Приложение №7
Утверждено приказом
БУ «Музыкальный
театр Республики Карелия»
№62 от «18» марта 2026г.

СТАНДАРТ БЕЗОПАСНОЙ КОНФИГУРАЦИИ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ (АРМ) И СЕРВЕРОВ

1. Общие положения

1.1. Настоящий Стандарт безопасной конфигурации автоматизированных рабочих мест и серверов (далее — Стандарт) разработан в соответствии с:

- Приказом 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»;
- Приказом 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»;
- ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» (в части управления конфигурацией);
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Политикой защиты информации БУ «Музыкальный театр Республики Карелия»;
- Стандартом идентификации и аутентификации БУ «Музыкальный театр Республики Карелия»;
- Стандартом антивирусной защиты БУ «Музыкальный театр Республики Карелия»;
- Стандартом управления доступом БУ «Музыкальный театр Республики Карелия».

1.2. **Цель Стандарта** — обеспечение защиты информации путем установления единых требований к безопасной настройке (конфигурации) автоматизированных рабочих мест и серверов, минимизация уязвимостей, предотвращение несанкционированного доступа и нарушения функционирования информационных систем Учреждения.

1.3. **Задачи Стандарта**:

- определение требований к установке и настройке операционных систем;
- установление правил управления учетными записями и привилегиями;
- регламентация требований к обновлению программного обеспечения;
- определение порядка контроля целостности и безопасной конфигурации;
- установление требований к защите от вредоносного ПО;
- распределение ответственности за поддержание безопасной конфигурации.

1.4. **Область действия**: настоящий Стандарт распространяется на:

- **автоматизированные рабочие места (АРМ)** работников Учреждения, включая АРМ администраторов БИС, бухгалтеров, специалистов осуществляющих работу с защищаемой информацией;
- **серверное оборудование** (при наличии), включая серверы баз данных, файловые серверы, серверы приложений;

• **системное и прикладное программное обеспечение**, установленное на указанных устройствах.

1.5. **Особые условия**: На момент утверждения настоящего Стандарта в Учреждении отсутствуют информационные системы персональных данных (ИСПДн), введенные в эксплуатацию. Требования к безопасной конфигурации устанавливаются с учетом текущего уровня рисков. В случае создания ИСПДн требования настоящего Стандарта подлежат пересмотру и усилению согласно разделу 9.

2. Термины и определения

Автоматизированное рабочее место (АРМ) — программно-технический комплекс, предназначенный для автоматизации деятельности определенного должностного лица.

Сервер — аппаратно-программный комплекс, выделенный для выполнения сервисных функций по запросам клиентов (рабочих станций).

Конфигурация — совокупность настроек программного и аппаратного обеспечения, определяющих его функционирование.

Безопасная конфигурация — конфигурация, при которой обеспечивается минимизация поверхности атаки, отключены неиспользуемые службы и сервисы, установлены необходимые параметры защиты.

Управление конфигурацией — процесс идентификации, учета, контроля и аудита изменений конфигурации программного обеспечения и технических средств.

Контроль целостности — проверка неизменности программного обеспечения и данных, обеспечивающая обнаружение фактов несанкционированной модификации.

Базовая линия безопасности (baseline) — минимально необходимый набор требований к конфигурации, обеспечивающий защиту информации.

Привилегированная учетная запись — учетная запись с правами администратора, позволяющая изменять конфигурацию системы, устанавливать ПО, управлять другими пользователями.

3. Классификация АРМ и серверов

3.1. В Учреждении устанавливается следующая классификация АРМ и серверов:

Категория	Тип	Описание	Примеры
Категория 1	АРМ с доступом к информации ограниченного доступа	Рабочие места, с которых осуществляется доступ к конфиденциальной информации, финансовым данным	АРМ бухгалтера, АРМ администратора БИС
Категория 2	АРМ общего назначения	Рабочие места, используемые для выполнения общих служебных задач без доступа к информации ограниченного доступа	АРМ специалистов, АРМ руководителей
Категория 3	Серверы приложений	Серверы, на которых функционируют прикладные информационные системы	Сервер «1С Бухгалтерия» (при наличии)

Категория	Тип	Описание	Примеры
Категория 4	Файловые серверы	Серверы для хранения служебной документации, файловых ресурсов	Файловый сервер (при наличии)

3.2. Для каждой категории устанавливаются соответствующие требования к безопасной конфигурации.

4. Требования к установке и настройке операционных систем

4.1. **Общие требования к установке ОС**:

Требование	Описание	Категории
Использование лицензионного ПО	Операционная система должна быть лицензионной, с действующей подпиской на обновления	Все
Минимальная установка	Установка только необходимых компонентов (минимальная конфигурация без избыточных служб)	Все
Разметка диска	Разделение диска на системный раздел и раздел данных (при возможности)	Категории 1, 3, 4
Установка последних обновлений	Перед вводом в эксплуатацию установка всех критических обновлений безопасности	Все

4.2. **Настройка параметров безопасности ОС**:

4.2.1. **Отключение неиспользуемых служб и сервисов**:

• должны быть отключены все службы, не необходимые для выполнения должностных обязанностей;

• перечень разрешенных служб определяется для каждой категории АРМ/сервера.

4.2.2. **Настройка сетевых экранов**:

• на всех АРМ и серверах должен быть включен межсетевой экран (брандмауэр);

• разрешен только минимально необходимый сетевой доступ (по принципу "запрещено все, что не разрешено явно").

4.2.3. **Параметры безопасности, устанавливаемые по умолчанию**:

Параметр	Значение	Обоснование
Автоматическое обновление	Включено (с уведомлением администратора)	Своевременное устранение уязвимостей
Блокировка экрана	Не более 15 минут неактивности	Предотвращение НСД
Пароль на экранную заставку	Установлен	Защита при отсутствии пользователя

Параметр	Значение	Обоснование
Учетные записи гостя	Отключены	Исключение анонимного доступа
Учетная запись администратора	Переименована	Затруднение подбора

5. Управление учетными записями и привилегиями

5.1. **Принцип минимальных привилегий**:

• пользователям предоставляются только те права, которые необходимы для выполнения должностных обязанностей;

• работа с правами администратора допускается только для выполнения задач администрирования.

5.2. **Требования к типам учетных записей**:

Тип учетной записи	Права	Использование
Пользовательская	Обычный пользователь (без прав администратора)	Повседневная работа
Административная	Полный доступ к управлению системой	Только для администрирования

5.3. **Настройка контроля учетных записей (UAC)**:

• на ОС Windows — UAC должен быть включен на уровне не ниже "Уведомлять только при попытках программ внести изменения в компьютер";

• на ОС Linux — использование sudo с ограниченным набором команд.

5.4. **Запрет на использование административных учетных записей для повседневной работы**:

• администраторы должны иметь две учетные записи: обычную и административную (для выполнения задач администрирования);

• вход с административной учетной записью осуществляется только по необходимости.

6. Управление обновлениями программного обеспечения

6.1. **Обновление операционных систем**:

Тип обновления	Периодичность	Ответственный
Критические обновления безопасности	В течение 24 часов после выхода	Ведущий инженер-программист
Обновления безопасности (некритические)	Еженедельно	Ведущий инженер-программист

Тип обновления	Периодичность	Ответственный
Прочие обновления	Ежемесячно (по результатам тестирования)	Ведущий инженер-программист

6.2. **Обновление прикладного программного обеспечения**:

• обновления для офисных пакетов, браузеров, профильных приложений устанавливаются по мере выхода;

• перед установкой обновлений рекомендуется тестирование на некритичных АРМ (при наличии возможности).

6.3. **Настройка автоматического обновления**:

• на всех АРМ должна быть настроена автоматическая загрузка обновлений;

• установка обновлений может выполняться автоматически или с подтверждением администратора.

6.4. **Контроль устаревшего ПО**:

• использование программного обеспечения, не поддерживаемого производителем (например, Windows 7, Windows 8), запрещено;

• при невозможности замены такого ПО (по техническим причинам) должны применяться дополнительные компенсирующие меры защиты.

7. Требования к безопасной конфигурации прикладного ПО

7.1. **Браузеры**:

Настройка	Рекомендуемое значение
Автозаполнение паролей	Отключено
Сохранение паролей	Отключено
Блокировка всплывающих окон	Включена
Защита от фишинга и вредоносных сайтов	Включена
Расширения	Только разрешенные администратором

7.2. **Почтовые клиенты**:

Настройка	Рекомендуемое значение
Автоматическое открытие вложений	Отключено
Блокировка внешних изображений	Включена (рекомендуется)
Область карантина	Включена

7.3. **Офисные приложения**:

Настройка	Рекомендуемое значение
Макросы	Отключены (или требование подтверждения)

Настройка	Рекомендуемое значение
Активные содержимые (ActiveX)	Отключены
Защищенный просмотр	Включен

7.4. **Специализированное ПО («1С Бухгалтерия», «Яндекс Тикетс»)**:

• конфигурация выполняется в соответствии с рекомендациями производителя;

• доступ к настройкам должен быть ограничен администраторами соответствующих систем.

8. Контроль целостности и аудит конфигурации

8.1. **Контроль целостности программного обеспечения** должен обеспечивать обнаружение изменений в:

• системных файлах операционной системы;

• исполняемых модулях прикладного ПО;

• конфигурационных файлах средств защиты информации.

8.2. **Периодичность контроля**:

Тип контроля	Периодичность	Ответственный
Плановый контроль целостности	Ежемесячно	Ведущий инженер-программист
Внеплановый контроль	После инцидентов, подозрений на компрометацию	Ведущий инженер-программист

8.3. **Аудит изменений конфигурации**:

• все изменения конфигурации АРМ и серверов должны регистрироваться;

• ведется **Журнал учета изменений конфигурации** (Приложение № 2);

• изменения должны быть санкционированы ответственным лицом.

8.4. **Инвентаризация программного обеспечения**:

• не реже одного раза в год проводится инвентаризация установленного ПО;

• выявляется нелицензионное и неразрешенное ПО;

• результаты инвентаризации оформляются актом.

9. Требования к защите серверов

9.1. **Физическая защита серверов**:

• серверы должны размещаться в помещениях с ограниченным доступом (серверная);

• доступ в серверную разрешен только уполномоченным лицам.

9.2. **Сетевая безопасность серверов**:

• серверы должны быть изолированы от пользовательских АРМ средствами межсетевого экранирования;

• доступ к серверам разрешен только по необходимым протоколам и портам;

• удаленное администрирование серверов — только по защищенным протоколам (SSH, RDP через VPN).

9.3. **Специфические настройки серверов**:

Параметр	Значение
Автоматический вход в систему	Запрещен
Энергосбережение (переход в сон/гибернацию)	Отключено
Неиспользуемые службы	Отключены
Журналирование	Расширенное (входы, изменения, ошибки)

9.4. **При использовании виртуализации** (при наличии):

• гипервизор должен быть настроен в соответствии с рекомендациями производителя по безопасности;

• виртуальные машины должны быть изолированы друг от друга.

10. Порядок действий при создании ИСПДн

10.1. В случае принятия решения о создании информационной системы персональных данных (ИСПДн) ответственный за организацию защиты информации обязан:

10.1.1. В течение **10 рабочих дней** инициировать пересмотр настоящего Стандарта в части усиления требований к безопасной конфигурации.

10.1.2. Обеспечить выполнение следующих дополнительных требований:

Требование	Текущий уровень	Требуемый уровень для ИСПДн
Сертифицированные средства защиты	Не обязательны	Обязательны (Secret Net Studio, Dallas Lock и др.)
Контроль целостности	Базовый	Расширенный (с использованием СЗИ)
Защита от НСД	Встроенные средства	Сертифицированные средства
Доверенная загрузка	Не требуется	Требуется (для К1, К2)
Аудит событий	Основные события	Расширенный перечень
Управление обновлениями	Ручное/полуавтоматическое	Централизованное

10.2. Рекомендуемые сертифицированные средства защиты для ИСПДн:

Средство защиты	Назначение
Secret Net Studio	Защита от НСД для Windows, контроль целостности, антивирус

Средство защиты	Назначение
Secret Net LSP	Защита от НСД для Linux
Dallas Lock	Доверенная загрузка, защита от НСД
Kaspersky Endpoint Security	Антивирусная защита

11. Обязанности и ответственность

11.1. **Распределение ответственности**:

Роль	Ответственность
Ведущий инженер-программист	Техническая реализация безопасной конфигурации АРМ и серверов, установка обновлений, контроль целостности, ведение журналов
Администраторы БИС	Соблюдение требований при работе на АРМ, своевременное информирование о проблемах
Бухгалтеры	Соблюдение требований при работе на АРМ, своевременное информирование о проблемах
Ответственный за защиту информации	Общий контроль соблюдения Стандарта, санкционирование изменений

11.2. **Обязанности пользователей АРМ**:

- не вносить изменения в конфигурацию АРМ (не устанавливать ПО, не изменять настройки);
- не отключать средства защиты (антивирус, брандмауэр);
- блокировать экран при прекращении работы;
- незамедлительно сообщать о любых сбоях, подозрительных явлениях;
- не подключать личные устройства без разрешения.

11.3. **Ответственность**:

Нарушение	Ответственность
Самостоятельное изменение конфигурации АРМ	Дисциплинарная
Установка неразрешенного ПО	Дисциплинарная
Отключение средств защиты	Дисциплинарная
Несообщение о сбоях и инцидентах	Дисциплинарная

12. Заключительные положения

12.1. Настоящий Стандарт вступает в силу с даты его утверждения директором Учреждения.

12.2. Изменения и дополнения в настоящий Стандарт вносятся путем утверждения новой редакции либо путем утверждения изменений к нему.

12.3. С настоящим Стандартом должны быть ознакомлены под подпись все работники, использующие АРМ в служебной деятельности.

12.4. Контроль за соблюдением требований настоящего Стандарта возлагается на лицо, ответственное за организацию защиты информации.

