСПДн | ФИО исполнителей и их подписи | ФИО ответственного за эксплуатацию ПЭВМ, подпись | Подпись ответственного за обеспечение безопасности персональных данных | Примечание (ссылка на заявку) |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | | 4 | 5 | 6 | 7 |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**Приложение 5**

к Положению об обеспечении безопасности персональных данных в информационных системах Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань»
от «___» _____ 2014 г.

# ЖУРНАЛ

**учета обращений субъектов персональных данных по вопросам обработки персональных данных**
**инв. № _____**

Начат: «___» _____ 20__г.

Окончен: «___» _____ 20__г.

На _____ листах

| № п/п | Сведения о запрашивающем лице | Краткое содержание обращения | Цель запроса | Отметка о предоставлении информации или об отказе в ее предоставлении | Дата передачи / отказа в предоставлении информации | Подпись ответственного лица | Примечание |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**Приложение 6**

к Положению об обеспечении безопасности персональных данных в информационных системах Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань»
от «___» _____ 2014 г.

**ЖУРНАЛ**
**учета машинных носителей информации,**
**на которых хранятся и (или) обрабатываются персональные данные**
**инв. № _____**

Начат: «____» _____ 20___ г.

Окончен: «____» _____ 20___ г.

На _____ листах

| № п/п | Наименование носителя | Тип носителя | Номер (серийный/ инвентарный) | ФИО ответсвенного за носитель | Примечание | Дата и номер акта уничтожения |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | | | | | | |
| | | | | | | |
| | | | | | | |

## Приложение 7

к Положению об обеспечении безопасности персональных данных в информационных системах Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань» от «___» _____ 2014 г.

**АКТ**

«___» _____ 20__ г. № _____

Сызрань

***Об уничтожении машиночитаемых носителей и электронных файлов, содержащих персональные данные***

Экспертная комиссия в составе:

Председатель:

_____ _____

Члены комиссии:

1. _____ _____
2. _____ _____
3. _____ _____

составили настоящий акт о том, что в результате проведенной экспертной оценки подлежат уничтожению следующие машиночитаемые носители, содержащие персональные данные:

| № п/п | Дата окончания срока обработки зафиксированных на носителе персональных данных | Учетный номер съемного носителя или наименование технического средства ИСПДн, на котором уничтожаются файлы | Примечание |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| | | | |
| | | | |
| | | | |

Всего съемных носителей _____ _____
(цифрами и прописью)

На съемных носителях уничтожены персональные данные путем стирания ее с помощью возможностей операционной системы.

Перечисленные съемные носители уничтожены путем_____

_____

(механического уничтожения, сжигания, разрезания, деформирования и т.п.)

Председатель:

_____ _____ _____

Члены комиссии:

_____ _____ _____

_____ _____ _____

_____ _____ _____

**Приложение 8**

к Положению об обеспечении безопасности персональных данных в информационных системах Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань»
от «___» _____ 2014 г.

**ЖУРНАЛ**
**учета средств защиты информации, эксплуатационной и технической документации к ним**
**инв. № _____**

Начат: «___» _____ 20__г.

Окончен: «___» _____ 20__г.

На _____ листах

| № п/п | Индекс и наименование средства защиты информации | Серийный (заводской) номер | Номер специального защитного знака | Наименование организации, установившей СЗИ | Место установки | Примечание |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | | | | | | |
| | | | | | | |
| | | | | | | |

## Приложение 9

к Положению об обеспечении безопасности персональных данных в информационных системах Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань»
от «___» _____ 2014 г.

# ЖУРНАЛ
# учета средств криптографической защиты информации, эксплуатационной и технической документации к ним
# инв. № _____

Начат: «____» _____ 20___ г.

Окончен: «____» _____ 20___ г.

