Приложение №1
Утверждено приказом
БУ «Музыкальный
театр Республики Карелия»
№61 от «18» марта 2026г.

ПОЛИТИКА ЗАЩИТЫ ИНФОРМАЦИИ В БЮДЖЕТНОМ УЧРЕЖДЕНИИ «МУЗЫКАЛЬНЫЙ ТЕАТР РЕСПУБЛИКИ КАРЕЛИЯ»

1. Общие положения

1.1. Настоящая Политика защиты информации (далее – Политика) определяет систему организационных и технических мер по защите информации, обрабатываемой в информационных системах и информационно-телекоммуникационной инфраструктуре Бюджетного учреждения «Музыкальный театр Республики Карелия» (далее – Оператор, Учреждение).

1.2. Основной задачей в области защиты информации Учреждение признает совершенствование мер и средств обеспечения оптимального уровня информационной безопасности и защиты информации, обрабатываемой информационными системами в инфраструктуре Учреждения, в соответствии с требованиями действующего законодательства Российской Федерации, нормативных, методических и организационно-распорядительных документов уполномоченных органов.

1.3. Политика разработана в соответствии с положениями:

- Конституции Российской Федерации;
- Гражданского кодекса Российской Федерации;
- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федерального закона от 6 декабря 2011 года № 402-ФЗ «О бухгалтерском учете»;
- Закона Российской Федерации от 9 октября 1992 года № 3612-I «Основы законодательства Российской Федерации о культуре»;
- Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказа ФСТЭК России от 11.04.2025 № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (далее – Приказ ФСТЭК № 117);
- Политики Учреждения в отношении обработки персональных данных, утверждённой в установленном порядке;
- Перечня лиц, имеющих доступ к персональным данным, утверждённого в установленном порядке;
- Устава Учреждения;
- Положения о порядке приобретения и возврата театральных билетов Учреждения;

• Иных нормативных правовых актов и локальных актов Учреждения.

1.4. Политика определяет цели, задачи, принципы, структуру и способы защиты информации, собираемой, принимаемой, обрабатываемой, хранимой и передаваемой информационными системами Учреждения.

1.5. Основной **целью** обеспечения защиты информации является защита прав субъектов информационных отношений (работников, посетителей (зрителей), партнеров, самого Учреждения) от возможного нанесения им ущерба посредством случайного или преднамеренного воздействия на информацию. Обеспечение защиты информации направлено на предотвращение следующих негативных последствий:

• нарушение конфиденциальности информации ограниченного доступа;

• нарушение функционирования информационных систем, обеспечивающих основную (театрально-зрелищную), финансовую и административную деятельность;

• материальный ущерб Учреждению и третьим лицам;

• нарушение целостности и доступности информации, необходимой для деятельности Учреждения;

• предотвращение реализации угроз безопасности информации.

1.6. Обеспечение защиты информации осуществляется в соответствии со следующими основными **принципами**:

• **Законности:** соблюдение действующего законодательства РФ.

• **Системности:** учет всех актуальных угроз при создании системы защиты.

• **Комплексности:** согласованное применение организационных и технических мер, эшелонированная защита.

• **Своевременности:** разработка системы защиты параллельно с развитием информационных систем.

• **Преемственности и непрерывности:** постоянное совершенствование мер защиты.

• **Достаточности:** соответствие уровня затрат на защиту ценности информации.

• **Ответственности:** персональная ответственность каждого работника за свои действия.

• **Минимизации привилегий:** предоставление пользователям прав, минимально достаточных для выполнения обязанностей.

• **Адаптивности:** возможность изменения требований защиты информации при изменении структуры информационных систем Учреждения (включая возможное создание ИСПДн в будущем).

1.7. В целях обеспечения защиты информации Учреждение при взаимодействии с контрагентами (подрядчиками, партнерами, волонтерами) должно выполнять мероприятия по заключению соглашений о неразглашении и контролю их действий.

1.8. Политика размещается на официальном сайте Учреждения https://mrteatr.ru/about/dokumenty/ и доступна для ознакомления всем заинтересованным лицам.