ПРИЛОЖЕНИЕ № 1
к Стандарту безопасной конфигурации АРМ и серверов

ЧЕК-ЛИСТ ПРОВЕРКИ БЕЗОПАСНОЙ КОНФИГУРАЦИИ АРМ

АРМ: _____ (инв. номер / сетевое имя)
Пользователь: _____
Дата проверки: «» _____ *20* г.
Проверяющий: _____

№	Параметр проверки	Требование	Соответствие (Да/Нет/Н/П)	Примечание
1. Операционная система				
1.1	Версия ОС	Поддерживаемая производителем		
1.2	Установлены последние обновления безопасности	Проверить дату последних обновлений		
1.3	Неиспользуемые службы отключены	Проверить список служб		
1.4	Брандмауэр включен	Включен, настроены правила		
2. Учетные записи				

№	Параметр проверки	Требование	Соответствие (Да/Нет/Н/П)	Примечание
2.1	Пользователь работает с правами обычного пользователя	Не администратор		
2.2	Гостевая учетная запись отключена	Отключена		
2.3	Административная учетная запись переименована	Не "Administrator"		
3. Политика безопасности				
3.1	Блокировка экрана при неактивности	Не более 15 минут		
3.2	Экранная заставка с паролем	Установлена		
3.3	UAC включен	Не ниже среднего уровня		
4. Антивирусная защита				
4.1	Антивирус установлен	Да		
4.2	Антивирусные базы обновлены	Не старше 3 дней		
4.3	Антивирусный монитор включен	Активен		
5. Программное				

№	Параметр проверки	Требование	Соответствие (Да/Нет/Н/П)	Примечание
обеспечение				
5.1	Отсутствует неразрешенное ПО	Проверить список программ		
5.2	Браузеры настроены безопасно	Согласно разделу 7		
5.3	Макросы в офисных приложениях отключены	Отключены		
6. Прочее				
6.1	Съемные носители контролируются	Проверить политику		
6.2	Пользователь ознакомлен с требованиями	Под подпись		

Заключение:

- АРМ соответствует требованиям безопасной конфигурации
- АРМ требует донастройки (замечания: _____)

Подпись проверяющего: _____

ПРИЛОЖЕНИЕ № 2

к Стандарту безопасной конфигурации АРМ и серверов

ЖУРНАЛ УЧЕТА ИЗМЕНЕНИЙ КОНФИГУРАЦИИ АРМ И СЕРВЕРОВ

№ п/п	Дата изменения	Объект изменения (АРМ/сервер)	Описание изменения	Причина изменения	Инициатор	Ответственный	Согласование с ответственным за ЗИ	Отметка о результате
1								
2								
3								

ПРИЛОЖЕНИЕ № 3

к Стандарту безопасной конфигурации АРМ и серверов

ПАМЯТКА ПО БЕЗОПАСНОЙ РАБОТЕ НА АРМ

(для пользователей)

Уважаемый коллега!

Для обеспечения безопасности информации в Музыкальном театре соблюдайте следующие правила при работе на вашем рабочем компьютере:

ЗАПРЕЩАЕТСЯ:

1. **Изменять настройки** операционной системы, антивируса, брандмауэра.
2. **Устанавливать любое программное обеспечение** без разрешения ведущего инженера-программиста (игры, мессенджеры, неизвестные программы).
3. **Отключать или блокировать** антивирусную защиту.
4. **Передавать свой пароль** другим лицам, записывать его на стикерах, приклеенных к монитору.
5. **Оставлять рабочее место** с незаблокированным компьютером.
6. **Подключать личные флешки** без необходимости и без проверки антивирусом.

НЕОБХОДИМО:

1. **Блокировать экран** (Win+L — для Windows) при каждом уходе с рабочего места.
2. **Сообщать ведущему инженеру-программисту** о любых сбоях, замедлениях, подозрительных сообщениях.
3. **Использовать только разрешенное ПО** для выполнения служебных задач.
4. **Своевременно сохранять** рабочие файлы в сетевые папки (резервное копирование).
5. **Завершать сеанс работы** в конце рабочего дня (выключать или перезагружать компьютер).

ПРИ ПОДОЗРЕНИИ НА ЗАРАЖЕНИЕ:

- Немедленно прекратите работу.
- Сообщите ведущему инженеру-программисту.
- Не пытайтесь самостоятельно лечить компьютер.

Контакты:

- Ведущий инженер-программист: _____
-
- Ответственный за защиту информации: _____

С памяткой ознакомлен(а):

_____ / _____ /

«» _____ ***20*** г.

Приложение №6
Утверждено приказом
БУ «Музыкальный
театр Республики Карелия»
№62 от «18» марта 2026г.

СТАНДАРТ ЗАЩИТЫ МОБИЛЬНЫХ УСТРОЙСТВ И УДАЛЕННОГО ДОСТУПА

1. Общие положения

1.1. Настоящий Стандарт защиты мобильных устройств и удаленного доступа (далее — Стандарт) разработан в соответствии с:

- Приказом 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»;
- 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»;
- Политикой защиты информации БУ «Музыкальный театр Республики Карелия»;
- Политикой Учреждения в отношении обработки персональных данных, утверждённой в установленном порядке;
- Стандартом идентификации и аутентификации БУ «Музыкальный театр Республики Карелия»;
- Стандартом антивирусной защиты БУ «Музыкальный театр Республики Карелия».

1.2. **Цель Стандарта** — обеспечение защиты информации при использовании мобильных устройств (включая личные устройства сотрудников) и при организации удаленного доступа к информационным ресурсам Учреждения, предотвращение несанкционированного доступа к информации ограниченного доступа.

1.3. **Задачи Стандарта**:

- определение категорий устройств, допускаемых к использованию;
- установление требований к защите мобильных устройств;
- регламентация порядка организации удаленного доступа;
- определение требований к аутентификации при удаленном доступе;
- установление порядка использования личных устройств (BYOD);
- распределение ответственности за обеспечение защиты при удаленной работе.

1.4. **Область действия**: настоящий Стандарт распространяется на:

- **служебные мобильные устройства** (ноутбуки, планшеты, смартфоны), выданные Учреждением;
- **личные мобильные устройства сотрудников** (BYOD), используемые для доступа к информационным ресурсам Учреждения;
- **удаленный доступ** к информационным системам «1С Бухгалтерия», «Яндекс Тикетс», служебной документации, электронной почте;
- **беспроводные сети связи** (Wi-Fi), используемые для доступа к информационным системам.

1.5. **Особые условия**: На момент утверждения настоящего Стандарта в Учреждении отсутствуют информационные системы персональных данных (ИСПДн), введенные в эксплуатацию. Требования к удаленному доступу и мобильным устройствам

устанавливаются с учетом текущего уровня рисков. В случае создания ИСПДн требования настоящего Стандарта подлежат пересмотру и усилению согласно разделу 10.

2. Термины и определения

Мобильное устройство — портативное устройство, предназначенное для обработки, хранения и передачи информации (ноутбук, планшет, смартфон), имеющее возможность подключения к сетям связи.

Удаленный доступ — доступ к информационным ресурсам Учреждения, осуществляемый вне контролируемой зоны (вне помещений Учреждения) с использованием сетей связи общего пользования (включая сеть «Интернет»).

BYOD (Bring Your Own Device) — модель использования личных устройств сотрудников в служебных целях.

VPN (Virtual Private Network) — виртуальная частная сеть, обеспечивающая защищенное соединение между устройством и корпоративной сетью через сеть общего пользования.

Строгая аутентификация — аутентификация, реализуемая с использованием двух и более различных факторов (пароль + аппаратный токен/одноразовый пароль).

Контролируемая зона — пространство (территория, здание, помещение), в котором осуществляется контролируемое пребывание лиц и транспортных средств.

MDM (Mobile Device Management) — система управления мобильными устройствами, позволяющая централизованно настраивать параметры безопасности, контролировать соответствие требованиям и удаленно блокировать/очищать устройства.

3. Категории мобильных устройств и сценарии использования

3.1. В Учреждении устанавливаются следующие категории мобильных устройств:

Категория	Тип устройств	Статус	Допуск к информации
Категория 1	Служебные ноутбуки	Собственность Учреждения	Доступ к информации ограниченного доступа, служебной информации
Категория 2	Служебные планшеты/смартфоны	Собственность Учреждения	Доступ к служебной информации, корпоративной почте
Категория 3	Личные устройства (BYOD)	Собственность сотрудника	Ограниченный доступ (только к системам, не содержащим информацию ограниченного доступа)

3.2. **Сценарии использования**:

Сценарий	Описание	Допустимость
Работа в контролируемой зоне (в здании театра)	Использование стационарных АРМ и служебных ноутбуков в помещениях Учреждения	Разрешено
Работа вне контролируемой зоны	Доступ к информационным ресурсам из дома,	Ограниченно, по согласованию

Сценарий	Описание	Допустимость
(дистанционно)	командировок и т.п.	
Использование личных устройств для доступа к служебной информации	Подключение к корпоративной почте, просмотр документов	Ограниченно, при соблюдении требований раздела 7

4. Требования к служебным мобильным устройствам (ноутбуки)

4.1. Служебные ноутбуки, выдаваемые сотрудникам, должны соответствовать следующим требованиям:

Требование	Описание
Операционная система	Лицензионная, с актуальными обновлениями безопасности
Антивирусная защита	Установлено сертифицированное (при необходимости) антивирусное средство
Шифрование данных	Шифрование жесткого диска (BitLocker, VeraCrypt или аналоги)
Парольная защита	Блокировка экрана при бездействии (не более 15 минут)
Учетная запись	Только локальная учетная запись с правами пользователя (не администратора)
Учет	Ноутбук закреплен за сотрудником приказом (распоряжением)

4.2. **Запрещается**:

- использование нелицензионного программного обеспечения;
- отключение средств антивирусной защиты;
- передача служебного ноутбука третьим лицам (членам семьи, знакомым);
- подключение к публичным незащищенным сетям Wi-Fi без использования VPN.

5. Требования к удаленному доступу

5.1. Удаленный доступ пользователей к информационным системам Учреждения для выполнения служебных обязанностей осуществляется с соблюдением следующих требований:

Требование	Обязательность	Примечание
Использование сетей связи, расположенных на территории Российской Федерации	Обязательно	Запрет на использование зарубежных VPN-сервисов
Применение средств защиты	Обязательно	Для доступа к информации

Требование	Обязательность	Примечание
каналов передачи данных (VPN)		ограниченного доступа
Строгая аутентификация пользователей	Обязательно	При создании ИСПДн или при доступе к критически важным системам
Фиксация фактов удаленного доступа в журналах	Обязательно	Дата, время, идентификатор пользователя

5.2. **Организация VPN-подключения**:

5.2.1. Для организации удаленного доступа используется сертифицированное (при необходимости) средство VPN.

5.2.2. Настройка VPN осуществляется ведущим инженером-программистом только для сотрудников, имеющих обоснованную необходимость удаленного доступа.

5.2.3. VPN-подключение должно обеспечивать:

- шифрование всех передаваемых данных;
- аутентификацию пользователя перед установкой соединения;
- разграничение доступа к корпоративным ресурсам.

5.3. **Порядок предоставления удаленного доступа**:

Шаг	Действие	Ответственный
1	Сотрудник подает служебную записку с обоснованием необходимости удаленного доступа	Сотрудник / Руководитель
2	Согласование с ответственным за защиту информации	Ответственный за ЗИ
3	При положительном решении — настройка VPN-доступа	Ведущий инженер-программист
4	Инструктаж сотрудника по безопасной работе вне офиса	Ответственный за ЗИ
5	Периодический контроль активности удаленного доступа	Ведущий инженер-программист

5.4. **Удаленный доступ к ИСПДн** (при их создании):

- допускается только при наличии сертифицированных средств криптографической защиты информации (СКЗИ);
- применяется строгая (двухфакторная) аутентификация;
- доступ предоставляется только на время выполнения служебных обязанностей.

6. Требования к аутентификации при удаленном доступе

6.1. **Текущий уровень** (в отсутствие ИСПДн):

- допускается однофакторная аутентификация (логин/пароль) с усиленными требованиями к паролю:
  - длина не менее **10 символов**;

— использование всех четырех категорий символов (строчные, прописные, цифры, спецсимволы);
— срок действия пароля — **не более 90 дней.**

6.2. **При создании ИСПДн или доступе к критически важным системам**:

• применяется **строгая (двухфакторная) аутентификация** с использованием:
— аппаратных токенов (RuToken, JaCarta и аналоги);
— одноразовых паролей (OTP) через мобильное приложение;
— сертифицированных средств криптографической защиты информации.

6.3. **Регистрация попыток доступа**:

• все успешные и неуспешные попытки удаленного доступа подлежат регистрации в журналах;

• периодичность анализа журналов — не реже одного раза в месяц.

7. Использование личных мобильных устройств (BYOD)

7.1. **Общие принципы BYOD**:

• использование личных устройств для служебных целей допускается только в исключительных случаях при невозможности предоставления служебного устройства;

• решение о допуске личного устройства принимается ответственным за защиту информации на основании служебной записки.

7.2. **Требования к личным устройствам**:

Требование	Обязательность	Примечание
Наличие пароля (PIN-кода) блокировки экрана	Обязательно	Пароль не менее 6 символов (цифры/буквы)
Актуальная версия ОС	Обязательно	Поддержка обновлений безопасности производителем
Антивирусное ПО	Обязательно	Для Android-устройств — обязательно, для iOS — рекомендуется
Запрет на jailbreak/root	Обязательно	Устройство не должно иметь модифицированной ОС
Шифрование данных	Рекомендуется	Встроенные средства шифрования должны быть включены

7.3. **Ограничения при использовании BYOD**:

• на личных устройствах **не допускается** хранение информации ограниченного доступа (локальное копирование файлов, баз данных);

• доступ возможен только через веб-интерфейсы (без скачивания документов) или с использованием защищенных каналов;

• при утере устройства сотрудник обязан немедленно сообщить об этом ответственному за защиту информации для блокировки доступа.

