

**ПОЛОЖЕНИЕ**  
**по организации и проведению работ по обеспечению безопасности информации,**  
**обрабатываемой в информационных системах муниципального автономного учреждения**  
**«Дворец культуры «Родина»**

**1. Общие положения**

1.1. Настоящее Положение по организации и проведению работ по обеспечению безопасности информации, обрабатываемой в информационных системах муниципального автономного учреждения «Дворец культуры «Родина» (далее – Положение), разработано в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.2. Целью разработки настоящего Положения является определение порядка организации и проведения работ по обеспечению безопасности информации ограниченного доступа (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну (далее – информация), обрабатываемой в информационных системах (далее – ИС) Муниципального автономного учреждения «Дворец культуры «Родина» (далее – МАУ «Дворец культуры «Родина») на всех стадиях (этапах) создания ИС, в ходе ее эксплуатации и вывода из эксплуатации.

**2. Термины и определения**

2.1. В настоящем Положении используются следующие термины и их определения:

- **информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- **конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
- **оператор информационной системы** – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;
- **обработка информации** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение информации;
- **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- **технические средства информационной системы** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации, аппаратные средства защиты информации;
- **пользователь информационной системы** – лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования;

- **уничтожение информации** – действия, в результате которых становится невозможным восстановить содержание информации в информационной системе и (или) в результате которых уничтожаются материальные носители информации;
- **уровень защищенности персональных данных** – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах;
- **целостность информации** – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

### **3. Порядок организации и проведения работ по обеспечению безопасности информации**

3.1. Под организацией обеспечения безопасности информации, обрабатываемой в ИС МАУ «Дворец культуры «Родина», понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности защищаемой информации, реализуемых в рамках создаваемой системы защиты информации (далее – система ЗИ).

3.2. Система ЗИ включает в себя организационные и технические меры, определенные с учетом актуальных угроз безопасности информации, уровня защищенности информации (в том числе персональных данных), который необходимо обеспечить, класса информационной системы и информационных технологий, используемых в ИС.

3.3. Защита информации, содержащейся в ИС, обеспечивается путем выполнения требований к организации и мерам защиты информации, содержащейся в ИС.

3.4. Для обеспечения защиты информации, содержащейся в ИС, МАУ «Дворец культуры «Родина» назначается должностное лицо (работник), ответственное за защиту информации (далее – Ответственный), содержащейся в ИС.

3.5. Для обеспечения выполнения мер, предусмотренных законодательством Российской Федерации в области персональных данных, МАУ «Дворец культуры «Родина» назначается ответственный за организацию обработки персональных данных.

3.6. Для обеспечения соблюдения условий использования средств криптографической защиты информации (при их использовании) МАУ «Дворец культуры «Родина» назначается ответственный за эксплуатацию средств криптографической защиты информации в МАУ «Дворец культуры «Родина».

3.7. Для проведения работ по защите информации в ходе создания и эксплуатации ИС обладателем информации (заказчиком) и оператором в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».

3.8. Для обеспечения защиты информации, содержащейся в ИС, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии с Федеральным законом от 27.12.2002 № 184-ФЗ «О техническом регулировании».

3.9. Для обеспечения защиты информации, содержащейся в ИС, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии с Федеральным законом от 27.12.2002 № 184-ФЗ «О техническом регулировании».

3.10. Защита информации, содержащейся в ИС, является составной частью работ по созданию и эксплуатации ИС и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер

защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в ИС, в рамках системы (подсистемы) защиты ИС.

3.11. Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации ИС, в зависимости от информации, содержащейся в ИС, целей создания ИС и задач, решаемых этой ИС, должны быть направлены на исключение:

- неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);
- неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);
- неправомерного блокирования информации (обеспечение доступности информации).

3.12. Для обеспечения защиты информации, содержащейся в ИС, проводятся следующие мероприятия:

- формирование требований к защите информации, содержащейся в ИС;
- разработка системы защиты информации ИС;
- внедрение системы защиты информации ИС;
- оценка эффективности реализованных в рамках системы защиты информации мер по обеспечению безопасности информации (форма оценки эффективности и документов, разрабатываемых по результатам оценки эффективности, принимается МАУ «Дворец культуры «Родина» самостоятельно и (или) по соглашению с лицом, привлекаемым для проведения оценки эффективности реализованных мер по обеспечению безопасности информации) и ввод ее в действие;
- обеспечение защиты информации в ходе эксплуатации ИС;
- обеспечение защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации.