На _____ листах

| № п.п. | Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов | Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых докумен-тов | Номера экземпляров (криптографичес-кие номера) ключевых документов | Отметка о получении | | Отметка о выдаче | | Отметка о подключении (установке) СКЗИ | | | Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов | | | Примечание |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | От кого получены | Дата и номер сопроводи-тельного письма | Ф.И.О. пользователя криптосредств, производившего подключение (установку) | Дата подключения (установки) и подписи лиц, произведших подключение (установку) | Ф.И.О. пользователя криптосредств, производившего подключение (установку) | Дата подключения (установки) и подписи лиц, произведших подключение (установку) | Номера аппаратных средств, в которые установлены или к кото-рым подклю-чены крипто-средства | Дата изъятия (уничто-жения) | Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение) | Номер акта или расписка об уничтожении | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |

**Приложение 10**

к Положению об обеспечении безопасности персональных данных в информационных системах Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань» от «___» _____ 2014 г.

# ИНСТРУКЦИЯ
# пользователя по работе в информационных системах персональных данных

## 1. Общие положения

1.1 Настоящая инструкция определяет общие положения работы пользователей в ИСПДн МБУ «Краеведческий музей г. о. Сызрань» при автоматизированной обработке информации, содержащей ПДн.

1.2 Допуск пользователей для работы с ПДн осуществляется на основании приказа, который издает директор МБУ «Краеведческий музей г. о. Сызрань», и в соответствии со списком лиц, допущенных к работе в данной ИСПДн.

1.3 Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

1.4 Пользователь отвечает за правильность включения и выключения персональной электронно-вычислительной машины (далее – ПЭВМ), входа в систему и все действия при работе на ПЭВМ.

## 2. Общие обязанности пользователей по обеспечению информационной безопасности

2.1 Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

– строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

– знать и строго выполнять правила работы со средствами защиты информации, установленными в ИСПДн;

– хранить в тайне свой пароль (пароли);

– выполнять требования «Положения об обеспечении безопасности персональных данных в информационных системах» в полном объеме;

– немедленно извещать ответственного за технические средства обработки ПДн и/или ответственного за обеспечение безопасности ПДн в случае утери индивидуального устройства идентификации или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

– нарушении целостности пломб (наклеек), нарушении или несоответствии номеров печатей на составляющих узлах и блоках ПЭВМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к данной защищенной ПЭВМ;

– несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ПЭВМ;

– отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ПЭВМ, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

– некорректного функционирования установленных на ПЭВМ средств защиты;

– новых, неизвестных пользователю, подключенных к ПЭВМ устройств.

## 3. Пользователю ИСПДн категорически ЗАПРЕЩАЕТСЯ:

3.1 Использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях.

3.2 Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения ПЭВМ.

3.3 Осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц.

3.4 Записывать и хранить защищаемую информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации (гибких магнитных дисках, флеш-накопителях и т.п.).

3.5 Оставлять включенной без присмотра ПЭВМ, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры).

3.6 Оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения).

3.7 Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации.

**Приложение 11**

к Положению об обеспечении безопасности персональных данных в информационных системах Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань» от «___» _____ 2014 г.

# ИНСТРУКЦИЯ
# по организации парольной защиты в информационных системах персональных данных

## 1. Общие положения

1.1 Целью применения и реализации инструкции по организации парольной защиты в информационных системах персональных данных является недопущение утечки ПДн, а также их несанкционированной модификации или уничтожения и действует для всех пользователей и администраторов МБУ «Краеведческий музей г. о. Сызрань».

1.2 Правила парольной защиты регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль над действиями пользователей при работе с паролями.

1.3 Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями возлагается на ответственного за обеспечение безопасности ПДн.

## 2. Применение парольной защиты

2.1 Личные пароли должны генерироваться и распределяться централизованно либо создаваться пользователями ИСПДн самостоятельно с учетом следующих требований:

– пароль должен быть не менее 6-ти символов;

– в числе символов пароля ***обязательно должны присутствовать*** буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождения и т.д.), а также общепринятые сокращения (anonymous, user, пользователь и т.п.);

– при смене пароля новое значение должно отличаться от значений 10 предыдущих паролей;

- максимальный срок действия пароля пользователя составляет 90 дней;
- минимальный срок действия пароля пользователя составляет 2 дня;

2.2 Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

2.3 Пользователь не имеет права сообщать личный пароль другим лицам.