7.4. **Запрещается** использование личных устройств для доступа к ИСПДн (при их создании).

8. Требования к беспроводным сетям связи (Wi-Fi)

8.1. 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).

8.2. **Требования к корпоративной Wi-Fi сети**:

Параметр	Значение
Тип защиты	WPA2/WPA3 Enterprise (с использованием RADIUS-сервера) или WPA2/WPA3 Personal со сложным ключом
Идентификация пользователей	По индивидуальным учетным записям
Шифрование трафика	Обязательно
Срок действия ключа	Не более 90 дней
Отделение от гостевой сети	Обязательно

8.3. **Гостевая Wi-Fi сеть**:

- предназначена только для доступа в Интернет;
- не имеет доступа к корпоративным ресурсам;
- ограничение скорости и времени сессии (рекомендуется).

8.4. **Запрещается**:

- использование нешифрованных открытых сетей Wi-Fi в помещениях Учреждения;
- подключение корпоративных устройств к публичным сетям Wi-Fi вне офиса без использования VPN.

9. Действия при утере или краже мобильного устройства

9.1. При утере или краже мобильного устройства (служебного или личного, используемого для доступа) сотрудник обязан:

Действие	Срок
Немедленно сообщить ответственному за защиту информации и ведущему инженеру-программисту	Немедленно (в течение 1 часа)
Сообщить об утере в правоохранительные органы (при краже)	В течение 24 часов
Предоставить всю известную информацию об устройстве (модель, IMEI, учетные записи)	При сообщении

9.2. **Действия ответственных лиц**:

Действие	Ответственный	Срок
Блокировка учетной записи пользователя во всех системах	Ведущий инженер-программист	Немедленно

Действие	Ответственный	Срок
Блокировка VPN-доступа	Ведущий инженер-программист	Немедленно
Смена паролей к системам, доступным с устройства	Ведущий инженер-программист	В течение 1 часа
Удаленная блокировка/очистка устройства (при наличии технической возможности)	Ведущий инженер-программист	В течение 1 часа
Фиксация инцидента в Журнале инцидентов	Ответственный за ЗИ	В течение 24 часов
Оценка рисков утечки информации	Ответственный за ЗИ	В течение 48 часов

9.3. При использовании личного устройства (BYOD) ответственность за сохранность устройства несет сотрудник, однако Учреждение принимает меры по блокировке доступа к своим ресурсам.

10. Порядок действий при создании ИСПДн

10.1. В случае принятия решения о создании информационной системы персональных данных (ИСПДн) ответственный за организацию защиты информации обязан:

10.1.1. В течение **10 рабочих дней** инициировать пересмотр настоящего Стандарта в части усиления требований к удаленному доступу и мобильным устройствам.

10.1.2. Обеспечить выполнение следующих дополнительных требований:

Требование	Текущий уровень	Требуемый уровень для ИСПДн
Аутентификация при удаленном доступе	Однофакторная (усиленная)	Строгая (двухфакторная)
Сертификация VPN-средств	Не обязательна	Обязательна (при обработке ПДн)
Использование личных устройств (BYOD)	Ограниченно	Запрещено для доступа к ИСПДн
MDM-управление служебными устройствами	Не применяется	Рекомендуется
Шифрование данных на мобильных устройствах	Рекомендуется	Обязательно
Контроль подключения к внешним сетям	Базовый	Усиленный контроль

10.2. Для ИСПДн классов К2 и К1 рекомендуется внедрение системы управления мобильными устройствами (MDM) для централизованного контроля соответствия устройств требованиям безопасности.

11. Обязанности и ответственность

11.1. **Обязанности сотрудников при удаленной работе и использовании мобильных устройств**:

- соблюдать требования настоящего Стандарта;
- обеспечивать сохранность служебных устройств;
- не передавать устройства третьим лицам;
- не оставлять устройства без присмотра в общественных местах;
- незамедлительно сообщать об утере, краже или компрометации;
- использовать только разрешенные каналы удаленного доступа (VPN);
- не подключаться к публичным незащищенным сетям Wi-Fi без VPN;
- не хранить информацию ограниченного доступа на личных устройствах;
- блокировать экран при прекращении работы.

11.2. **Ответственность**:

Нарушение	Ответственность
Утеря служебного устройства по халатности	Дисциплинарная, материальная (в соответствии с договором о полной материальной ответственности)
Несанкционированное подключение к информационным системам	Дисциплинарная, вплоть до увольнения
Разглашение информации ограниченного доступа	Дисциплинарная, административная (в соответствии с законодательством)
Несообщение об утере устройства	Дисциплинарная

11.3. Контроль соблюдения требований осуществляется ответственным за защиту информации путем:

- периодического анализа журналов удаленного доступа;
- выборочных проверок используемых устройств (при наличии технической возможности);
- инструктажей сотрудников.

12. Заключительные положения

12.1. Настоящий Стандарт вступает в силу с даты его утверждения директором Учреждения.

12.2. Изменения и дополнения в настоящий Стандарт вносятся путем утверждения новой редакции либо путем утверждения изменений к нему.

12.3. С настоящим Стандартом должны быть ознакомлены под подпись все работники, имеющие право удаленного доступа и/или использующие мобильные устройства в служебных целях.

12.4. Контроль за соблюдением требований настоящего Стандарта возлагается на лицо, ответственное за организацию защиты информации.

ПРИЛОЖЕНИЕ № 1

к Стандарту защиты мобильных устройств и удаленного доступа

ЗАЯВКА НА ПРЕДОСТАВЛЕНИЕ УДАЛЕННОГО ДОСТУПА

1. Сведения о сотруднике:

ФИО: _____

Должность: _____

Структурное подразделение: _____

2. Обоснование необходимости удаленного доступа:

_____

_____

3. Запрашиваемые ресурсы:

Информационная система	**Уровень доступа (чтение/запись)**	**Период доступа**
«1С Бухгалтерия»		
«Яндекс Тикетс»		
Служебная документация		
Корпоративная почта		

4. Используемое устройство:

- Служебный ноутбук (инв. № _____)
- Личное устройство (с соблюдением требований BYOD)

5. Согласование:

Руководитель структурного подразделения:

_____ / _____ / «» _____ ***20*** г.

Ответственный за защиту информации:

_____ / _____ / «» _____ ***20*** г.

6. Отметка о выполнении:

Доступ предоставлен: «» _____ ***20*** г.

Сотрудник проинструктирован: «» _____ ***20*** г.

Ответственный за настройку: _____ / _____ /

ПРИЛОЖЕНИЕ № 2

к Стандарту защиты мобильных устройств и удаленного доступа

ПАМЯТКА ПО БЕЗОПАСНОЙ РАБОТЕ ВНЕ ОФИСА

(для сотрудников, использующих удаленный доступ)

Уважаемый коллега!

При работе вне офиса (удаленно) соблюдайте следующие правила безопасности:

ДО РАБОТЫ:

• Убедитесь, что на вашем устройстве установлены все необходимые обновления и работает антивирус.

• Убедитесь, что включено шифрование диска (для ноутбуков).

• Запомните (запишите в надежном месте) контакты ответственных лиц для экстренной связи.

ВО ВРЕМЯ РАБОТЫ:

☑НЕОБХОДИМО:

• Подключаться к корпоративным ресурсам **ТОЛЬКО через VPN**.

• Использовать только защищенные сети Wi-Fi (с паролем). В публичных сетях (кафе, аэропорты) работать только через VPN.

• Блокировать экран при каждом отлучении (даже на минуту).

• Хранить служебные документы только в защищенных корпоративных папках (не скачивать на устройство без необходимости).

• Сообщать ответственному за защиту информации о любых подозрительных ситуациях.

⊖ЗАПРЕЩАЕТСЯ:

• Передавать служебное устройство членам семьи, друзьям, знакомым.

• Отключать антивирус или VPN.

• Подключаться к открытым (незащищенным) сетям Wi-Fi.

• Оставлять устройство без присмотра в общественных местах (кафе, транспорт, гостиница).

• Использовать простые пароли или записывать их на стикерах, приклеенных к устройству.

ПРИ УТЕРЕ УСТРОЙСТВА:

1. НЕМЕДЛЕННО (в течение 1 часа) сообщите ответственному за защиту информации и ведущему инженеру-программисту.
2. Сообщите об утере в полицию (при краже).
3. Не пытайтесь самостоятельно искать устройство, если это связано с риском.

Контакты:

• Ответственный за защиту информации: _____

• Ведущий инженер-программист: _____

С памяткой ознакомлен(а):

_____ / _____ /

«» _____ ***20*** г.

ПРИЛОЖЕНИЕ № 3

к Стандарту защиты мобильных устройств и удаленного доступа

ЖУРНАЛ УЧЕТА СЛУЖЕБНЫХ МОБИЛЬНЫХ УСТРОЙСТВ

№ п/п	Тип устройства	Модель	Инвентарный номер	Серийный номер	ФИО сотрудника	Должность	Дата выдачи	Дата возврата	Примечание
1	Ноутбук								
2	Ноутбук								
3									

ПРИЛОЖЕНИЕ № 4

к Стандарту защиты мобильных устройств и удаленного доступа

ЖУРНАЛ РЕГИСТРАЦИИ УДАЛЕННОГО ДОСТУПА

(для контроля ответственным лицом)

Дата	Время	ФИО сотрудника	Используемый IP-адрес	Тип устройства	Ресурс доступа	Длительность сессии	Примечания

Приложение №5
Утверждено приказом
БУ «Музыкальный
театр Республики Карелия»
№62 от «18» марта 2026г.

СТАНДАРТ БЕЗОПАСНОЙ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1. Общие положения

1.1. Настоящий Стандарт безопасной разработки программного обеспечения (далее — Стандарт) разработан в соответствии с:

- Приказом 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»;
- **ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»** (далее — ГОСТ Р 56939-2024);
- ГОСТ Р 58412 «Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения»;
- ГОСТ Р ИСО/МЭК 12207 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств»;
- Политикой защиты информации БУ «Музыкальный театр Республики Карелия»;
- Политикой Учреждения в отношении обработки персональных данных, утверждённой в установленном порядке;

1.2. **Цель Стандарта** — обеспечение безопасности информации на всех этапах жизненного цикла программного обеспечения, используемого в деятельности Учреждения, путем предотвращения появления, своевременного выявления и устранения недостатков, в том числе уязвимостей, в программном обеспечении.

1.3. **Задачи Стандарта**:

- определение требований к процессам разработки, доработки и модификации ПО;
- установление порядка взаимодействия с подрядными организациями-разработчиками;
- регламентация требований к анализу безопасности ПО (статическому, динамическому, композиционному);
- определение порядка управления уязвимостями в разрабатываемом ПО;
- распределение ответственности за обеспечение безопасности разработки.

1.4. **Область действия**: настоящий Стандарт распространяется на:

- **ситуации самостоятельной разработки ПО** (в случае, если Учреждение собственными силами разрабатывает программное обеспечение — например, силами ведущего инженера-программиста);
- **ситуации привлечения подрядных организаций** для разработки, доработки или модификации ПО (сайт, интеграции с внешними системами, мобильные приложения и т.п.);
- **процессы закупки готового ПО**, требующие оценки безопасности.

1.5. **Особые условия**: На момент утверждения настоящего Стандарта в Учреждении **отсутствует собственная команда разработки**. Основной акцент Стандарта

сделан на взаимодействие с подрядными организациями и контроль безопасности приобретаемого и разрабатываемого ПО. Требования настоящего Стандарта подлежат пересмотру при создании ИСПДн или организации собственной разработки.

2. Термины и определения

Безопасное программное обеспечение — программное обеспечение, разработанное в ходе реализации совокупности процессов (мер), направленных на предотвращение появления и устранение недостатков программы.

Уязвимость программы — недостаток программы, который может быть использован для реализации угроз безопасности информации.

Статический анализ исходного кода программы — вид работ по инструментальному исследованию программы, основанный на анализе исходных текстов программы с использованием специализированных инструментальных средств (статических анализаторов) в режиме, не предусматривающем исполнения кода.

Динамический анализ кода программы — вид работ по инструментальному исследованию программы, основанный на анализе кода программы в режиме непосредственного исполнения (функционирования) кода.

Композиционный анализ — анализ компонентного состава ПО для выявления уязвимостей в используемых сторонних библиотеках и компонентах с открытым исходным кодом.

Поверхность атаки — множество подпрограмм (функций, модулей) программного обеспечения, обрабатывающих данные, поступающие посредством интерфейсов, напрямую или косвенно подверженных риску атаки.

Сборочная среда — совокупность программных и аппаратных средств, служб связи, интерфейсов, форматов данных, протоколов, стандартов, обеспечивающих преобразование исходного кода программ в программные модули.

SBOM (Software Bill of Materials) — спецификация компонентного состава ПО, включающая информацию об используемых библиотеках, их версиях и лицензиях.

3. Ключевые принципы безопасной разработки

3.1. Учреждение при организации разработки (самостоятельной или с привлечением подрядчиков) руководствуется следующими принципами:

№	Принцип	Содержание
1	**Безопасность на ранних этапах (Shift Left)**	Меры безопасности внедряются на самых ранних этапах жизненного цикла разработки — этапах проектирования и разработки, а не после сдачи проекта
2	**Минимизация поверхности атаки**	При проектировании архитектуры ПО должны минимизироваться интерфейсы, доступные для внешнего воздействия
3	**Безопасность по умолчанию**	Безопасные настройки и конфигурации должны устанавливаться по умолчанию, не требуя от пользователя дополнительных действий
4	**Регулярное**	Своевременное устранение выявленных уязвимостей,

№	Принцип	Содержание
	обновление	обновление используемых компонентов
5	**Защита среды разработки**	Среда разработки, тестирования и сборки ПО должна быть защищена от несанкционированного доступа
6	**Прозрачность цепочки поставок**	Контроль происхождения и безопасности используемых сторонних компонентов

3.2. Указанные принципы должны быть отражены в технических заданиях на разработку ПО и договорах с подрядными организациями.