#### **4. Формирование требований к защите информации, содержащейся в информационных системах**

4.1. Формирование требований к защите информации, содержащейся в ИС, осуществляется МАУ «Дворец культуры «Родина».

4.2. Формирование требований к защите информации, содержащейся в ИС, включает:

- принятие решения о необходимости защиты информации, содержащейся в ИС;
- определение уровня защищенности персональных данных при их обработке в ИС и (или) классификацию ИС по требованиям защиты информации;
- определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в ИС, и разработку на их основе модели угроз безопасности информации;
- определение требований к системе ЗИ ИС.

4.3. При принятии решения о необходимости защиты информации, содержащейся в ИС, осуществляется:

- анализ целей создания ИС и задач, решаемых этой ИС;
- определение информации, подлежащей обработке в ИС;
- анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать ИС;
- принятие решения о необходимости создания системы ЗИ ИС, а также определение целей и задач защиты информации в ИС, основных этапов создания системы ЗИ ИС и функций по обеспечению защиты информации, содержащейся в ИС, оператора и уполномоченных лиц.

4.4. Результаты определения уровня защищенности персональных данных при их обработке в ИС оформляются актом. Результаты классификации ИС оформляются актом классификации.

4.5. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей ИС, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

4.6. Требования к системе ЗИ ИС определяются в зависимости от класса защищенности ИС и угроз безопасности информации, включенных в модель угроз безопасности информации.

## **5. Разработка системы защиты информации информационной системы**

5.1. Разработка системы ЗИ ИС организуется МАУ «Дворец культуры «Родина».

5.2. Разработка системы ЗИ ИС осуществляется в соответствии с техническим заданием на создание системы ЗИ ИС и включает:

- проектирование системы защиты информации ИС;
- разработку эксплуатационной документации на систему ЗИ ИС;
- макетирование и тестирование системы ЗИ ИС (при необходимости).

5.3. Система ЗИ ИС не должна препятствовать достижению целей создания ИС и ее функционированию.

5.4. При разработке системы ЗИ ИС учитывается ее информационное взаимодействие с иными ИС и информационно-телекоммуникационными сетями.

5.5. При проектировании системы ЗИ информационной системы:

– определяются типы субъектов доступа и объектов доступа, являющихся объектами защиты;

– определяются методы управления доступом, типы доступа и правила разграничения доступа субъектов доступа к объектам доступа, подлежащие реализации в ИС;

– выбираются меры защиты информации, подлежащие реализации в системе ЗИ ИС;

– определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;

– определяется структура системы ЗИ ИС, включая состав (количество) и места размещения ее элементов;

– осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности ИС;

– определяются требования к параметрам настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей ИС, приводящих к возникновению угроз безопасности информации;

– определяются меры защиты информации при информационном взаимодействии с иными ИС и информационно-телекоммуникационными сетями.

5.6. Результаты проектирования системы ЗИ ИС отражаются в проектной документации на систему ЗИ ИС.

5.7. Разработка эксплуатационной документации на систему ЗИ ИС осуществляется в соответствии с техническим заданием на создание системы ЗИ ИС.

5.8. При макетировании и тестировании системы ЗИ ИС в том числе осуществляются:

– проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами;

– проверка выполнения выбранными средствами защиты информации требований к системе защиты информации ИС;

– корректировка проектных решений, разработанных при создании ИС и (или) системы защиты информации ИС.

## **6. Внедрение системы защиты информации информационной системы**

6.1. Внедрение системы ЗИ ИС организуется МАУ «Дворец культуры «Родина».

6.2. Внедрение системы ЗИ ИС осуществляется в соответствии с проектной и эксплуатационной документацией на систему ЗИ ИС и в том числе включает:

- установку и настройку средств защиты информации в ИС;
- разработку документов, определяющих правила и процедуры, реализуемые МАУ «Дворец культуры «Родина» для обеспечения защиты информации в ИС в ходе ее эксплуатации;
- внедрение организационных мер защиты информации;
- предварительные испытания системы ЗИ ИС;
- опытную эксплуатацию системы ЗИ ИС;
- анализ уязвимостей ИС и принятие мер защиты информации по их устранению;
- приемочные испытания системы ЗИ ИС.