1.9. Основные понятия, используемые в Политике, соответствуют терминам, определенным в Федеральном законе № 152-ФЗ «О персональных данных» и Политике Учреждения в отношении обработки персональных данных, с учетом особенностей, установленных разделом 15 настоящей Политики.

2. Информационные системы Учреждения и субъекты информационных отношений

2.1. К **субъектам** правоотношений, связанных с использованием информационных систем Учреждения и обеспечением защиты информации, относятся:

• Учреждение как обладатель информации (оператор персональных данных);

• работники Учреждения как пользователи информационных систем в соответствии с должностными обязанностями;

• работники подрядных организаций, обеспечивающих эксплуатацию средств вычислительной техники, сетевой инфраструктуры и информационных систем Учреждения;

• иные пользователи (посетители (зрители), физические и юридические лица), информация о которых обрабатывается в информационных системах Учреждения.

2.2. **Объектами** информационных отношений являются:

• информационные технологии и информационные ресурсы Учреждения, включая:

— бухгалтерскую систему «1С Бухгалтерия»;

— билетно-информационную систему «Яндекс Тикетс»;

— официальный сайт Учреждения;

— официальные группы в социальных сетях;

— автоматизированные рабочие места работников;

• процессы обработки информации в информационных системах Учреждения;

• информационная инфраструктура (локальная вычислительная сеть, каналы связи, серверное и сетевое оборудование);

• системы и средства защиты информации;

• объекты и помещения, в которых размещены средства обработки информации.

2.3. **Особые условия:** На момент утверждения настоящей Политики в Учреждении **отсутствуют информационные системы персональных данных (ИСПДн), введенные в эксплуатацию в установленном порядке**. Обработка персональных данных посетителей и работников осуществляется в соответствии с Политикой обработки персональных данных без создания специализированных ИСПДн, подлежащих регистрации в уполномоченных органах.

2.4. В случае принятия решения о создании и вводе в эксплуатацию ИСПДн требования настоящей Политики подлежат пересмотру и дополнению в соответствии с разделом 15.

2.5. Доступ работников Учреждения к информационным системам осуществляется в соответствии с выполняемыми должностными обязанностями на основе принципа минимальных привилегий. Перечень лиц, имеющих право доступа к информации ограниченного доступа, определен в Перечне, утвержденном в установленном порядке.

2.6. Работники подрядных организаций имеют доступ к оборудованию и системам Учреждения в соответствии с заключенными договорами и соглашениями о конфиденциальности (Обязательство о неразглашении).

2.7. Работники Учреждения (пользователи) **обязаны**:

• знать и соблюдать требования локальных актов по защите информации и работе с информацией ограниченного доступа;

• соблюдать правила работы в сети Интернет и использования съемных носителей;

• блокировать рабочую станцию при прекращении работы;

• не оставлять помещения с оргтехникой без присмотра;

• незамедлительно сообщать ответственному за организацию защиты информации о нарушениях, инцидентах, фактах утраты носителей или компрометации учетных данных.

2.8. Все работники под роспись знакомятся с нормативными документами по вопросам защиты информации и обработки информации ограниченного доступа.

3. Распределение ответственности за обеспечение защиты информации

3.1. Система управления защитой информации строится на принципах персональной ответственности и разграничения прав и обязанностей.

3.2. **Директор Учреждения:**

- несет персональную ответственность за обеспечение защиты информации;
- утверждает политики и документы в области защиты информации;
- выделяет необходимые ресурсы;
- назначает приказом **лицо, ответственное за организацию защиты информации**;
- принимает решения о применении мер ответственности к нарушителям.

3.3. **Лицо, ответственное за организацию защиты информации:**

- организует разработку и актуализацию документов по защите информации;
- организует классификацию информационных систем (при необходимости) и формирование моделей угроз;
- координирует внедрение и настройку средств защиты информации;
- осуществляет контроль за соблюдением требований;
- организует анализ уязвимостей и расследование инцидентов;
- обеспечивает взаимодействие с государственными органами (ФСТЭК России, ФСБ России, Роскомнадзор) по вопросам защиты информации в установленном порядке;
- обеспечивает наличие у сотрудников, привлекаемых к работам по защите информации, необходимой квалификации;
- **организует пересмотр документов и мер защиты информации в случае принятия решения о создании ИСПДн**.