4. Требования при самостоятельной разработке ПО

4.1. В случае организации в Учреждении собственной разработки ПО (силами ведущего инженера-программиста или иных сотрудников) должны быть реализованы меры, предусмотренные разделами 4 и 5 ГОСТ Р 56939-2024.

4.2. **Основные процессы безопасной разработки согласно ГОСТ Р 56939-2024**:

№	Группа процессов	Входящие процессы
1	Планирование и управление требованиями	Определение требований безопасности, управление рисками, планирование процессов
2	Проектирование	**Моделирование угроз**, определение архитектуры безопасности, анализ поверхности атаки
3	Реализация (кодирование)	**Управление секретами**, стандарты кодирования, анализ кода
4	Анализ и тестирование	**Статический анализ (SAST), динамический анализ (DAST), композиционный анализ (SCA),** функциональное тестирование
5	Сборка и поставка	Безопасность сборочной среды, формирование **SBOM**, контроль целостности
6	Эксплуатация и сопровождение	Управление инцидентами, реагирование на уязвимости, обновление ПО

4.3. **Моделирование угроз** должно проводиться на этапе проектирования с использованием актуальных баз данных угроз (БДУ ФСТЭК России) и учетом специфики разрабатываемого ПО.

4.4. **Анализ защищенности кода**:

• статический анализ исходного кода должен проводиться с использованием специализированных инструментов (статических анализаторов);

• динамический анализ — в процессе тестирования функционирующего ПО;

• композиционный анализ — для выявления уязвимостей в сторонних библиотеках и компонентах.

4.5. **Документирование**:

• все этапы разработки должны документироваться;

• документация разработчика ПО включает программные и иные документы, предназначенные для организации и проведения работ по созданию ПО и подтверждения соответствия требованиям;

• должны фиксироваться результаты анализа, выявленные уязвимости и принятые меры.

5. Требования при привлечении подрядных организаций

5.1. В случае привлечения подрядных организаций для разработки, доработки или модификации ПО, Учреждение обязано включать требования по безопасной разработке в договоры и технические задания.

5.2. **Требования к подрядным организациям**:

№	Требование	Обоснование
1	Наличие опыта безопасной разработки	Подтверждается портфолио, референциями
2	Соблюдение требований ГОСТ Р 56939-2024 при разработке	Должно быть указано в договоре
3	Проведение статического и динамического анализа кода	Требование к процессу разработки
4	Предоставление результатов анализа безопасности	Отчеты о тестировании, анализе кода
5	Предоставление SBOM (спецификации компонентного состава)	Для контроля используемых библиотек
6	Гарантийные обязательства по устранению уязвимостей	На период эксплуатации

5.3. **Запрет на разработку в эксплуатируемых системах**:

• работники подрядных организаций **не допускаются к разработке (развитию) и (или) тестированию программного обеспечения непосредственно в эксплуатируемых информационных системах** Учреждения;

• разработка и тестирование должны проводиться в изолированной среде (стенде), не влияющей на продуктивную среду.

5.4. **Приемка результатов работ** должна включать:

• проверку полноты и качества разработанного ПО;

• анализ результатов тестирования безопасности;

• проверку наличия документации (включая описание архитектуры, инструкции);

• **проверку на отсутствие критических уязвимостей** (оценка защищенности).

5.5. При выявлении уязвимостей в процессе приемки они должны быть устранены подрядчиком до подписания акта приемки.

6. Требования к закупаемому готовому ПО

6.1. При приобретении готового программного обеспечения (лицензий, "коробочных" решений) Учреждение должно оценивать его безопасность.

6.2. **Критерии оценки безопасности закупаемого ПО**:

Критерий	Что проверяется
Происхождение ПО	Наличие сертификатов ФСТЭК/ФСБ (при необходимости), репутация производителя
Наличие документации	Руководство пользователя, руководство по администрированию, описание настроек безопасности
Обновляемость	Наличие механизмов обновления, политика поддержки производителя
Соответствие законодательству	Реестр отечественного ПО (при необходимости), лицензионная чистота

6.3. При наличии технической возможности рекомендуется проводить тестирование закупаемого ПО в изолированной среде перед вводом в эксплуатацию.

7. Управление уязвимостями в разрабатываемом ПО

7.1. **Выявление уязвимостей** осуществляется в ходе:

- статического анализа кода (при самостоятельной разработке);
- динамического анализа (тестирования);
- композиционного анализа сторонних компонентов;
- тестирования на проникновение (при необходимости);
- получения информации от производителей компонентов, поставщиков.

7.2. **Оценка уязвимостей** проводится по степени опасности:

- **критические** — позволяют осуществить несанкционированный доступ к информации или нарушить функционирование системы;
- **высокой степени опасности** — позволяют осуществить атаку при определенных условиях;
- **средней и низкой степени опасности** — ограниченное влияние на безопасность.

7.3. **Сроки устранения уязвимостей** (в соответствии с Политикой защиты информации):

Категория	Срок устранения
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

7.4. **Информирование ФСТЭК России**:

• о выявленных новых уязвимостях, которые могут привести к нарушению безопасности информации, Учреждение информирует ФСТЭК России в течение 5 рабочих дней с момента обнаружения.

8. Требования к среде разработки и инфраструктуре

8.1. Если разработка ведется собственными силами, среда разработки должна соответствовать следующим требованиям:

Требование	Описание
Защита от НСД	Доступ к среде разработки только для авторизованных лиц
Актуальное ПО	Использование лицензионного, своевременно обновляемого ПО
Антивирусная защита	Установка сертифицированных (при необходимости) антивирусных средств
Контроль версий	Использование систем контроля версий (git, svn)
Разделение сред	Разработка, тестирование, продуктивная среда разделены

8.2. **Сборочная среда**:

• должна быть защищена от несанкционированного доступа и модификации;

• процесс сборки должен быть автоматизирован и воспроизводим;

• используемые инструменты сборки должны быть проверены на отсутствие вредоносного кода.

8.3. **Управление секретами**:

• хранение паролей, ключей доступа, токенов аутентификации должно осуществляться в защищенных хранилищах (не в коде);

• запрещается размещение секретов в открытом виде в исходном коде, системах контроля версий, конфигурационных файлах.

9. Требования к сторонним компонентам и библиотекам

9.1. При разработке ПО (собственными силами или подрядчиками) должен осуществляться контроль используемых сторонних компонентов.

9.2. **Требования к сторонним компонентам**:

Требование	Описание
Легальность происхождения	Использование компонентов с открытыми лицензиями, разрешающими коммерческое использование
Актуальность версий	Использование поддерживаемых версий, не содержащих известных критических уязвимостей
Отсутствие известных уязвимостей	Проверка по базам уязвимостей (CVE, БДУ ФСТЭК)

Требование	Описание
Включение в SBOM	Фиксация всех используемых компонентов и их версий

9.3. **Композиционный анализ (SCA)** должен проводиться для выявления уязвимостей в сторонних компонентах.

9.4. При выявлении уязвимостей в сторонних компонентах должны приниматься меры:

- обновление до безопасной версии;
- замена компонента на альтернативный;
- применение компенсирующих мер защиты (при невозможности обновления).

10. Порядок взаимодействия с подрядчиками

10.1. **Этап выбора подрядчика**:

- оценка компетенций в области безопасной разработки;
- запрос референсов по аналогичным проектам.

10.2. **Этап заключения договора**:

- включение требований настоящего Стандарта в договор;
- включение обязанности соблюдать требования ГОСТ Р 56939-2024;
- определение порядка приемки работ (включая проверку безопасности);
- включение обязательства о неразглашении информации ограниченного доступа.

10.3. **Этап разработки**:

- контроль соблюдения требований (при необходимости — запрос промежуточных результатов);
- проведение регулярных совещаний по статусу работ.

10.4. **Этап приемки**:

- проверка полноты и качества разработанного ПО;
- анализ документации;
- проверка на отсутствие критических уязвимостей;
- подписание акта приемки.

10.5. **Постгарантийное обслуживание**:

- определение порядка устранения выявленных в процессе эксплуатации уязвимостей;
- сроки реакции на инциденты и уязвимости.

11. Особенности при создании ИСПДн

11.1. В случае принятия решения о создании информационной системы персональных данных (ИСПДн), требующей разработки или доработки ПО, ответственный за организацию защиты информации обязан:

11.1.1. Ужесточить требования к безопасной разработке в соответствии с классом ИСПДн.

11.1.2. Обеспечить выполнение следующих дополнительных требований:

Требование	Для ИСПДн класса К3	Для ИСПДн класса К2 и К1
Статический анализ кода	Рекомендуется	Обязателен

Требование	Для ИСПДн класса К3	Для ИСПДн класса К2 и К1
Динамический анализ кода	Рекомендуется	Обязателен
Композиционный анализ (SCA)	Рекомендуется	Обязателен
Тестирование на проникновение	Не требуется	Рекомендуется
Сертификация ПО	По необходимости	При наличии требований

11.2. В договоры с подрядчиками на разработку ПО для ИСПДн должны включаться повышенные требования к безопасности и ответственности за утечки данных.

12. Ответственность и контроль

12.1. **Распределение ответственности**:

Роль	Ответственность
Ответственный за организацию защиты информации	Общий контроль соблюдения Стандарта, согласование требований к разработке, приемка результатов
Ведущий инженер-программист	Техническая оценка разрабатываемого ПО, контроль требований при самостоятельной разработке
Руководители подразделений-заказчиков ПО	Формирование требований, участие в приемке

12.2. **Контроль соблюдения требований** осуществляется путем:

- анализа договоров и технических заданий;
- проверки наличия в договорах требований по безопасной разработке;
- оценки результатов приемочных испытаний.

12.3. Нарушение требований настоящего Стандарта (неисполнение подрядчиком обязательств по безопасности, закупка ПО без оценки рисков) влечет дисциплинарную ответственность виновных лиц.

13. Заключительные положения

13.1. Настоящий Стандарт вступает в силу с даты его утверждения директором Учреждения.

13.2. Изменения и дополнения в настоящий Стандарт вносятся путем утверждения новой редакции либо путем утверждения изменений к нему.

13.3. С настоящим Стандартом должны быть ознакомлены под подпись работники, участвующие в закупке, разработке и приемке программного обеспечения.

13.4. Контроль за соблюдением требований настоящего Стандарта возлагается на лицо, ответственное за организацию защиты информации.

ПРИЛОЖЕНИЕ № 1

к Стандарту безопасной разработки ПО

ЧЕК-ЛИСТ ДЛЯ ОЦЕНКИ ПОДРЯДНОЙ ОРГАНИЗАЦИИ-РАЗРАБОТЧИКА

№	Критерий	Оценка	Примечание
1	Наличие опыта разработки аналогичного ПО	Да / Нет / Частично	
2	Наличие опыта работы с государственными учреждениями	Да / Нет	
3	Готовность включить в договор требования по безопасной разработке	Да / Нет	
4	Наличие в штате специалистов по информационной безопасности	Да / Нет	
5	Использование инструментов статического анализа кода	Да / Нет	
6	Использование инструментов динамического анализа кода	Да / Нет	
7	Использование инструментов композиционного анализа (SCA)	Да / Нет	
8	Готовность предоставить SBOM (спецификацию компонентов)	Да / Нет	
9	Наличие политики управления уязвимостями	Да / Нет	
10	Готовность к тестированию на проникновение (пентестам)	Да / Нет	
11	Наличие положительных отзывов от заказчиков	Да / Нет	
12	Финансовая стабильность (отсутствие рисков банкротства)	Да / Нет	

Итоговая оценка: _____

Рекомендация: _____

Ответственный: _____ / _____ /

Дата: «» _____ ***20*** г.

ПРИЛОЖЕНИЕ № 2

к Стандарту безопасной разработки ПО

ТРЕБОВАНИЯ К ДОГОВОРУ С ПОДРЯДНОЙ ОРГАНИЗАЦИЕЙ

(рекомендуемые формулировки для включения в договор)

1. Требования к процессу разработки:

«Исполнитель обязуется осуществлять разработку программного обеспечения в соответствии с требованиями ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» в части, применимой к данному виду работ.»

2. Требования к анализу кода:

«Исполнитель обязуется проводить статический и динамический анализ разрабатываемого программного обеспечения с использованием специализированных инструментов, а также композиционный анализ используемых сторонних библиотек и компонентов. Результаты анализа предоставляются Заказчику.»

3. Требования к компонентному составу:

«Исполнитель обязуется предоставить Заказчику спецификацию компонентного состава разработанного программного обеспечения (SBOM — Software Bill of Materials), включающую информацию об используемых библиотеках, их версиях и лицензиях.»

4. Запрет на разработку в продуктивной среде:

«Исполнитель гарантирует, что разработка, доработка и тестирование программного обеспечения осуществляются в изолированной среде (стенде), не связанной с продуктивными информационными системами Заказчика. Доступ к продуктивным системам осуществляется исключительно для развертывания готового, протестированного ПО в порядке, согласованном с Заказчиком.»

5. Устранение уязвимостей:

«Исполнитель обязуется в течение гарантийного срока (____ месяцев) безвозмездно устранять выявленные в разработанном программном обеспечении уязвимости в следующие сроки:

- критические уязвимости — не более 24 часов;
- уязвимости высокой степени опасности — не более 7 календарных дней;
- уязвимости средней и низкой степени опасности — не более 30 календарных дней.»

6. Конфиденциальность:

«Исполнитель обязуется обеспечить конфиденциальность информации, ставшей известной в ходе разработки, включая исходный код, архитектурные решения, персональные данные (при их использовании в тестовых целях).»