2.4 В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п., технологической необходимости использования имен и паролей сотрудников (исполнителей) в их отсутствие, пользователи обязаны сразу после исчерпания инцидента сменить пароль или запросить изменение пароля у ответственного за обеспечение безопасности ПДн.

2.5 Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 90дней.

2.6 Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой на основании письменного указания начальника отдела.

2.7 Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) ответственного за обеспечение безопасности ПДн.

## 3. Ответственность

3.1 Ответственность за действия пользователей ИСПДн при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственного за обеспечение безопасности ПДн.

**Приложение 12**

к Положению об обеспечении безопасности персональных данных в информационных системах Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань» от «___» _____ 2014 г.

# ИНСТРУКЦИЯ
# по организации антивирусной защиты в информационных системах персональных данных

## 1. Общие требования

1.1 Правила антивирусной защиты определяют требования к организации защиты ИСПДн МБУ «Краеведческий музей г. о. Сызрань» от разрушающего воздействия вредоносных программ и устанавливают ответственность руководителя и сотрудников, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

1.2 Целью защиты ИСПДн от вредоносных программ является предотвращение и нейтрализация негативных воздействий вредоносных программ на средства вычислительной техники.

1.3 К использованию в ИСПДн допускаются только лицензионные средства защиты от вредоносных программ (далее – антивирусные средства).

1.4 Установка и начальная настройка антивирусных средств в ИСПДн осуществляется ответственным за обеспечение безопасности ПДн.

1.5 Ответственный за обеспечение безопасности ПДн должен организовывать осуществление периодического обновления сигнатур антивирусных средств и контроль их работоспособности не реже чем, один раз в неделю.

1.6 Пользователи ИСПДн обязаны руководствоваться в работе настоящей инструкцией.

## 2. Применение средств защиты от вредоносных программ

2.1 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

2.2 Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль.

2.3 Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

2.4 В ИСПДн запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

2.5 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с ответственным за обеспечение безопасности ПДн, если он назначен на объекте) должен провести внеочередной антивирусный контроль своего персонального компьютера.

2.6 В случае обнаружения, при проведении антивирусной проверки, зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу персонального компьютера;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение безопасности ПДн;
- провести «лечение» или удаление зараженных файлов.

## 3. Ответственность

3.1 Ответственность за организацию антивирусного контроля в ИСПДн, в соответствии с требованиями настоящей инструкции, возлагается на ответственного за обеспечение безопасности ПДн.

3.2 Ответственность за проведение мероприятий антивирусной защиты ИСПДн и соблюдение требований настоящей инструкции возлагается на ответственного за обеспечение безопасности в организации и всех пользователей ИСПДн.

**Приложение 13**

к Положению об обеспечении безопасности персональных данных в информационных системах Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань» от «___» _____ 2014 г.

# ИНСТРУКЦИЯ
# по организации обновления общесистемного и прикладного программного обеспечения информационных системах персональных данных

## 1. Общие положения

1.1 В системе управления ИСПДн МБУ «Краеведческий музей г. о. Сызрань» должна обеспечиваться и регламентироваться деятельность, связанная с обновлением программного обеспечения (далее – ПО), а также обновлений операционных систем (далее – ОС).

1.2 Тестирование обновлений ПО не должно осуществляться на ресурсах действующей информационной инфраструктуры.

1.3 Правила и порядок обновления ПО, ОС и приложений в целях информационной безопасности ИСПДн направлены на защиту ресурсов от:

- нарушения штатной работы информационных ресурсов и сервисов;
- разрушения;
- нарушения штатного функционирования оборудования;
- несанкционированной модификации;
- несанкционированного копирования.