3.4. **Сотрудники, обеспечивающие эксплуатацию информационных систем:**

- **Ведущий инженер-программист** – несет ответственность за техническую эксплуатацию систем, сетевого и серверного оборудования; реализует технические меры защиты информации по заданию ответственного за защиту информации; обеспечивает резервное копирование и контроль целостности; незамедлительно информирует ответственного за защиту информации об инцидентах.
- **Администраторы БИС** – несут ответственность за соблюдение требований защиты информации при работе в информационных системах в рамках своих должностных обязанностей, определенных в установленном порядке.

3.5. **Требования к квалификации сотрудников по защите информации (в соответствии с Приказом ФСТЭК № 117):**

- не менее 30 процентов работников, на которых возложены функции по обеспечению защиты информации, должны иметь высшее или среднее профессиональное образование в области информационной безопасности либо пройти профессиональную переподготовку в этой области.
- При отсутствии профильного образования у специалиста он должен быть направлен на переподготовку в течение первого года после назначения.

3.6. Все работники Учреждения несут ответственность за соблюдение требований по защите информации в части, их касающейся.

4. Требования к организации защиты информации, содержащейся в информационных системах Учреждения

4.1. В информационных системах Учреждения объектами защиты являются: информация, технические средства, программное обеспечение, средства защиты информации.

4.2. Для проведения работ по защите информации при необходимости могут привлекаться организации, имеющие лицензию на техническую защиту конфиденциальной информации.

4.3. Применяемые средства защиты информации должны быть сертифицированы ФСТЭК России или ФСБ России (в соответствующей части). **В случае отсутствия ИСПДн и информации, требующей применения сертифицированных средств**

защиты, допускается использование некриптографических методов защиты с последующим переходом на сертифицированные СЗИ при создании ИСПДн.

4.4. Защита информации обеспечивается на всех этапах создания и эксплуатации информационной системы. Организационные и технические меры должны быть направлены на обеспечение:

- **конфиденциальности** (защита от неправомерного доступа, копирования, распространения) – **для информации ограниченного доступа**;
- **целостности** (защита от неправомерного уничтожения или модифицирования) – **для всей значимой информации**;
- **доступности** (защита от неправомерного блокирования) – **для информации, критически важной для деятельности Учреждения**.

4.5. **Мероприятия по защите информации:**

- формирование требований к защите;
- разработка системы защиты информации;
- внедрение системы защиты информации;
- обеспечение защиты в ходе эксплуатации;
- обеспечение защиты при выводе из эксплуатации.

4.6. Формирование требований к защите включает:

- классификацию информационной системы (определение необходимого уровня защиты);
- определение угроз безопасности информации (при необходимости – разработку частной модели угроз);
- определение требований к системе защиты.

4.7. Классификация информационных систем проводится в случае обработки информации, отнесенной к категориям ограниченного доступа, или при создании ИСПДн.

4.8. Угрозы безопасности информации определяются по результатам оценки возможностей нарушителей, анализа уязвимостей и последствий. Определение актуальных угроз проводится **не реже одного раза в год** (в соответствии с Приказом ФСТЭК № 117).

5. Внедрение, эксплуатация и вывод из эксплуатации информационных систем

5.1. Внедрение системы защиты информации организуется ответственным за защиту информации и включает установку и настройку средств защиты, внедрение организационных мер, анализ уязвимостей и приемочные испытания.

5.2. Анализ уязвимостей проводится для оценки возможности преодоления системы защиты. При выявлении уязвимостей принимаются дополнительные меры защиты.

5.3. Обеспечение защиты в ходе эксплуатации включает:

- анализ угроз (не реже 1 раза в год);
- планирование мероприятий;
- управление (администрирование) системой защиты;
- **управление конфигурацией** информационной системы и ее системы защиты;
- информирование и обучение персонала;
- **реагирование на инциденты**;
- контроль за уровнем защищенности.