ПРИЛОЖЕНИЕ № 3

к Стандарту безопасной разработки ПО

ПАМЯТКА ПО ПРИЕМКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

При приемке разработанного ПО необходимо проверить:

1. Документация:

- Руководство пользователя
- Руководство администратора (при наличии)
- Описание архитектуры
- Инструкция по развертыванию
- Спецификация компонентного состава (SBOM)

2. Результаты анализа безопасности:

- Отчет о статическом анализе кода (SAST)
- Отчет о динамическом анализе (DAST) / результатах тестирования
- Отчет о композиционном анализе (SCA)
- Информация об устраненных уязвимостях

3. Функциональное тестирование:

- Соответствие функциональным требованиям
- Корректность работы в штатном режиме
- Обработка ошибок и исключительных ситуаций

4. Соответствие требованиям безопасности:

- Отсутствие критических уязвимостей
- Безопасные настройки по умолчанию
- Корректная работа механизмов аутентификации и авторизации
- Защита каналов передачи данных (при необходимости)

5. Передача материалов:

- Исходный код (если предусмотрено договором)
- Исполняемые модули
- Установочный дистрибутив (при наличии)
- Информация о сторонних компонентах и лицензиях

Решение о приемке: _____

Ответственный за приемку: _____ / _____ /

Дата: «» _____ ***20*** г.

Приложение №4
Утверждено приказом
БУ «Музыкальный
театр Республики Карелия»
№62 от «18» марта 2026г.

СТАНДАРТ РЕЗЕРВНОГО КОПИРОВАНИЯ

1. Общие положения

1.1. Настоящий Стандарт резервного копирования (далее — Стандарт) разработан в соответствии с:

- Приказом 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»;
- 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»;
- Политикой защиты информации БУ «Музыкальный театр Республики Карелия»;
- Политикой Учреждения в отношении обработки персональных данных, утверждённой в установленном порядке;
- Перечнем лиц, имеющих доступ к персональным данным, утверждённым в установленном порядке;
- Стандартом антивирусной защиты БУ «Музыкальный театр Республики Карелия».

1.2. **Цель Стандарта** — обеспечение сохранности информации, возможности ее восстановления при сбоях, инцидентах или чрезвычайных ситуациях, а также обеспечение непрерывности деятельности Учреждения.

1.3. **Задачи Стандарта**:

- определение перечня информации, подлежащей резервному копированию;
- установление периодичности и типов резервного копирования;
- определение требований к хранению резервных копий;
- регламентация порядка восстановления информации из резервных копий;
- установление порядка тестирования работоспособности резервных копий;
- распределение ответственности за выполнение резервного копирования.

1.4. **Область действия**: настоящий Стандарт распространяется на:

- бухгалтерскую систему «1С Бухгалтерия» (базы данных);
- билетно-информационную систему «Яндекс Тикетс» (данные о продажах, отчетность);
- официальный сайт Учреждения (при наличии технической возможности);
- файловые ресурсы, содержащие служебную информацию ограниченного доступа;
- автоматизированные рабочие места (критически важные конфигурации).

1.5. **Особые условия**: На момент утверждения настоящего Стандарта в Учреждении отсутствуют информационные системы персональных данных (ИСПДн), введенные в эксплуатацию. Требования настоящего Стандарта учитывают текущий уровень и предусматривают возможность их усиления при создании ИСПДн в соответствии с разделом 9.

2. Термины и определения

Резервное копирование (резервирование) — процесс создания копии информации на носителе, предназначенном для восстановления информации в случае утраты или повреждения оригинала.

Резервная копия — копия информации, созданная в процессе резервного копирования.

Восстановление — процесс переноса информации с резервной копии на целевой носитель для обеспечения возможности ее использования.

Интервал времени восстановления (RTO — Recovery Time Objective) — целевое время, необходимое для восстановления функционирования информационной системы после инцидента .

Точка восстановления — момент времени, на который создана резервная копия и до которого может быть восстановлена информация.

Полное резервное копирование — создание копии всех выбранных данных независимо от наличия предыдущих копий.

Инкрементальное резервное копирование — создание копии только тех данных, которые изменились с момента последнего резервного копирования.

Дифференциальное резервное копирование — создание копии данных, изменившихся с момента последнего полного резервного копирования.

3. Перечень информации, подлежащей резервному копированию

3.1. Обязательному резервному копированию подлежат:

№	Информационный ресурс	Состав резервируемых данных	Критичность	Периодичность
1	База данных «1С Бухгалтерия»	Все данные бухгалтерского учета, конфигурации	Высокая	Ежедневно
2	Данные билетно-информационной системы «Яндекс Тикетс»	Отчеты о продажах, данные по возвратам, выгрузки	Средняя	Еженедельно
3	Официальный сайт Учреждения	Файлы сайта, база данных (при наличии)	Средняя	Еженедельно
4	Служебная документация	Приказы, договоры, отчеты (сетевые папки)	Высокая	Еженедельно
5	Конфигурации АРМ	Настройки рабочих мест, профили пользователей	Низкая	При изменении

3.2. При создании ИСПДн в перечень дополнительно включаются:
- базы данных персональных данных;
- специальное программное обеспечение ИСПДн;
- программное обеспечение средств защиты информации (САВЗ, СКЗИ);
- общее программное обеспечение (операционные системы, драйверы).

4. Периодичность и типы резервного копирования

4.1. Для различных категорий информации устанавливается следующая периодичность резервного копирования:

Категория информации	Тип копирования	Периодичность	Срок хранения
Критическая (базы 1С, приказы, договоры)	Полное	Ежедневно	30 дней
Важная (данные билетной системы, сайт)	Полное	Еженедельно	60 дней
Вспомогательная (конфигурации, настройки)	Полное	При изменении	До следующего изменения
Архивная (закрытые периоды, старые отчеты)	Полное	Ежемесячно	1 год

4.2. **Рекомендуемая схема ротации** (при технической возможности):
- ежедневные копии — хранятся 7 дней;
- еженедельные копии — хранятся 4 недели;
- ежемесячные копии — хранятся 12 месяцев.

4.3. **Создание резервных копий программных, программно-аппаратных средств и их конфигураций** должно обеспечивать возможность восстановления выполнения значимых функций в установленный интервал времени восстановления.

5. Требования к носителям и местам хранения резервных копий

5.1. Резервное копирование должно осуществляться на разные типы машинных носителей информации в местах, обеспечивающих исключение несанкционированного доступа к резервным копиям.

5.2. **Требования к носителям**:

Тип носителя	**Назначение**	**Требования**
Внешний жесткий диск (основной)	Ежедневное/еженедельное копирование	Объем не менее 1 ТБ, хранение в серверной/кабинете администратора
Внешний жесткий диск (резервный)	Дублирование критических данных	Хранение в сейфе у ответственного лица

Тип носителя	Назначение	Требования
Съемные носители (флеш-накопители)	Только для переноса небольших объемов	Не рекомендуется для постоянного хранения
Облачное хранилище	Дополнительное резервирование	Только с применением шифрования (при необходимости)

5.3. **Места хранения**:

• основное место хранения — помещение серверной или кабинет ведущего инженера-программиста (контролируемая зона);

• резервное место хранения (для критических данных) — сейф в кабинете ответственного за защиту информации или ином защищенном помещении;

• при наличии технической возможности рекомендуется хранение одной копии в другом здании (территориально распределенное хранение).

5.4. **Учет носителей**:

• все носители, содержащие резервные копии, подлежат обязательному учету в **Журнале учета носителей резервных копий** (Приложение № 1);

• носители должны быть промаркированы с указанием даты создания, типа информации и ответственного лица.

5.5. **Запрещается**:

• передача носителей с резервными копиями за пределы контролируемой зоны без согласования с ответственным за защиту информации;

• копирование информации с носителей резервных копий, за исключением случаев восстановления.

6. Порядок резервного копирования

6.1. **Ответственные лица**:

Информационный ресурс	Ответственный за резервирование	Действия
«1С Бухгалтерия»	Ведущий инженер-программист	Настройка автоматического резервирования, контроль
«Яндекс Тикетс»	Главный администратор БИС	Выгрузка отчетов, сохранение данных
Служебная документация	Ведущий инженер-программист	Настройка автоматического копирования сетевых папок
Конфигурации АРМ	Ведущий инженер-программист	Создание точек восстановления, образов системы

6.2. **Порядок выполнения резервного копирования баз данных «1С Бухгалтерия»**:

1. Проверка доступности носителя для резервного копирования.
2. Запуск процесса резервного копирования (автоматически по расписанию или вручную).

3. Контроль успешности завершения процесса (проверка логов, размера созданного файла).

4. Регистрация факта создания резервной копии в Журнале учета резервных копий.

6.3. **Порядок резервного копирования данных билетной системы**:

1. Формирование отчетов по продажам и возвратам за период.
2. Выгрузка отчетов в формате, допускающем восстановление (xlsx, csv, pdf).
3. Сохранение выгруженных файлов в сетевую папку, подлежащую резервированию.
4. Дополнительное копирование на внешний носитель (еженедельно).

6.4. **Автоматизация процессов**:

• для систем, поддерживающих автоматическое резервирование, должны быть настроены задания по расписанию;

• рекомендуется использование средств централизованного резервного копирования при наличии серверной инфраструктуры.

7. Порядок восстановления информации из резервных копий

7.1. **Основания для восстановления**:

• сбои программного или аппаратного обеспечения;

• случайное удаление или искажение данных;

• инцидент информационной безопасности (заражение вредоносным ПО, несанкционированный доступ);

• необходимость предоставления данных за прошедшие периоды.

7.2. **Порядок действий при необходимости восстановления**:

Шаг	Действие	Ответственный
1	Сообщить о инциденте (утрате данных) ведущему инженеру-программисту и ответственному за защиту информации	Пользователь, обнаруживший проблему
2	Зафиксировать факт инцидента в Журнале инцидентов	Ответственный за ЗИ
3	Определить причину возникновения неисправности и объем утраченных данных	Ведущий инженер-программист
4	Выбрать резервную копию для восстановления (наиболее актуальную)	Ведущий инженер-программист
5	Проверить целостность и пригодность резервной копии	Ведущий инженер-программист
6	Выполнить восстановление данных из резервной копии	Ведущий инженер-программист
7	Проверить полноту и корректность восстановленных данных	Пользователь / Ведущий инженер-программист
8	Зарегистрировать факт восстановления в Журнале	Ведущий инженер-

Шаг	Действие	Ответственный
	учета резервных копий (графа "вид резервирования" — "полное восстановление" либо "частичное восстановление")	программист

7.3. **Приоритет выбора резервной копии**:

1. Наиболее актуальная полная резервная копия.
2. Предыдущая полная резервная копия (при невозможности использования первой).
3. Еженедельная резервная копия.

7.4. **Восстановление персональных данных** (при создании ИСПДн):

• данные, созданные после последнего резервирования, восстанавливаются пользователями, осуществившими их внесение;

• факты восстановления фиксируются в Журнале резервирования.

8. Тестирование резервных копий и тренировки по восстановлению

8.1. **Периодическое тестирование** резервных копий на работоспособность должно проводиться **не реже одного раза в два года** в форме тренировок.

8.2. **Цели тестирования**:

• проверка возможности восстановления данных из резервных копий;

• оценка реального времени восстановления;

• проверка готовности ответственных лиц к действиям в нештатных ситуациях.

8.3. **Порядок проведения тренировки**:

1. Назначение ответственного за проведение тренировки.
2. Выбор одной из резервных копий для тестового восстановления.
3. Восстановление данных на тестовом оборудовании (при возможности).
4. Проверка целостности и полноты восстановленных данных.
5. Оценка фактического времени восстановления.
6. Составление акта о результатах тренировки (Приложение № 3).

8.4. При превышении интервалов времени восстановления должна обеспечиваться возможность выполнения пользователями значимых функций в неавтоматизированном режиме в соответствии с внутренними регламентами.

9. Порядок действий при создании ИСПДн

9.1. В случае принятия решения о создании информационной системы персональных данных (ИСПДн) ответственный за организацию защиты информации обязан:

9.1.1. В течение **10 рабочих дней** инициировать пересмотр настоящего Стандарта в части усиления требований к резервному копированию.

9.1.2. Обеспечить выполнение следующих дополнительных требований:

Требование	Текущий уровень	Требуемый уровень для ИСПДн
Периодичность копирования баз данных	Ежедневно	Ежедневно + журнал транзакций (при возможности)
Хранение резервных	Одно место	Два места (основное и резервное,

Требование	Текущий уровень	Требуемый уровень для ИСПДн
копий		территориально разделенные)
Учет носителей	Рекомендуется	Обязательный журнал учета
Шифрование резервных копий	Не требуется	При необходимости (для К1, К2)
Контроль целостности	Визуальный	Автоматизированный (контрольные суммы)
Тестирование восстановления	Раз в 2 года	Ежегодно

9.2. Для ИСПДн резервированию подлежат:

- базы данных ПДн;
- специальное программное обеспечение;
- общее программное обеспечение (операционные системы);
- программное обеспечение средств защиты информации.

9.3. Хранение внешних носителей резервных копий должно осуществляться в защищенном хранилище (сейфе).

9.4. При выводе из эксплуатации носителей с резервными копиями ПДн они подлежат физическому уничтожению или гарантированному стиранию.

10. Ответственность и контроль

10.1. **Распределение ответственности**:

Роль	Ответственность
Ведущий инженер-программист	Техническая реализация резервного копирования, восстановление данных, ведение журналов
Главный администратор БИС	Своевременное сохранение отчетных данных билетной системы
Бухгалтеры	Контроль наличия резервных копий бухгалтерских данных (по возможности)
Ответственный за защиту информации	Общий контроль соблюдения Стандарта, организация тренировок

10.2. **Контроль соблюдения требований** осуществляется путем:

- еженедельной проверки факта создания резервных копий;
- ежемесячного анализа журналов резервного копирования;
- периодического тестирования восстановления.