## 2. Правила управления обновлениями программного обеспечения

2.1 Отслеживание появления новых уязвимостей в используемой ОС, появление обновлений, изготовленных производителями с целью устранения указанных уязвимостей, должно регламентироваться и производиться в плановом порядке.

2.2 Установке обновлений должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий от вновь устанавливаемых обновлений. Для этих целей может быть собран тестовый стенд, имитирующий действующую информационную инфраструктуру.

2.3 В случае обнаружения негативного воздействия устанавливаемого обновления на штатное функционирование информационной инфраструктуры, данное обновление устанавливаться не должно.

2.4 Установке новых версий ПО или внесению изменений и дополнений в действующее ПО должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий указанного ПО.

2.5 Установка протестированных обновлений может быть произведена только на основании решения ответственного за обеспечение безопасности ПДн.

2.6 Установка новых версий ПО или внесение изменений и дополнений в действующее ПО может быть произведено только по согласованию с ответственным за обеспечение безопасности ПДн.

2.7 После проведения работ по установке обновлений и (или) новых версий ПО или внесению изменений и дополнений в действующее ПО ответственным за обеспечение безопасности ПДн должны быть сделаны отметки в «Журнале учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств информационной системы персональных данных» и в «Техническом паспорте (Формуляре) на автоматизированную систему…».

## 3. Ответственность

3.1 Ответственность за выполнением требований настоящей инструкции должен осуществлять ответственный за технические средства обработки ПДн.

**Приложение 14**

к Положению об обеспечении безопасности персональных данных в информационных системах Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань» от «___» _____ 2014 г.

# ИНСТРУКЦИЯ
# по организации резервирования и восстановления программного обеспечения и баз данных информационных систем персональных данных

## 1. Общие требования

1.1 Настоящая инструкция разработана с целью обеспечения возможности незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

1.2 Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности ИСПДн МБУ «Краеведческий музей г. о. Сызрань».

## 2. Порядок резервирования и хранения резервных копий

2.1 Необходимо осуществлять резервное копирование актуальной информации и данных, используемых для полного восстановления баз данных, содержащих ПДн.

2.2 Резервное копирование осуществляется во внешнее хранилище (сервер резервного копирования, HDD, SSD, магнитный диск, CD-ROM, USB накопитель).

2.3 Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль в соответствии с инструкцией по антивирусной защите.

2.4 Еженедельно, в пятницу, по окончании рабочего дня, должно осуществляться полное копирование данных, необходимых для восстановления работы базы данных, содержащих ПДн, во внешнее хранилище.

2.5 Электронные носители, на которые осуществляется резервное копирование актуальных ПДн и их копии должны быть поставлены на соответствующий учет.

2.6 Электронные носители, на которые осуществляется резервное копирование актуальных ПДн, должны храниться в специально оборудованном для хранения месте, обеспечивающем сохранность этих носителей.

2.7 Для организации резервного копирования допускается применение

специализированных программных (программно-аппаратных) комплексов резервного копирования.

## 3. Порядок восстановления работоспособности ИСПДн

3.1 В случае потери работоспособности ИСПДн, должно быть обеспечено ее восстановление из резервной копии.

3.2 Восстановление из резервной копии осуществляется в соответствии с документацией, предлагающейся к системе резервного копирования ПО.

## 4. Порядок восстановления работоспособности ИСПДн

4.1 Ответственность за организацию резервного копирования и восстановления ИСПДн в соответствии с требованиями настоящей инструкции возлагается на сотрудника, ответственного за технические средства обработки ПДн.

**Приложение 15**

к Положению об обеспечении безопасности персональных данных в информационных системах Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань» от «___» _____ 2014 г.