5.4. Управление изменениями конфигурации должно осуществляться регламентированно, с санкционированием и документированием всех изменений.

5.5. Реагирование на инциденты включает их обнаружение, анализ, информирование, планирование и принятие мер по устранению и предотвращению повторения.

5.6. Информирование и обучение персонала проводятся **не реже 1 раза в два года** (в соответствии с Приказом ФСТЭК № 117).

5.7. При выводе из эксплуатации системы осуществляется архивирование информации (при необходимости) и гарантированное уничтожение (стирание) данных или физическое уничтожение машинных носителей информации, содержащих сведения ограниченного доступа.

6. Требования к защите информации, содержащейся в информационной системе

6.1. Организационные и технические меры защиты информации должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа;
- управление доступом;
- ограничение программной среды (при необходимости);
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений (при необходимости);
- контроль (анализ) защищенности;
- целостность информационной системы и информации;
- доступность информации;
- защиту технических средств и систем связи.

6.2. **Идентификация и аутентификация:** В связи с отсутствием в Учреждении ИСПДн на текущем этапе применяется однофакторная парольная аутентификация. Требования к строгой (двухфакторной) аутентификации, предусмотренные Приказом ФСТЭК № 117, подлежат выполнению **при создании ИСПДн или при организации удаленного доступа к информационным системам, обрабатывающим информацию ограниченного доступа**.

6.3. Технические меры защиты информации реализуются посредством применения сертифицированных средств защиты информации **в случаях, установленных законодательством РФ**. При отсутствии соответствующих требований допускается применение иных средств защиты, обеспечивающих необходимый уровень безопасности.

7. Требования к программно-техническим средствам

Программно-технические средства информационных систем Учреждения должны:

- располагаться на территории Российской Федерации (для систем, обрабатывающих информацию ограниченного доступа);
- при необходимости использовать сертифицированные средства защиты информации;
- обеспечивать резервное копирование и восстановление информации;
- обеспечивать протоколирование и сохранение сведений о доступе и действиях с информацией (для критически важных систем);
- функционировать в бесперебойном режиме с учетом допустимых регламентных простоев.

8. Порядок взаимодействия информационных систем Учреждения с иными информационными системами

8.1. Взаимодействие с иными информационными системами (сайт «Госуслуги», порталы поставщиков билетов, сайт Учреждения, государственные информационные системы) осуществляется с соблюдением требований законодательства в области защиты информации.

8.2. Передача информации ограниченного доступа (в том числе персональных данных) осуществляется с использованием защищенных каналов связи и, при необходимости, сертифицированных средств криптографической защиты информации.

8.3. При взаимодействии должны обеспечиваться идентификация и аутентификация систем, подтверждение целостности передаваемой информации (при технической возможности).

8.4. В случае если сторонняя информационная система обрабатывает персональные данные, полученные от Учреждения, такая система должна соответствовать требованиям к защите персональных данных (проверяется при заключении договора).

8.5. При привлечении подрядных организаций для разработки программного обеспечения, требования к безопасной разработке включаются в техническое задание, а их работники не допускаются к разработке непосредственно в эксплуатируемых информационных системах.

9. Обеспечение защиты персональных данных

9.1. Защита, хранение, обработка и передача персональных данных осуществляются с соблюдением требований Федерального закона № 152-ФЗ, Постановления Правительства № 1119, Приказа ФСТЭК № 21 и Приказа ФСТЭК № 117.

9.2. **Особые условия:** В связи с отсутствием в Учреждении ИСПДн, введенных в эксплуатацию, обработка персональных данных осуществляется в рамках общесистемных мер защиты информации, предусмотренных настоящей Политикой, и в строгом соответствии с Политикой обработки персональных данных, утвержденной в установленном порядке.

9.3. Состав обрабатываемых персональных данных и порядок обработки определен в Политике Учреждения в отношении обработки персональных данных.

9.4. Все персональные сведения Учреждение получает преимущественно от самих субъектов (посетителей при покупке билетов). При получении от третьих лиц – уведомляет субъекта и получает его согласие.