10.3. Нарушение требований настоящего Стандарта влечет дисциплинарную ответственность в соответствии с законодательством РФ.

11. Заключительные положения

11.1. Настоящий Стандарт вступает в силу с даты его утверждения директором Учреждения.

11.2. Изменения и дополнения в настоящий Стандарт вносятся путем утверждения новой редакции либо путем утверждения изменений к нему.

11.3. С настоящим Стандартом должны быть ознакомлены под подпись все работники, ответственные за резервное копирование и восстановление данных.

11.4. Контроль за соблюдением требований настоящего Стандарта возлагается на лицо, ответственное за организацию защиты информации.

ПРИЛОЖЕНИЕ № 1

к Стандарту резервного копирования

ЖУРНАЛ УЧЕТА НОСИТЕЛЕЙ РЕЗЕРВНЫХ КОПИЙ

№ п/п	Дата учета	Тип носителя	Идентификатор носителя (метка)	Содержание резервной копии	Ответственный	Место хранения	Отметка о выбытии (дата, причина)
1		Внешний HDD	НЖМД-001	Резервные копии 1С (ежедневные)	Савкин Д.А.	Серверная	
2		Внешний HDD	НЖМД-002	Резервные копии 1С (архивные)	Савкин Д.А.	Серверная	
3		Внешний HDD	НЖМД-003	Копии сетевых папок, отчеты БИС	Савкин Д.А.	Сейф Усольцевой Ю.В.	
4							

ПРИЛОЖЕНИЕ № 2
к Стандарту резервного копирования

ЖУРНАЛ УЧЕТА СОЗДАНИЯ И ИСПОЛЬЗОВАНИЯ РЕЗЕРВНЫХ КОПИЙ

Дата	Информационный ресурс	Тип копирования (полное/инкрементальное)	Носитель (идентификатор)	Результат (успешно/ошибки)	Факт восстановления (да/нет, причина)	Ответственный	Примечание

ПРИЛОЖЕНИЕ № 3

к Стандарту резервного копирования

АКТ ТЕСТИРОВАНИЯ РЕЗЕРВНОГО КОПИРОВАНИЯ № ___

г. Петрозаводск «» _____ 20 г.

Комиссия в составе:

1. _____ — ответственный за организацию защиты информации;
2. _____ — ведущий инженер-программист;
3. _____ — (при необходимости),

провела тестирование возможности восстановления информации из резервных копий.

В ходе тестирования:

1. Выбрана резервная копия от «» _____ 20 г., содержащая: _____
2. Произведено восстановление данных на тестовом оборудовании.
3. Фактическое время восстановления составило: _____ (часов/минут).
4. Проверена целостность и полнота восстановленных данных: _____

Результаты тестирования:

- восстановление выполнено успешно, данные соответствуют оригиналу;
- восстановление выполнено с замечаниями (указать): _____
- восстановление не удалось (указать причины): _____

Выводы и рекомендации:

_____

Подписи членов комиссии:

_____ /_____/
_____ /_____/
_____ /_____/

ПРИЛОЖЕНИЕ № 4

к Стандарту резервного копирования

ПАМЯТКА ПО РЕЗЕРВНОМУ КОПИРОВАНИЮ ДЛЯ ОТВЕТСТВЕННЫХ ЛИЦ

Общие правила:

1. Регулярность — главный принцип резервного копирования.
2. Все резервные копии должны проверяться на возможность восстановления.
3. Храните копии в разных местах (основное и резервное).
4. Ведите журналы учета — это подтверждение выполнения требований.

Ежедневно:

- Контролировать автоматическое создание резервных копий 1С.
- Проверять отсутствие ошибок в логах резервирования.

Еженедельно:

- Создавать копии данных билетной системы.
- Проверять наличие свободного места на носителях.

Ежемесячно:

- Проводить выборочную проверку целостности резервных копий.
- Обновлять архивные копии за прошедший месяц.

При возникновении сбоя:

1. Не паниковать.
2. Оценить масштаб проблемы.
3. Выбрать подходящую резервную копию.
4. Восстановить данные.
5. Зафиксировать факт восстановления в журнале.

Контактная информация:

- Ведущий инженер-программист: _____
- Ответственный за защиту информации: _____

Приложение №3
Утверждено приказом
БУ «Музыкальный
театр Республики Карелия»
№62 от «18» марта 2026г.

СТАНДАРТ АНТИВИРУСНОЙ ЗАЩИТЫ

1. Общие положения

1.1. Настоящий Стандарт антивирусной защиты (далее — Стандарт) разработан в соответствии с:

- Приказом 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»;
- Приказом ФСТЭК России от 20.03.2012 № 28 «Об утверждении Требований к средствам антивирусной защиты»;
- 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»;
- Политикой защиты информации БУ «Музыкальный театр Республики Карелия»;
- Политикой Учреждения в отношении обработки персональных данных, утверждённой в установленном порядке;
- Перечнем лиц, имеющих доступ к персональным данным, утверждённым в установленном порядке;
- Стандартом идентификации и аутентификации БУ «Музыкальный театр Республики Карелия»;
- Стандартом управления доступом БУ «Музыкальный театр Республики Карелия».

1.2. **Цель Стандарта** — обеспечение защиты информации Учреждения от вредоносных программ, несанкционированного доступа, а также предотвращение нарушений целостности, доступности и конфиденциальности информации вследствие воздействия вредоносного кода.

1.3. **Задачи Стандарта**:

- определение порядка применения средств антивирусной защиты (САВЗ);
- установление требований к используемым антивирусным средствам;
- регламентация действий по обновлению антивирусных баз и программных модулей;
- определение порядка действий при обнаружении вредоносных объектов;
- распределение ответственности за обеспечение антивирусной защиты.

1.4. **Область действия**: настоящий Стандарт распространяется на:

- все автоматизированные рабочие места (АРМ) работников Учреждения;
- серверное оборудование (при наличии);
- информационные системы «1С Бухгалтерия» и «Яндекс Тикетс»;
- съемные машинные носители информации;
- личные мобильные устройства работников (при использовании в служебных целях).

1.5. **Особые условия**: На момент утверждения настоящего Стандарта в Учреждении отсутствуют информационные системы персональных данных (ИСПДн), введенные в

эксплуатацию. Требования к сертификации средств антивирусной защиты применяются в соответствии с текущим уровнем защищаемой информации. В случае создания ИСПДн требования настоящего Стандарта подлежат пересмотру и усилению согласно разделу 9.

2. Термины и определения

Вредоносная программа — программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы.

Средство антивирусной защиты (САВЗ) — программное средство, предназначенное для обнаружения, предотвращения распространения и уничтожения вредоносных программ, а также для восстановления информации, подвергшейся воздействию вредоносных программ.

Антивирусная база — совокупность данных, содержащих сведения о вредоносных программах, их сигнатурах и методах нейтрализации.

Антивирусный сканер — компонент САВЗ, осуществляющий проверку объектов по требованию пользователя или по расписанию.

Антивирусный монитор — компонент САВЗ, осуществляющий проверку объектов в режиме реального времени (при доступе, создании, модификации).

Карантин — изолированное хранение подозрительных или зараженных объектов с целью последующего анализа или восстановления.

Эвристический анализатор — компонент САВЗ, позволяющий обнаруживать неизвестные вредоносные программы по характерным признакам.

Сертифицированное САВЗ — средство антивирусной защиты, прошедшее испытания во ФСТЭК России и имеющее действующий сертификат соответствия.

3. Требования к средствам антивирусной защиты

3.1. На всех автоматизированных рабочих местах и серверах Учреждения должны быть установлены средства антивирусной защиты.

3.2. **Требования к САВЗ**:

- возможность обнаружения и нейтрализации известных вредоносных программ;
- наличие антивирусного монитора (защита в реальном времени);
- наличие антивирусного сканера (проверка по требованию);
- возможность автоматического обновления антивирусных баз;
- возможность создания карантина;
- наличие эвристического анализатора для обнаружения неизвестных угроз;
- ведение журналов событий (дата, время, тип угрозы, результат обработки);
- возможность централизованного управления (при наличии серверной инфраструктуры).

3.3. **Требования к сертификации САВЗ**:

Категория информации	Требование к сертификации
Общедоступная информация, служебная информация без грифа ограничения доступа	Сертификация не обязательна, рекомендуется использование лицензионных антивирусных средств
Персональные данные (при наличии ИСПДн)	Обязательно использование сертифицированных ФСТЭК России САВЗ

Категория информации	Требование к сертификации
Информация, содержащая государственную тайну	Сертифицированные САВЗ с соответствующим уровнем доверия

3.4. **На текущем этапе** (в связи с отсутствием ИСПДн) допускается использование:

- коммерческих антивирусных средств российского производства;
- бесплатных антивирусных средств для домашнего использования **не допускается**.

3.5. **При создании ИСПДн** Учреждение обязано перейти на использование сертифицированных ФСТЭК России средств антивирусной защиты. Рекомендованные сертифицированные САВЗ (по состоянию на 2026 год):

Производитель	Продукт	Сертификат ФСТЭК	Класс защиты	Тип САВЗ
«Доктор Веб»	Dr.Web Enterprise Security Suite	3509, 5003	2, 4	А, Б, В, Г
«Доктор Веб»	Dr.Web Industrial	4903	2	А, Б, В, Г
«Лаборатория Касперского»	Kaspersky Endpoint Security	4068, 509	2, 4	Б, В
«Лаборатория Касперского»	Kaspersky Security Center	3155	2	А
Positive Technologies	PT MultiScanner	4380/1	4	А
Positive Technologies	PT Sandbox	4604	4	А, Б
«Код Безопасности»	Secret Net Studio	3745	4	А, Б, В, Г
VR Technologies	VR Protect	4990	4	А, Б, В

4. Порядок установки и настройки САВЗ

4.1. **Установка САВЗ** осуществляется ведущим инженером-программистом на все АРМ и серверы Учреждения.

4.2. **Параметры настройки САВЗ**:

Параметр	Значение	Обоснование
Антивирусный монитор	Включен постоянно	Обеспечение защиты в реальном времени
Проверка при открытии файлов	Включена	Предотвращение запуска вредоносных программ

Параметр	Значение	Обоснование
Проверка при сохранении файлов	Включена	Контроль создаваемых файлов
Проверка съемных носителей	Включена (при подключении)	Контроль внешних источников угроз
Проверка электронной почты	Включена (при наличии почтового клиента)	Защита от вредоносных вложений
Эвристический анализатор	Включен (средний уровень)	Обнаружение неизвестных угроз
Действие при обнаружении	Лечение (если возможно), иначе карантин	Сохранение возможности восстановления

4.3. После установки САВЗ должна быть проведена полная проверка всех дисков и критических областей системы.

5. Обновление антивирусных баз и программных модулей

5.1. **Периодичность обновления антивирусных баз**:
- рекомендуется — ежедневно;
- минимально допустимо — не реже 1 раза в 3 дня;
- при создании ИСПДн — ежедневно (обязательно).

5.2. **Способ обновления**:
- автоматическое обновление через Интернет (при наличии подключения);
- ручное обновление (для компьютеров без доступа к Интернету) — не реже 1 раза в неделю.

5.3. **Обновление программных модулей САВЗ** (версий антивируса) проводится по мере выхода новых версий, но не реже 1 раза в год.

5.4. Ответственный за обновление — ведущий инженер-программист или администратор соответствующей информационной системы.

5.5. **Контроль обновлений**:
- еженедельная проверка даты последнего обновления баз;
- немедленное принятие мер при обнаружении компьютеров с устаревшими базами.

6. Порядок действий при обнаружении вредоносных объектов

6.1. **При обнаружении вредоносной программы антивирусным средством** автоматически выполняются действия в соответствии с настройками (лечение, карантин, удаление).

6.2. **При невозможности автоматического лечения** работник обязан:

1. Немедленно прекратить работу с компьютером.
2. Сообщить о инциденте ведущему инженеру-программисту или ответственному за защиту информации.
3. Не предпринимать самостоятельных действий по удалению файлов (если это не предусмотрено инструкцией).

6.3. **Действия ответственного лица**:

1. Зафиксировать факт обнаружения вредоносной программы (время, тип угрозы, зараженные файлы).
2. Провести анализ зараженной системы.
3. Принять меры по лечению или удалению зараженных объектов.
4. При необходимости восстановить информацию из резервных копий.
5. Выяснить возможные причины заражения (открытие подозрительных файлов, использование съемных носителей, посещение опасных сайтов).
6. Провести внеплановый инструктаж с работником по правилам антивирусной безопасности.

6.4. **При массовом заражении** (более 3 компьютеров):

1. Создать комиссию по расследованию инцидента.
2. Оценить масштабы заражения и нанесенный ущерб.
3. Принять меры по локализации и ликвидации последствий.
4. При необходимости отключить зараженные компьютеры от сети.
5. Подготовить отчет для директора Учреждения.

7. Профилактические мероприятия

7.1. **Периодические проверки**:

Тип проверки	Периодичность	Ответственный
Полная проверка всех дисков	Не реже 1 раза в месяц	Ведущий инженер-программист
Проверка актуальности антивирусных баз	Еженедельно	Ведущий инженер-программист
Проверка работоспособности антивирусного монитора	Еженедельно	Ведущий инженер-программист
Анализ журналов событий антивируса	Ежемесячно	Ответственный за ЗИ

7.2. **Мониторинг уязвимостей**:

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

• При выявлении критических уязвимостей в программном обеспечении, которые могут быть использованы для распространения вредоносных программ, должны приниматься меры по их устранению в установленные сроки:

— критические уязвимости — не более 24 часов;
— уязвимости высокой степени опасности — не более 7 дней.