# ИНСТРУКЦИЯ
# о порядке проведения служебного расследования, нарушений режима информационной безопасности

## 1. Общие положения

1.1 Данный порядок устанавливает правила классификации инцидентов информационной безопасности и процедуры служебного расследования (назначения, проведения и выработки выводов) для определения мер по возможному предотвращению инцидентов информационной безопасности.

## 2. Классификация инцидентов информационной безопасности

2.1 Инциденты информационной безопасности и их последствия классифицируются по значимости на:

- Нарушения I категории.
- Нарушения II категории.
- Нарушения III категории.

2.2 Нарушения I категории, к каковым относятся нарушения, повлекшие за собой разглашение (утечку) защищаемых ПДн и/или утрату содержащих их отчуждаемых носителей, уничтожение (искажение) ИСПДн, выведение из строя технических и программных средств, а именно:

- подбор административного пароля (успешный);
- несанкционированная реконфигурация параметров ИСПДн;
- утрата учтенного отчуждаемого съемного носителя;
- утрата или кража резервной копии базы ПДн;
- несанкционированная передача массивов ПДн;
- несанкционированное копирование ПДн на внешние неучтенные носители;
- умышленное нарушение работоспособности ИСПДн;

– несанкционированный доступ к ПДн ИСПДн;

– несанкционированное внесение изменений в ИСПДн;

– умышленное заражение компьютеров и серверов ИСПДн вирусами;

– проведение работ с ИСПДн, повлекшее за собой необратимую потерю данных.

2.3 Нарушения II категории, к каковым относятся: нарушения, в результате которых возникают предпосылки к разглашению (утечке) защищаемых ПДн, утрате содержащих их отчуждаемых носителей, уничтожению (искажению) ИСПДн, выведению из строя технических и программных средств, а именно:

– ошибка при входе в ИСПДн (набор не назначенного пароля, более пяти раз подряд, периодически);

– несанкционированное (неоднократное) оставление включенного ПК без активации средств защиты;

– перезагрузка компьютера, при сбоях в работе ПК, (неоднократная) в т.ч. аварийная (неоднократная) перезагрузка, путем нажатия кнопки RESET;

– попытка входа под чужим именем, паролем, многократная неудачная;

– попытка входа под чужим именем пользователя, паролем, удачная;

– несанкционированная очистка журналов аудита;

– несанкционированная установка (удаление) ПО ИСПДн;

– несанкционированное изменение конфигурации ПО ИСПДн;

– попытка получения прав администратора на локальном ПК (увеличения собственных прав, получение прав на отладку программ) удачная и неудачная;

– попытка получения прав администратора в домене или на удаленной машине удачная и неудачная;

– неумышленное заражение локального или сетевого ПК компьютерными вирусами;

– несанкционированное использование сканирующего ПО;

– несанкционированное использование анализаторов протоколов (снифферов);

– несанкционированный просмотр, вывод на печать и т.п. ПДн.

2.4 Нарушения III категории, к каковым относятся нарушения, не несущие признаков нарушений I и II категорий, а именно:

– попытка неудачного доступа к ПДн ИСПДн (периодическая);

– перевод времени на ПК;

– выполнение собственных производственных обязанностей на компьютере в неразрешенное время;

– перезагрузка компьютера, при сбоях в работе ПК, (однократная) в т.ч. аварийная перезагрузка, путем нажатия кнопки RESET;

– нецелевое использование корпоративных ресурсов (печать, Internet, mail, и т.п.).

## 3. Назначение служебного расследования

3.1 Служебное расследование назначается по нарушениям I и II категорий.

3.2 Разбором инцидентов информационной безопасности занимается комиссия по организации работ по защите ПДн (далее – Комиссия).

3.3 Служебное расследование может быть инициировано на основании следующей информации:

– сообщения сотрудников, клиентов Организации, направленные в Организацию в виде сообщений по электронной почте, служебных записок, писем, заявлений и т.д.;

– уведомления/сообщения органов осуществляющих контроль или надзор за деятельностью Организации;

– данные, полученные на основании анализа журналов СЗПДн.