9.5. Персональные данные являются конфиденциальной информацией.

9.6. Учреждение принимает организационные и технические меры по обеспечению безопасности персональных данных в соответствии с требованиями законодательства, в том числе:

- обеспечивает режим безопасности помещений, в которых размещены средства обработки информации;
- обеспечивает сохранность носителей информации;
- утверждает перечни работников, имеющих доступ к персональным данным;
- при необходимости использует средства защиты информации, прошедшие процедуру оценки соответствия.

9.7. Порядок действий при выявлении неправомерной обработки, неточных данных, достижении целей обработки или отзыве согласия регламентирован разделом 6 Политики обработки персональных данных и должен соответствовать установленным срокам (блокирование, уточнение, уничтожение).

10. Обеспечение организационно-распорядительной документацией

Для реализации требований настоящей Политики в Учреждении разрабатываются и утверждаются следующие внутренние документы:

• **Стандарты (правила) защиты информации**, определяющие требования к конфигурациям, программному обеспечению, дистанционной работе и др.;

• **Регламенты защиты информации**, устанавливающие порядок:

— создания, учета, изменения и блокирования учетных записей (включая привилегированные);
— предоставления удаленного доступа;
— допуска работников подрядных организаций к информационным системам;
— выявления, оценки и устранения уязвимостей;
— обработки и хранения информации ограниченного доступа;
— мониторинга информационной безопасности;
— восстановления штатного функционирования после сбоев;
— контроля уровня защищенности информации.

11. Мониторинг, отчетность и управление уязвимостями

11.1. В Учреждении организуется мониторинг информационной безопасности информационных систем, взаимодействующих с сетью «Интернет».

11.2. Проводится регулярная оценка состояния защиты информации на основе:

• **показателя защищенности** – не реже одного раза в шесть месяцев (для информационных систем, подлежащих оценке в соответствии с Приказом ФСТЭК № 117);

• **показателя уровня зрелости** – не реже одного раза в два года (для информационных систем, подлежащих оценке в соответствии с Приказом ФСТЭК № 117).

11.3. Результаты оценки направляются в территориальный орган ФСТЭК России не позднее 5 рабочих дней после их расчета **в случае, если такая обязанность установлена для информационных систем Учреждения**.

11.4. О выявленных новых уязвимостях, которые могут привести к нарушению безопасности информации, специалист по защите информации информирует ФСТЭК России в течение 5 рабочих дней с момента обнаружения **в случаях, предусмотренных законодательством**.

11.5. Установлены следующие сроки устранения выявленных уязвимостей:

• **критические уязвимости** – не более 24 часов с момента выявления;

• **уязвимости высокой степени опасности** – не более 7 календарных дней;

• **уязвимости средней и низкой степени опасности** – в сроки, установленные планом мероприятий, но не более 30 календарных дней.

12. Требования к удаленному доступу и использованию мобильных устройств

12.1. Удаленный доступ пользователей к информационным системам Учреждения для выполнения служебных обязанностей осуществляется:

• с использованием сетей связи, расположенных на территории Российской Федерации;

• с применением средств защиты каналов передачи данных (VPN и др.) при доступе к информации ограниченного доступа;

• с соблюдением требований аутентификации, установленных локальными актами.

12.2. Допускается использование личных мобильных устройств работников для доступа к информационным системам при соблюдении условий, установленных в локальных актах (наличие антивирусных средств, контроль со стороны Учреждения).

12.3. Беспроводные сети связи, используемые для доступа к информационным системам Учреждения, должны быть отделены от сетей, предназначенных для доступа в Интернет и общедоступной информации (гостевых сетей), **при наличии технической возможности**.

13. Аттестация и контроль защищенности информационных систем

13.1. Аттестация информационных систем (подтверждение соответствия требованиям защиты информации) проводится:

- для государственных информационных систем – в обязательном порядке;
- для иных информационных систем, обрабатывающих информацию ограниченного доступа, – по решению директора Учреждения.