6.3. Установка и настройка средств защиты информации в ИС должна проводиться в соответствии с эксплуатационной документацией на систему ЗИ ИС и документацией на средства защиты информации.

6.4. Разрабатываемые организационно-распорядительные документы по защите информации должны определять правила и процедуры:

- управления (администрирования) системой ЗИ ИС;
- выявления инцидентов, которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению угроз безопасности информации, и реагирования на них;
- управления конфигурацией ИС и системы ЗИ ИС;
- контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС;
- защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации.

6.5. При внедрении организационных мер защиты информации осуществляются:

- реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения;
- проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и ответственных лиц по реализации организационных мер защиты информации;
- отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.

6.6. Предварительные испытания системы ЗИ ИС включают проверку работоспособности системы ЗИ ИС, а также принятие решения о возможности опытной эксплуатации системы защиты информации ИС.

6.7. Опытная эксплуатация системы ЗИ ИС включает проверку функционирования системы ЗИ ИС, в том числе реализованных мер ЗИ, а также готовность пользователей и ответственных лиц к эксплуатации системы ЗИ ИС.

6.8. Анализ уязвимостей ИС проводится в целях оценки возможности преодоления нарушителем системы ЗИ ИС и предотвращения реализации угроз безопасности информации. Анализ уязвимостей ИС включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения ИС.

6.9. Приемочные испытания системы ЗИ ИС включают проверку выполнения требований к системе ЗИ ИС в соответствии с техническим заданием на создание системы ЗИ ИС.

## **7. Оценка эффективности реализованных в рамках системы защиты информации мер по обеспечению безопасности информации**

7.1. Оценка эффективности реализованных в рамках системы защиты информации мер по обеспечению безопасности информации организуется МАУ «Дворец культуры «Родина» и включает проведение комплекса организационных и технических мероприятий, в результате которых подтверждается соответствие системы ЗИ ИС требованиям по безопасности информации.

7.2. Оценка эффективности реализованных в рамках системы защиты информации мер по обеспечению безопасности информации проводится МАУ «Дворец культуры «Родина» самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

7.3. По решению МАУ «Дворец культуры «Родина» оценка эффективности реализованных мер может быть проведена в рамках работ по аттестации информационной системы в соответствии с приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

7.4. В качестве исходных данных, необходимых для аттестации ИС, используются модель угроз безопасности информации, акт классификации ИС, техническое задание на создание системы ЗИ ИС, проектная и эксплуатационная документация на систему ЗИ ИС, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей ИС, материалы предварительных и приемочных испытаний системы ЗИ ИС. Аттестат соответствия выдается на весь срок эксплуатации ИС.

7.5. В ходе эксплуатации ИС МАУ «Дворец культуры «Родина» должен обеспечивать поддержку соответствия системы защиты информации аттестату соответствия в рамках реализации мероприятий по защите информации, предусмотренных п. 8 настоящего Положения.

## **8. Обеспечение защиты информации в ходе эксплуатации информационной системы**

8.1. Обеспечение защиты информации в ходе эксплуатации ИС осуществляется МАУ «Дворец культуры «Родина» в соответствии с эксплуатационной документацией на систему защиты информации и организационно-распорядительными документами по защите информации и в том числе включает следующие мероприятия:

- планирование мероприятий по защите информации;
- управление (администрирование) системой ЗИ ИС;
- выявление инцидентов и реагирование на них;
- управление конфигурацией ИС и ее системы ЗИ;
- контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в ИС.

8.2. В ходе управления (администрирования) системой ЗИ ИС осуществляются:

- заведение и удаление учетных записей пользователей, управление полномочиями пользователей ИС и поддержание правил разграничения доступа в ИС;
- управление средствами защиты информации в ИС, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты

информации, управление учетными записями пользователей, восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;

- установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации или по их поручению;

- централизованное управление системой защиты информации ИС (при необходимости);

- регистрация и анализ событий в ИС, связанных с защитой информации;

- информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации ИС и отдельных средств защиты информации, а также их обучение;

- сопровождение функционирования системы ЗИ ИС в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации.