3.4 При обнаружении нарушений I и/или II категорий работа с ПДн должна приостанавливаться, до устранения всех выявленных нарушений, их последствий.

## 4. Порядок регистрации инцидента информационной безопасности

4.1 При получении сообщения об инциденте информационной безопасности по электронной почте или по телефонному звонку, необходимо убедиться в достоверности полученной информации (например путем совершения «обратного» звонка по указанным в сообщении телефонам, проверки данных указанных в подписи сообщения или названных при звонке).

4.2 Сотрудник, получивший информацию об инциденте, должен сообщить об этом ответственному за обеспечение безопасности персональных данных. Ответственный за обеспечение безопасности персональных данных сообщает об инциденте ответственному за организацию обработки персональных данных и начальнику подразделения, в котором случился инцидент.

4.3 Все инциденты информационной безопасности должны регистрироваться в «Журнале учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств информационной системы ПДн» (Приложение 4 к Положению об обеспечении безопасности персональных данных в информационных системах

Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань»). Журнал должен постоянно актуализироваться.

## 5. Порядок разбора инцидента информационной безопасности

5.1 После сбора информации ответственным за обеспечение безопасности персональных данных, Комиссия анализирует все данные об обстоятельствах инцидента (электронные письма, логи информационных систем, показания сотрудников и др.).

5.2 Комиссия обязана установить, имела ли место утечка сведений, и обстоятельства ей сопутствующие, установить лица, виновные в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению.

5.3 По окончании разбора инцидента информационной безопасности Комиссией оформляется отчет, в котором указываются основные "контрольные точки" инцидента.

5.4 Отчет предоставляется руководителю организации. В конце отчета указывается причина возникновения инцидента и предложения по недопущению подобных инцидентов в будущем.

5.5 После окончания расследования Комиссия принимает решение о наказании виновных лиц и согласовывает решение с руководителем организации.

## 6. Права и обязанности

6.1 Члены комиссии имеют право в случае необходимости привлекать к работе:

- администраторов управления информатизации и телекоммуникаций;
- непосредственного начальника нарушителя;
- экспертов из других подразделений;
- привлеченных специалистов организаций-лицензиатов.

6.2 Требовать документального подтверждения факта нарушений информационной безопасности ПДн.

6.3 Устанавливать причины допущенных нарушений любым из способов, не противоречащим законодательству РФ.

6.4 Брать письменные объяснения по поводу выявленных нарушений у любого сотрудника.

6.5 Все отделы и сотрудники, работающие с ПДн обязаны:

- временно (на время проведения служебного расследования) приостановить свою деятельность по работе с ИСПДн;
- содействовать проведению служебного расследования.

## 7. Ответственность

7.1 Ответственность за выявление и классификацию инцидента информационной безопасности, требующего проведения процедуры служебного расследования несет ответственный за обеспечение безопасности ПДн.

7.2 Ответственность за назначение процедуры служебного расследования несет руководитель организации.

7.3 Ответственность за проведение процедуры служебного расследования несет комиссия по организации работ по защите ПДн.

7.4 Ответственность за надлежащее выполнение настоящей инструкции несет ответственный за обеспечение безопасности ПДн.

| **Лист ознакомления с «Положением об обеспечении безопасности персональных данных в информационных системах Муниципального бюджетного учреждения «Краеведческий музей городского округа Сызрань»»** | | |
|---|---|---|
| Занимаемая должность, дата ознакомления | Подпись | И. О. Фамилия |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |
| «___» _____ 20___ г. | | |

МБУ «Краеведческий музей г. о. Сызрань»
В данном документе прошито, пронумеровано и скреплено печатью 54 (пятьдесят четыре) листов

Директор Ова

04.08.2014г.
дата

Администрация городского округа Муниципальное бюджетное учреждение культуры «Краеведческий музей городского округа Сызрань» ИНН 6325048630 ОГРН 1086325002499