8. Обязанности работников по обеспечению антивирусной защиты

8.1. **Все работники Учреждения обязаны**:

• не отключать и не изменять настройки антивирусного средства без согласования с ответственным лицом;

• не устанавливать дополнительное программное обеспечение без разрешения;

• не открывать подозрительные файлы, полученные по электронной почте или из других источников;

• не использовать съемные носители неизвестного происхождения;

• немедленно сообщать о любых признаках заражения (медленная работа, появление подозрительных окон, блокировка файлов);

• проходить инструктаж по антивирусной защите не реже 1 раза в 2 года.

8.2. **Работникам запрещается**:

• использовать нелицензионное программное обеспечение;

• отключать антивирусный монитор;

• игнорировать сообщения антивируса об обнаружении угроз;

• самостоятельно лечить или удалять зараженные файлы без указаний ответственного лица;

• подключать личные съемные носители без предварительной проверки.

9. Порядок действий при создании ИСПДн

9.1. В случае принятия решения о создании информационной системы персональных данных (ИСПДн) ответственный за организацию защиты информации обязан:

9.1.1. В течение **10 рабочих дней** инициировать пересмотр настоящего Стандарта в части усиления требований к антивирусной защите.

9.1.2. Обеспечить выполнение следующих дополнительных требований:

Требование	**Текущий уровень**	**Требуемый уровень для ИСПДн**
Сертификация САВЗ	Не обязательна	Обязательна (сертификат ФСТЭК России)
Класс защиты САВЗ	Не определен	В соответствии с классом ИСПДн
Периодичность обновления баз	1-3 дня	Ежедневно
Централизованное управление	Желательно	Обязательно
Контроль съемных носителей	Базовый	Расширенный контроль
Аудит событий	Основные события	Расширенный перечень

9.2. Рекомендуемые сертифицированные САВЗ для различных классов ИСПДн:

• **ИСПДн класса К2 и К3** — САВЗ 2 класса защиты (Dr.Web Enterprise Security Suite, Kaspersky Endpoint Security, Kaspersky Security Center).

• **ИСПДн класса К1** — САВЗ 2 или 4 класса защиты в зависимости от требований.

10. Контроль и ответственность

10.1. **Контроль соблюдения требований** настоящего Стандарта осуществляется:

• ответственным за организацию защиты информации — постоянно;

• ведущим инженером-программистом — при проведении профилактических проверок;

• руководителями структурных подразделений — в части соблюдения работниками правил антивирусной безопасности.

10.2. **Периодический аудит** антивирусной защиты проводится не реже одного раза в год с составлением акта.

10.3. **Ответственность**:

• **пользователи** — за соблюдение правил работы и своевременное информирование о проблемах;

• **ведущий инженер-программист** — за своевременную установку обновлений и корректную настройку САВЗ;

• **ответственный за защиту информации** — за общий контроль и организацию расследований инцидентов.

10.4. Нарушение требований настоящего Стандарта влечет дисциплинарную ответственность в соответствии с законодательством РФ.

11. Заключительные положения

11.1. Настоящий Стандарт вступает в силу с даты его утверждения директором Учреждения.

11.2. Изменения и дополнения в настоящий Стандарт вносятся путем утверждения новой редакции либо путем утверждения изменений к нему.

11.3. С настоящим Стандартом должны быть ознакомлены под подпись все работники, имеющие доступ к информационным системам Учреждения.

11.4. Контроль за соблюдением требований настоящего Стандарта возлагается на лицо, ответственное за организацию защиты информации.

ПРИЛОЖЕНИЕ № 1

к Стандарту антивирусной защиты

ЖУРНАЛ УЧЕТА АНТИВИРУСНЫХ ПРОВЕРОК И ИНЦИДЕНТОВ

Дата	Проверяемый компьютер (инв. номер)	Тип проверки	Результат	Обнаруженные угрозы	Принятые меры	Ответственный

Типы проверок:

- П — плановая (ежемесячная)
- В — внеплановая (по требованию)
- И — проверка после инцидента

ПРИЛОЖЕНИЕ № 2
к Стандарту антивирусной защиты

ПАМЯТКА ПО АНТИВИРУСНОЙ ЗАЩИТЕ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ

(выдается каждому работнику под подпись)

Уважаемый коллега!

Для обеспечения безопасности информации в Музыкальном театре убедительно просим соблюдать следующие правила:

1. ЗАПРЕЩАЕТСЯ:

- Отключать антивирусную программу или изменять ее настройки.
- Игнорировать сообщения антивируса об обнаружении угроз.
- Устанавливать любые программы без разрешения системного администратора.
- Использовать нелицензионное программное обеспечение.
- Подключать личные флешки, диски и другие носители без необходимости.

2. НЕОБХОДИМО:

- Ежедневно обращать внимание на дату обновления антивирусных баз (значок антивируса в трее).
- При появлении подозрительных сообщений, замедлении работы, блокировках файлов — немедленно сообщать ведущему инженеру-программисту.
- Перед открытием файлов, полученных по электронной почте или на съемных носителях, убедиться, что они проверены антивирусом.

3. ПРИ ОБНАРУЖЕНИИ ВИРУСА:

1. Не паниковать.
2. Прекратить работу с компьютером.
3. Сообщить о проблеме по телефону: _____.
4. Не пытаться самостоятельно удалять файлы, на которые указывает антивирус.

Помните: от вашей внимательности зависит безопасность всего Учреждения!

С памяткой ознакомлен(а):

_____ / _____ /
(подпись) (ФИО)

«» _____ 20 г.

Приложение №2
Утверждено приказом
БУ «Музыкальный
театр Республики Карелия»
№62 от «18» марта 2026г.

СТАНДАРТ УПРАВЛЕНИЯ ДОСТУПОМ

1. Общие положения

1.1. Настоящий Стандарт управления доступом (далее – Стандарт) разработан в соответствии с:

- Приказом 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»;
- 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»;
- Политикой защиты информации БУ «Музыкальный театр Республики Карелия»;
- Политикой Учреждения в отношении обработки персональных данных, утверждённой в установленном порядке;
- Перечнем лиц, имеющих доступ к персональным данным, утверждённым в установленном порядке;
- Стандартом идентификации и аутентификации БУ «Музыкальный театр Республики Карелия».

1.2. **Цель Стандарта** – установление единых требований к управлению доступом пользователей к информационным ресурсам Учреждения, обеспечение защиты информации от несанкционированного доступа, предотвращение случайного или преднамеренного неправомерного использования информационных ресурсов.

1.3. **Область действия**: настоящий Стандарт распространяется на всех работников Учреждения, а также на подрядные организации (при предоставлении им доступа), взаимодействующих со следующими информационными ресурсами:

- бухгалтерская система «1С Бухгалтерия»;
- билетно-информационная система «Яндекс Тикетс»;
- официальный сайт Учреждения (административная часть);
- автоматизированные рабочие места (АРМ) работников;
- файловые ресурсы и сетевые папки;
- иные информационные системы, используемые в деятельности Учреждения.

1.4. **Особые условия**: На момент утверждения настоящего Стандарта в Учреждении отсутствуют информационные системы персональных данных (ИСПДн), введенные в эксплуатацию в установленном порядке. Требования настоящего Стандарта учитывают текущий уровень защиты и предусматривают возможность их усиления при создании ИСПДн в соответствии с разделом 8 настоящего Стандарта.

2. Термины и определения

Доступ – возможность получения информации и ее использования.

Права доступа – совокупность правил, регламентирующих порядок и условия доступа субъекта к объектам информационной системы.

Несанкционированный доступ (НСД) – доступ к информации или действиям с ней, осуществляемый с нарушением установленных прав доступа.

Разграничение доступа – применение правил, ограничивающих доступ субъектов к объектам информационной системы.

Привилегированный доступ – доступ, предоставляющий пользователю права, превышающие права обычного пользователя (администрирование, настройка, управление учетными записями).

Матрица доступа – таблица, определяющая для каждой категории пользователей (роли) разрешенные действия с объектами доступа.

Принцип минимальных привилегий – предоставление пользователям только тех прав доступа, которые необходимы им для выполнения должностных обязанностей.

3. Основные принципы управления доступом

3.1. Управление доступом в Учреждении осуществляется на основе следующих принципов:

3.1.1. **Законность** – предоставление доступа только на основании законных требований и должностных обязанностей.

3.1.2. **Персонификация** – каждый пользователь должен иметь уникальную учетную запись. Использование групповых учетных записей допускается только в исключительных случаях (технологические учетные записи) с обязательным контролем.

3.1.3. **Минимальные привилегии** – пользователям предоставляется минимально необходимый для выполнения работы набор прав.

3.1.4. **Разделение обязанностей** – критически важные операции должны требовать участия нескольких сотрудников (например, создание учетной записи и назначение прав).

3.1.5. **Своевременность** – права доступа предоставляются с момента возникновения необходимости и отзываются немедленно при ее прекращении.

3.1.6. **Контролируемость** – все действия по предоставлению, изменению и отзыву прав доступа должны документироваться.

4. Категории пользователей и объектов доступа

4.1. **Категории пользователей** (согласно Перечню лиц, имеющих доступ к персональным данным, утверждённому в установленном порядке, и организационной структуре):

Категория	Должности	Особенности доступа
Руководство	Директор, заместители директора	Полный доступ к информации в соответствии с компетенцией
Администраторы ИС	Ведущий инженер-программист	Полный доступ к настройке и администрированию ИС
Пользователи БИС	Администраторы билетно-информационной системы, главный администратор БИС	Доступ к билетно-информационной системе в соответствии с должностными обязанностями

Категория	Должности	Особенности доступа
Пользователи бухгалтерии	Бухгалтеры	Доступ к бухгалтерской системе «1С Бухгалтерия»
Обычные пользователи	Иные работники	Доступ только к общедоступным ресурсам и служебной информации в рамках обязанностей
Внешние пользователи	Подрядчики, партнеры	Ограниченный доступ на время выполнения работ по договору

4.2. **Объекты доступа**:

- информационные системы («1С Бухгалтерия», «Яндекс Тикетс», сайт);
- файловые ресурсы (сетевые папки, документы);
- аппаратные ресурсы (серверы, сетевое оборудование);
- служебная информация (приказы, распоряжения, отчеты);
- персональные данные (при наличии).

5. Порядок предоставления доступа

5.1. **Инициация предоставления доступа**:

5.1.1. Основанием для предоставления доступа является:

- прием на работу (для новых сотрудников);
- изменение должностных обязанностей;
- служебная записка от руководителя структурного подразделения;
- договор с подрядной организацией (для внешних пользователей).

5.1.2. Служебная записка должна содержать:

- ФИО сотрудника;
- должность;
- перечень информационных систем и ресурсов, к которым требуется доступ;
- необходимый уровень прав (чтение, запись, редактирование, администрирование);
- обоснование необходимости доступа.

5.2. **Согласование доступа**:

5.2.1. Служебная записка согласовывается с:

- руководителем структурного подразделения;
- ответственным за организацию защиты информации;
- владельцем информационной системы (при необходимости).

5.2.2. Ответственный за организацию защиты информации проверяет:

- соответствие запрашиваемых прав должностным обязанностям;
- соблюдение принципа минимальных привилегий;
- отсутствие конфликта интересов (разделение обязанностей).

5.3. **Техническая реализация**:

5.3.1. После согласования ведущий инженер-программист (или иное уполномоченное лицо) создает учетную запись и назначает права доступа в соответствии с утвержденной заявкой.

5.3.2. Срок создания учетной записи – не более 3 рабочих дней с момента получения согласованной заявки.

5.3.3. Пользователь должен быть ознакомлен с правилами работы в информационной системе под подпись.

6. Матрица доступа

6.1. **Матрица доступа к информационным системам Учреждения** (Р – чтение, З – запись/редактирование, А – администрирование, П – полный доступ)

Должность / Роль	«1С Бухгалтерия»	«Яндекс Тикетс»	Сайт (админка)	Сетевые папки	Примечание
Директор	П	Р	Р	П	По необходимости
Зам. директора по финансово-экономической деятельности	П	П	Р	П	
Ведущий инженер-программист	А	А	А	П	Техническое администрирование
Главный администратор БИС	–	П (отчеты)	–	Р	Доступ к отчетности
Администратор БИС	–	П (продажи)	–	–	Оформление и продажа билетов
Бухгалтер	П	Р (возвраты)	–	Р	Обработка возвратов, отчетность
Иные работники	–	–	–	По задаче	Только по служебной записке

6.2. Матрица доступа подлежит пересмотру **не реже одного раза в год**, а также при изменении организационной структуры или внедрении новых информационных систем.

6.3. Детальная матрица доступа с указанием конкретных прав по каждой информационной системе (с учётом должностных обязанностей конкретных сотрудников) хранится во внутренней документации Учреждения и доводится до сведения ответственных лиц в установленном порядке.

7. Порядок изменения и отзыва прав доступа

7.1. **Изменение прав доступа** осуществляется в том же порядке, что и предоставление (по служебной записке с обоснованием).

7.2. **Отзыв прав доступа** производится в следующих случаях:

Основание	Срок отзыва	Ответственный
Увольнение сотрудника	В день увольнения	Отдел кадров, ведущий инженер-программист
Перевод на другую должность	В день перевода	Руководитель подразделения
Окончание срока договора с подрядчиком	В день окончания	Ответственный за договор
Выявление нарушений	Немедленно	Ответственный за ЗИ
Длительное отсутствие (более 30 дней)	По заявлению руководителя	Ведущий инженер-программист

7.3. При увольнении сотрудника:

7.3.1. Отдел кадров обязан в день увольнения направить уведомление ответственному за защиту информации и ведущему инженеру-программисту.

7.3.2. Ведущий инженер-программист обязан заблокировать (удалить) учетную запись уволенного сотрудника во всех информационных системах.

7.3.3. Доступ к данным уволенного сотрудника (при необходимости) предоставляется его руководителю по отдельной заявке.