8.3. В ходе выявления инцидентов и реагирования на них осуществляются:

- определение лиц, ответственных за выявление инцидентов и реагирование на них;

- обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

- своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИС пользователями и администраторами;

- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

- планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИС и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

- планирование и принятие мер по предотвращению повторного возникновения инцидентов.

8.4. В ходе управления конфигурацией ИС и ее системы защиты информации осуществляются:

- поддержание конфигурации ИС и ее системы защиты информации в соответствии с эксплуатационной документацией на систему защиты информации;

- определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию ИС и ее системы защиты информации;

- управление изменениями базовой конфигурации ИС и ее системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации ИС и ее системы защиты информации, санкционирование внесения изменений в базовую конфигурацию ИС и ее системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию ИС и ее системы защиты информации, сохранение данных об изменениях базовой конфигурации ИС и ее системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию ИС и ее системы защиты информации;

- анализ потенциального воздействия планируемых изменений в базовой конфигурации ИС и ее системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИС;

- определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических

средств и программного обеспечения до внесения изменений в базовую конфигурацию ИС и ее системы защиты информации;

- внесение информации (данных) об изменениях в базовой конфигурации ИС и ее системы защиты информации в эксплуатационную документацию на систему защиты информации ИС.

8.5. В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС, осуществляются:

- контроль за событиями безопасности и действиями пользователей в ИС;
- контроль (анализ) защищенности информации, содержащейся в ИС;
- анализ и оценка функционирования системы ЗИ ИС, включая выявление, анализ и устранение недостатков в функционировании системы ЗИ ИС;
- периодический анализ изменения угроз безопасности информации в ИС, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;
- документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС;
- принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) системы защиты информации ИС.

## **9. Обеспечение защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации**

9.1. Мероприятия по выводу ИС из эксплуатации включают:

- подготовку документов, связанных с выводом ИС из эксплуатации;
- работы по выводу ИС из эксплуатации, в том числе работы по деинсталляции программного обеспечения ИС, по реализации прав на программное обеспечение ИС, демонтажу и списанию технических средств ИС (при необходимости), обеспечению хранения и дальнейшего использования информационных ресурсов ИС;
- обеспечение защиты информации, в том числе архивирование информации, содержащейся в ИС, уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

9.2. Архивирование информации, содержащейся в ИС, должно осуществляться при необходимости дальнейшего использования информации в деятельности МАУ «Дворец культуры «Родина».

9.3. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю ИС или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

9.4. Обеспечение защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации осуществляется в соответствии с эксплуатационной документацией на систему ЗИ ИС и организационно-распорядительными документами по защите информации.

9.5. В ходе проведения контроля выполнения мероприятий по защите Информации при выводе из эксплуатации ИС МАУ «Дворец культуры «Родина» или после принятия решения об окончании обработки информации, проверяется документальное оформление процедур, предусмотренных организационно-распорядительными документами по защите информации, регламентирующими вышеуказанные мероприятия, а также соблюдение требований законодательства об архивном деле в Российской Федерации.



## ПЛАН мероприятий по защите информации в информационных системах Муниципальное автономное учреждение «Дворец культуры «Родина»