13.2. Контроль уровня защищенности информации проводится не реже одного раза в три года или после компьютерного инцидента (для систем, подлежащих контролю).

13.3. Результаты контроля оформляются отчетом, который представляется директору Учреждения в течение 3 рабочих дней. В случае выявления нарушений информация направляется в ФСТЭК России в порядке, установленном законодательством.

14. Заключительные положения

14.1. Настоящая Политика вступает в силу с даты ее утверждения директором Учреждения.

14.2. Изменения и дополнения в настоящую Политику вносятся путем утверждения новой редакции Политики либо путем утверждения изменений и дополнений к ней.

14.3. Контроль за соблюдением требований настоящей Политики возлагается на лицо, ответственное за организацию защиты информации.

14.4. Вопросы, не урегулированные настоящей Политикой, регулируются действующим законодательством Российской Федерации и локальными нормативными актами Учреждения.

15. Особые условия. Порядок действий при создании информационных систем персональных данных (ИСПДн)

15.1. Настоящий раздел определяет порядок действий Учреждения в случае принятия решения о создании и вводе в эксплуатацию информационной системы персональных данных (ИСПДн).

15.2. Решение о создании ИСПДн оформляется приказом директора Учреждения с указанием:

- цели создания ИСПДн;
- категорий обрабатываемых персональных данных;
- перечня субъектов, чьи данные будут обрабатываться;
- сроков создания и ввода в эксплуатацию;
- ответственных лиц.

15.3. С момента принятия решения о создании ИСПДн ответственный за организацию защиты информации обязан:

15.3.1. В течение **10 рабочих дней** инициировать пересмотр настоящей Политики и иных локальных актов в части приведения их в соответствие с требованиями к защите ИСПДн.

15.3.2. Организовать проведение следующих мероприятий:

№	Мероприятие	Срок	Ответственный
1	Классификация ИСПДн (определение класса К1, К2 или К3)	До начала проектирования	Ответственный за ЗИ
2	Разработка частной модели угроз безопасности информации для ИСПДн	На этапе проектирования	Ответственный за ЗИ
3	Определение необходимых мер защиты информации (согласно Приказу ФСТЭК № 21)	На этапе проектирования	Ответственный за ЗИ
4	Внедрение строгой (двухфакторной) аутентификации для доступа к ИСПДн	До ввода в эксплуатацию	Ведущий инженер-программист
5	Усиление парольной политики (длина не менее 8 символов, срок действия 90 дней)	До ввода в эксплуатацию	Ведущий инженер-программист
6	Внедрение сертифицированных средств защиты информации (при необходимости)	До ввода в эксплуатацию	Ведущий инженер-программист
7	Проведение приемочных испытаний системы защиты ИСПДн	Перед вводом в эксплуатацию	Комиссия
8	Уведомление Роскомнадзора об обработке персональных данных (при необходимости)	В соответствии с законодательством	Ответственный за ЗИ

15.4. **Требования к усилению мер защиты при создании ИСПДн:**

Мера защиты	Текущий уровень	Требуемый уровень для ИСПДн
Длина пароля	6 символов	Не менее 8 символов
Срок действия пароля	180 дней	Не более 90 дней
Категории символов	2 из 4	3 из 4

Мера защиты	Текущий уровень	Требуемый уровень для ИСПДн
Аутентификация	Однофакторная	Строгая (двухфакторная) для привилегированных пользователей
Регистрация событий	Основные события	Расширенный перечень событий
Средства защиты	Некриптографические (возможно)	Сертифицированные СЗИ (при необходимости)

15.5. **Финансирование:** Расходы на создание системы защиты ИСПДн (приобретение сертифицированных средств защиты, привлечение специалистов, обучение персонала) предусматриваются при планировании бюджета на создание ИСПДн.

15.6. **Ответственность:** За несвоевременное выполнение мероприятий, предусмотренных настоящим разделом, ответственные лица несут дисциплинарную ответственность в соответствии с законодательством РФ.

15.7. Настоящий раздел вступает в силу с момента утверждения Политики и действует постоянно, обеспечивая готовность Учреждения к созданию ИСПДн в будущем.