8. Требования к привилегированному доступу

8.1. **Категории привилегированных пользователей**:

- ведущий инженер-программист (администрирование ИС);
- ответственный за защиту информации (контроль доступа);
- администраторы БИС (в части управления билетами);
- бухгалтеры (в части финансовых операций).

8.2. **Особые требования к привилегированному доступу**:

8.2.1. Привилегированные учетные записи должны быть строго персонифицированы.

8.2.2. Запрещается совместное использование привилегированных учетных записей.

8.2.3. Действия с использованием привилегированных учетных записей подлежат обязательной регистрации и периодическому контролю.

8.2.4. Для привилегированного доступа применяются усиленные требования к паролям (согласно Стандарту идентификации и аутентификации).

8.2.5. **При создании ИСПДн** для привилегированного доступа вводится строгая (двухфакторная) аутентификация.

8.3. Встроенные (стандартные) учетные записи администраторов (admin, root, Administrator и т.п.) должны быть:

- переименованы (если технически возможно);
- отключены (если не используются);
- пароли изменены на уникальные и сложные.

9. Контроль и периодический пересмотр прав доступа

9.1. **Периодический пересмотр** прав доступа проводится **не реже одного раза в год** комиссией в составе:

• ответственного за организацию защиты информации;
• ведущего инженера-программиста;
• представителя отдела кадров (при необходимости).

9.2. В ходе пересмотра проверяется:
• соответствие текущих прав доступа должностным обязанностям;
• наличие учетных записей уволенных сотрудников;
• наличие избыточных прав;
• соблюдение принципа минимальных привилегий.

9.3. Результаты пересмотра оформляются **Актом пересмотра прав доступа** (Приложение № 2 к настоящему Стандарту).

9.4. Внеплановый пересмотр проводится:
• при реорганизации Учреждения;
• при смене ответственных лиц;
• после серьезных инцидентов информационной безопасности;
• при создании новых информационных систем.

10. Порядок действий при создании ИСПДн

10.1. В случае принятия решения о создании информационной системы персональных данных (ИСПДн) ответственный за организацию защиты информации обязан:

10.1.1. В течение **10 рабочих дней** инициировать пересмотр настоящего Стандарта в части усиления требований к управлению доступом.

10.1.2. Обеспечить выполнение следующих дополнительных требований:

Требование	Реализация
Детальная матрица доступа к ИСПДн	Разрабатывается для каждой ИСПДн отдельно
Разделение обязанностей	Администратор ИСПДн и администратор безопасности – разные лица (при возможности)
Контроль привилегированного доступа	Усиленный мониторинг действий привилегированных пользователей
Регистрация действий	Расширенный перечень регистрируемых событий
Периодичность контроля	Ежеквартально (вместо ежегодного)

10.2. Все изменения, связанные с доступом к ИСПДн, должны фиксироваться в электронных журналах с невозможностью редактирования.

11. Ответственность

11.1. **Пользователи** несут ответственность за:
• использование только разрешенных информационных ресурсов;
• недопущение передачи своих учетных данных третьим лицам;
• своевременное информирование об изменении должностных обязанностей.

11.2. **Руководители подразделений** несут ответственность за:
• обоснованность запросов на предоставление доступа;

• своевременное информирование об увольнении или переводе сотрудников.

11.3. **Ответственный за организацию защиты информации** несет ответственность за:

• контроль соблюдения настоящего Стандарта;
• периодический пересмотр прав доступа;
• реагирование на нарушения.

11.4. **Ведущий инженер-программист** несет ответственность за:

• техническую реализацию предоставления/отзыва прав доступа;
• сохранность журналов регистрации;
• корректную настройку средств разграничения доступа.

11.5. За нарушение требований настоящего Стандарта работники могут быть привлечены к дисциплинарной ответственности в соответствии с законодательством РФ.

12. Заключительные положения

12.1. Настоящий Стандарт вступает в силу с даты его утверждения директором Учреждения.

12.2. Изменения и дополнения в настоящий Стандарт вносятся путем утверждения новой редакции либо путем утверждения изменений к нему.

12.3. С настоящим Стандартом должны быть ознакомлены под подпись все работники, имеющие доступ к информационным системам Учреждения.

12.4. Контроль за соблюдением требований настоящего Стандарта возлагается на лицо, ответственное за организацию защиты информации.

ПРИЛОЖЕНИЕ № 1
к Стандарту управления доступом

АКТ ПЕРЕСМОТРА ПРАВ ДОСТУПА № ____

г. Петрозаводск «» _____ 20 г.

Комиссия в составе:

1. _____ — ответственный за организацию защиты информации;
2. _____ — ведущий инженер-программист;
3. _____ — представитель отдела кадров (при необходимости),

провела периодический пересмотр прав доступа пользователей к информационным системам БУ «Музыкальный театр Республики Карелия».

В ходе пересмотра установлено:

1. Всего учетных записей в информационных системах: _____
2. Из них действующих: _____
3. Выявлено учетных записей уволенных сотрудников: _____
4. Выявлено избыточных прав доступа: _____
5. Выявлено нарушений принципа минимальных привилегий: _____

Комиссия решила:

1. Блокировать (удалить) учетные записи следующих сотрудников:
   _____
2. Скорректировать права доступа следующим сотрудникам:
   _____
3. Провести повторную проверку устранения недостатков в срок до «» _____ 20 г.

Подписи членов комиссии:

_____ /_____
_____ /_____
_____ /_____/

Ознакомлены (по необходимости):

_____ /_____
_____ /_____

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

СТАНДАРТ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

1. Общие положения

1.1. Настоящий Стандарт идентификации и аутентификации (далее – Стандарт) разработан в соответствии с:

- Приказом 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»;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Политикой защиты информации БУ «Музыкальный театр Республики Карелия»;
- Уставом Учреждения.

1.2. **Цель Стандарта** – установление единых требований к идентификации и аутентификации пользователей при доступе к информационным системам Учреждения, обеспечение защиты информации от несанкционированного доступа.

1.3. **Область действия**: настоящий Стандарт распространяется на всех работников Учреждения, а также на подрядные организации (при предоставлении им доступа), взаимодействующих со следующими информационными ресурсами:

- автоматизированные рабочие места (АРМ) работников;
- бухгалтерская система «1С Бухгалтерия»;
- билетно-информационная система «Яндекс Тикетс»;
- официальный сайт Учреждения (административная часть);
- иные информационные системы, используемые в деятельности Учреждения.

1.4. **Особый статус систем**: на момент утверждения настоящего Стандарта в Учреждении отсутствуют информационные системы персональных данных (ИСПДн), подлежащие регистрации в уполномоченных органах. В случае принятия решения о создании ИСПДн требования настоящего Стандарта подлежат пересмотру и ужесточению в соответствии с законодательством о персональных данных.

2. Термины и определения

Идентификация – присвоение субъектам и объектам доступа уникального признака (идентификатора) и сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов.

Аутентификация – проверка принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

ИСПДн (информационная система персональных данных) – информационная система, предназначенная для обработки персональных данных.

Привилегированная учетная запись – учетная запись, обладающая расширенными правами по управлению информационной системой, настройке программного обеспечения, доступу к конфиденциальной информации (при наличии).

3. Требования к идентификации пользователей

3.1. Каждому пользователю информационных систем Учреждения присваивается **уникальный идентификатор** (логин), который не должен повторяться в рамках одной информационной системы.

3.2. Формирование идентификатора осуществляется по правилу: фамилия_инициалы (например, ivanov_ii). Допускается добавление цифрового индекса при совпадении.

3.3. Запрещается использование:

- групповых учетных записей для идентификации конкретных лиц (за исключением временных технологических учетных записей, необходимых для функционирования программного обеспечения);

3.4. Идентификация осуществляется при каждом сеансе доступа к информационной системе.

4. Требования к парольной аутентификации

4.1. **Требования к паролям пользователей**:

- минимальная длина пароля – **не менее 6 символов** (для внутренних систем с невысоким уровнем риска);
- для систем, имеющих выход в сеть Интернет («Яндекс Тикетс», административная часть сайта) – **не менее 8 символов**;
- пароль должен содержать символы не менее чем **двух из четырех категорий**:
  - строчные буквы латинского алфавита (a–z);
  - прописные буквы латинского алфавита (A–Z);
  - цифры (0–9);
  - специальные символы (! @ # $ % ^ & * и др.);
- запрет на использование в пароле:
  - имени пользователя или его части (более 3 последовательных символов);
  - очевидных комбинаций (123456, qwerty, password и т.п.).

4.2. **Срок действия пароля**:

- для обычных пользователей – **не более 180 дней** (6 месяцев);
- для привилегированных учетных записей – **не более 90 дней**.

4.3. **История паролей**: запрещается использовать **2 последних использованных пароля**.

4.4. **Хранение паролей**:

- пароли должны храниться в информационных системах в хешированном (необратимом) виде;
- запрещается хранение паролей в открытом виде, в том числе в файлах, документах, на бумажных носителях.

4.5. **Передача паролей**:

- запрещается передавать пароли другим лицам, включая коллег и руководителей;
- первоначальные (временные) пароли должны передаваться пользователю защищенным способом (лично под подпись, по внутренней корпоративной связи).

5. Требования к привилегированным учетным записям

5.1. **Категории привилегированных пользователей** (согласно текущей организационной структуре):

- заместитель директора по финансово-экономической деятельности и маркетингу;
- ведущий инженер-программист;
- администраторы билетно-информационной системы;
- главный администратор билетно-информационной системы;
- бухгалтеры (в части доступа к «1С Бухгалтерия»).

5.2. Привилегированные учетные записи должны быть **персонифицированными**.

5.3. **Запрещается** использование одной привилегированной учетной записи несколькими лицами.

5.4. Привилегированные учетные записи должны иметь **минимально необходимые права** для выполнения возложенных обязанностей.

5.5. **Неиспользуемые привилегированные учетные записи** должны быть заблокированы в течение 5 рабочих дней после увольнения сотрудника или изменения его должностных обязанностей.

6. Требования к аутентификации

6.1. **В связи с отсутствием в Учреждении ИСПДн и информации, отнесенной к государственной тайне**, на текущем этапе применяется **однофакторная парольная аутентификация**.

6.2. Требования к строгой (двухфакторной) аутентификации, предусмотренные Приказом ФСТЭК № 117, будут введены в действие в следующих случаях:

- при создании информационной системы, обрабатывающей персональные данные;
- при организации удаленного доступа к информационным системам Учреждения;
- при подключении к государственным информационным системам, требующим повышенного уровня аутентификации.

6.3. **Удаленный доступ** к информационным системам Учреждения (при необходимости) должен осуществляться:

- с применением средств защиты каналов передачи данных (VPN);
- с использованием парольной аутентификации усиленной сложности (не менее 10 символов, все категории символов).

7. Регистрация и контроль действий

7.1. В информационных системах Учреждения должна быть обеспечена регистрация следующих событий:

- вход в систему (успешный/неуспешный);
- выход из системы;
- действия с привилегированными учетными записями (при технической возможности).

7.2. **Контроль использования** привилегированных учетных записей осуществляется не реже одного раза в квартал ответственным за организацию защиты информации.

8. Управление учетными записями

8.1. **Создание учетной записи** осуществляется на основании письменного распоряжения (служебной записки) от руководителя структурного подразделения, согласованного с ответственным за организацию защиты информации.

8.2. **Блокирование учетной записи** производится:

- при временном отсутствии сотрудника (более 30 дней) – по заявлению руководителя;
- при увольнении сотрудника – в день увольнения;
- при компрометации учетных данных – немедленно.

8.3. **Удаление учетной записи** производится не позднее 30 дней после увольнения сотрудника.

8.4. **Периодический пересмотр** прав доступа проводится не реже одного раза в год.

9. Действия при компрометации учетных данных

9.1. **Компрометацией** считается:

- разглашение пароля третьим лицам;
- подозрение на несанкционированный доступ к учетной записи;
- обнаружение признаков использования учетной записи посторонним лицом.

9.2. **При компрометации пользователь обязан**:

- немедленно уведомить ответственного за организацию защиты информации;
- при возможности – самостоятельно сменить пароль.

9.3. **Ответственный за защиту информации обязан**:

- заблокировать скомпрометированную учетную запись;
- организовать внеплановую смену пароля;
- провести проверку на предмет несанкционированных действий.

10. Порядок действий при создании ИСПДн

10.1. В случае принятия решения о создании информационной системы персональных данных (ИСПДн) ответственный за организацию защиты информации обязан:

10.2. В течение 10 рабочих дней инициировать пересмотр настоящего Стандарта в части:

- ужесточения требований к парольной политике (длина пароля не менее 8 символов, срок действия не более 90 дней);
- внедрения строгой (двухфакторной) аутентификации для доступа к ИСПДн;
- усиления требований к регистрации событий безопасности;
- приведения требований в соответствие с Постановлением Правительства № 1119 и Приказом ФСТЭК № 21.

10.3. Внедрение усиленных мер защиты информации должно быть завершено до начала эксплуатации ИСПДн.

11. Ответственность и контроль

11.1. Ответственность за соблюдение требований настоящего Стандарта несут:

- **пользователи** – за сохранность своих аутентификационных данных;

• **руководители структурных подразделений** – за своевременное информирование об изменении статуса сотрудников;

• **ответственный за организацию защиты информации** – за общий контроль соблюдения Стандарта.

11.2. Нарушение требований настоящего Стандарта влечет дисциплинарную ответственность.

12. Заключительные положения

12.1. Настоящий Стандарт подлежит пересмотру не реже одного раза в 3 года или при изменении законодательства РФ в области защиты информации, а также при принятии решения о создании ИСПДн.

12.2. Все изменения в Стандарт утверждаются приказом директора Учреждения.

12.3. С настоящим Стандартом должны быть ознакомлены под подпись все работники, имеющие доступ к информационным системам Учреждения.