№ п/п	Наименование мероприятия по защите информации	Условия и периодичность проведения мероприятий по защите информации	Ответственные исполнители
1.	Анализ угроз безопасности информации в ИС в ходе их эксплуатации		
1.1.	Выявление, анализ и устранение уязвимостей ИС	Не реже одного раза в год	Уполномоченные сотрудники МАУ «Дворец культуры «Родина», ответственный за защиту информации, содержащейся в ИС МАУ «Дворец культуры «Родина» (далее – ответственный за защиту информации)
1.2.	Анализ изменения угроз безопасности информации в ИС	Не реже одного раза в год	
1.3.	Оценка возможных последствий реализации угроз безопасности информации в ИС	В случае выявления новых угроз безопасности	
2.	Управление (администрирование) системой ЗИ ИС		
2.1.	Управление учетными записями пользователей и поддержание в актуальном состоянии правил разграничения доступа в ИС	При необходимости в ходе эксплуатации ИС	Уполномоченные сотрудники МАУ «Дворец культуры «Родина»
2.2.	Управление средствами защиты информации ИС	При необходимости в ходе эксплуатации ИС	Уполномоченные сотрудники МАУ «Дворец культуры «Родина»
2.3.	Управление обновлениями программных и программно-аппаратных средств, в том числе средств ЗИ	По мере выхода обновлений, с учетом особенностей функционирования ИС	Уполномоченные сотрудники МАУ «Дворец культуры «Родина»
2.4.	Централизованное управление системой ЗИ ИС (при необходимости)	При необходимости в ходе эксплуатации ИС	Уполномоченные сотрудники МАУ «Дворец культуры «Родина»
2.5.	Мониторинг и анализ зарегистрированных событий в ИС, связанных с обеспечением безопасности информации	Постоянно в ходе эксплуатации ИС	Уполномоченный сотрудник МАУ «Дворец культуры «Родина»
2.6.	Обеспечение функционирования систем ЗИ ИС в ходе их эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по защите информации	Постоянно в ходе эксплуатации ИС	Ответственный за защиту информации
3.	Управления конфигурацией ИС и их системами ЗИ		
3.1.	Определение компонентов ИС и их систем ЗИ, подлежащих изменению в рамках управления конфигурацией (идентификация объектов управления конфигурацией): программно-аппаратные, программные средства, включая средства защиты информации, их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю	При создании системы ЗИ ИС, далее при необходимости в случае изменения состава объектов управления конфигурацией	МАУ «Дворец культуры «Родина»
3.2.	Управление изменениями ИС и их системами ЗИ: разработка параметров настройки, обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на обеспечение защиты информации, санкционирование	При создании системы ЗИ ИС и далее при необходимости в ходе эксплуатации ИС	Ответственный за защиту информации

№ п/п	Наименование мероприятия по защите информации	Условия и периодичность проведения мероприятий по защите информации	Ответственные исполнители
	внесения изменений в ИС и их систему защиты информации		
3.3.	Контроль и документирование действий по внесению изменений в ИС и их системы защиты информации	Не реже одного раза в 2 года	Ответственный за защиту информации
4.	Реагирование на инциденты		
4.1.	Обнаружение инцидентов (в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов)	Постоянно в ходе эксплуатации ИС	Сотрудники МАУ «Дворец культуры «Родина» (пользователи ИС и уполномоченные ответственные лица)
4.2.	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИС	Постоянно в ходе эксплуатации ИС	Сотрудники МАУ «Дворец культуры «Родина» (пользователи ИС и уполномоченные ответственные лица)
4.3.	Идентификация и анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	При возникновении инцидентов безопасности	Уполномоченные сотрудники МАУ «Дворец культуры «Родина», ответственный за защиту информации (в пределах своих полномочий в зависимости от характера инцидента)
4.4.	Планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИС и их сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов	При возникновении инцидентов безопасности	Уполномоченные ответственные лица МАУ «Дворец культуры «Родина» (в пределах своих полномочий в зависимости от характера инцидента)
4.5.	Планирование и принятие мер по предотвращению повторного возникновения инцидентов	При возникновении инцидентов безопасности	
5.	Информирование и обучение персонала ИС по вопросам защиты информации		
5.1.	Информирование персонала ИС о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации ИС	Не реже одного раза в 2 года	Ответственный за защиту информации
5.2.	Доведение до персонала ИС требований по защите информации, а также положений организационно-распорядительных документов по защите информации	Не реже одного раза в 2 года. В случае изменения нормативной правовой базы, локальных актов МАУ «Дворец культуры «Родина» в области защиты информации обучение сотрудников должно быть проведено не позднее одного месяца с момента изменений	Ответственный за организацию обработки персональных данных и ответственный за защиту информации (в пределах своих полномочий)
5.3.	Обучение персонала ИС правилам эксплуатации средств защиты информации от несанкционированного доступа и средств	При создании системы защиты информации ИС и далее при необходимости в	Уполномоченные сотрудники МАУ «Дворец культуры «Родина»

№ п/п	Наименование мероприятия по защите информации	Условия и периодичность проведения мероприятий по защите информации	Ответственные исполнители
	антивирусной защиты	ходе эксплуатации ИС	
5.4.	Проведение практических занятий и тренировок с персоналом ИС по блокированию угроз безопасности информации и реагированию на инциденты	Не реже одного раза в 2 года	Ответственный за защиту информации, уполномоченные сотрудники МАУ «Дворец культуры «Родина»
5.5.	Контроль осведомленности персонала ИС об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации	Не реже одного раза в 2 года	Ответственный за защиту информации
6.	Мероприятия по защите информации, проводимые в целях обеспечения и поддержания уровня защищенности информации, содержащейся в ИС		
6.1.	Установка обновлений программного обеспечения (ПО) (общесистемного, прикладного, программных СЗИ), в том числе проверка обновлений баз средств защиты информации (для средств антивирусной защиты и средств анализа защищенности)	В автоматическом режиме при выпуске производителем новой версии ПО либо вручную (при наличии обновлений) не реже одного раза в 3 месяца	Уполномоченные сотрудники МАУ «Дворец культуры «Родина» (в пределах своих полномочий)
6.2.	Обеспечение работоспособности, правильности функционирования и параметров настройки программного обеспечения и средств защиты информации	Постоянно в ходе эксплуатации ИС	Уполномоченные сотрудники МАУ «Дворец культуры «Родина» (в пределах своих полномочий)
6.3.	Контроль состава технических средств, программного обеспечения и средств защиты информации	Не реже одного раза в год	Ответственный за защиту информации
6.4.	Соблюдение установленных правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей	В процессе эксплуатации и после вывода из эксплуатации ИС	Уполномоченные сотрудники МАУ «Дворец культуры «Родина» (в пределах своих полномочий)
6.5.	Учет и сохранность технической и эксплуатационной документации на технические и программные средства, применяемые в ИС	В процессе эксплуатации и после вывода из эксплуатации ИС	Ответственный за защиту информации
6.6.	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки защищаемой информации	При необходимости в процессе эксплуатации и после вывода из эксплуатации ИС	Ответственный за организацию обработки персональных данных и ответственный за защиту информации
6.7.	Учет средств защиты информации, эксплуатационной и технической документации к ним (при необходимости)	В процессе эксплуатации и после вывода из эксплуатации ИС	Уполномоченные сотрудники МАУ «Дворец культуры «Родина», ответственный за защиту информации, ответственный за эксплуатацию средств криптографической защиты СКЗИ (в пределах своих полномочий)
6.8.	Учёт машинных носителей информации	При необходимости в процессе эксплуатации и после вывода из эксплуатации ИС	Ответственный за защиту информации
6.9.	Обеспечение безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по	Непрерывно в процессе эксплуатации ИС и при необходимости в случае возникновения нарушений в	Уполномоченные сотрудники МАУ «Дворец культуры «Родина» (в пределах своих

№ п/п	Наименование мероприятия по защите информации	Условия и периодичность проведения мероприятий по защите информации	Ответственные исполнители
	восстановлению отказавших средств и их тестирование	функционировании технических средств	полномочий)
6.10.	Поддержание работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий	Непрерывно в процессе эксплуатации ИС	Ответственный за защиту информации
6.11.	Проведение периодических проверок компонентов ИС на наличие вредоносных компьютерных программ (вирусов)	В автоматическом режиме в соответствии с установленным расписанием и вручную по требованию	Пользователи ИС, уполномоченные сотрудники МАУ «Дворец культуры «Родина» (в пределах своих полномочий)
6.12.	Проверка расположения средств отображения информации	Не реже одного раза в год	Ответственный за защиту информации
6.13.	Документирование процедур и результатов контроля за обеспечением уровня защищенности информации, содержащейся в ИС	По результатам проведения контроля за обеспечением уровня защищенности информации, содержащейся в ИС	Ответственный за защиту информации
6.14.	Принятие решения о необходимости доработки (модернизации) системы защиты информации		МАУ «Дворец культуры «Родина»
7.	Обеспечение защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации		
7.1.	Архивирование информации, содержащейся в ИС	При необходимости дальнейшего использования информации в деятельности ГБУ НСО «ЦЗИ НСО»	Ответственный за защиту информации, уполномоченные сотрудники МАУ «Дворец культуры «Родина» (в пределах своих полномочий)
7.2.	Уничтожение (стирание) данных и остаточной информации с машинных носителей информации	При необходимости передачи машинного носителя информации другому пользователю ИС или в сторонние организации	Ответственный за защиту информации
7.3.	Физическое уничтожение машинных носителей остаточной информации	При выводе из эксплуатации машинных носителей информации	Ответственный за защиту информации