Приложение №2 к Приказу
от «07» июля 2025 г. № 0473

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

в Федеральном государственном бюджетном учреждении культуры
«Государственный музей изобразительных искусств имени А.С. Пушкина»
(ГМИИ им. А.С. Пушкина)

Москва 2025

1. Цель разработки и область применения

Настоящая Политика информационной безопасности (далее – «Политика») описывает общие подходы и требования к обеспечению информационной безопасности в Музее.

Политика применима ко всем категориям Пользователей, всем видам информационных систем и ресурсов Музея.

2. Список сокращений и понятий

В настоящем документе используются следующие сокращения.

ИБ	Информационная безопасность
ИС	Информационная система
ИР	Информационный ресурс
ИТ	Информационные технологии
КИ	Конфиденциальная информация
КИИ	Критическая информационная инфраструктура Российской Федерации
ДСП	Для служебного пользования
Музей	ГМИИ им. А.С. Пушкина
КСИБ	Комплексная система информационной безопасности
ОС	Операционная система
ПДн	Персональные данные
ПК	Персональный компьютер
ПО	Программное обеспечение
АРМП	Автоматизированное рабочее место пользователя
УЗ	Учетная запись пользователя

В настоящем документе используются следующие термины:

Пользователь – физическое лицо, которому предоставлено рабочее место или доступ к информационным ресурсам Музея, аутентифицирующийся в ИТ-инфраструктуре и/или в информационных системах Музея с использованием персональной учетной записи.

Внутренний пользователь – сотрудник Музея, выполняющий трудовые обязанности (задачи), возложенные на него заключенным с Музеем Трудовым договором (срочным или бессрочным), или физическое лицо, выполняющее работы/оказывающее услуги и прочее, на основании договора гражданско-правового договора, заключенного с Музеем.

Внешний пользователь – сотрудник Контрагента Музея (ИТ подрядчика Музея), посетитель Музея, которому предоставлен доступ к инфраструктуре Музея в рамках договорных (или иных) отношений Контрагента с Музеем.

VIP-пользователи - категория внутренних пользователей, дирекция, заместители директора.

Системные администраторы – внутренние пользователи, выполняющие роль администраторов операционных систем и инфраструктуры.

Администраторы информационной безопасности – внутренние пользователи, выполняющие роль администраторов средств защиты информации.

Руководитель подразделения – руководитель структурного подразделения Музея.

Группа поддержки пользователей – отделы ЭВСиС, ИС, обеспечивающее исполнение запросов пользователей на ИТ-услуги, контроль сроков исполнения запросов, закрытие запросов и контроль качества исполнения запроса.

Автоматизированное рабочее место пользователя – совокупность аппаратных и/или программных средств и информационных ресурсов индивидуального рабочего места, предоставляемые Музеем в распоряжение сотрудника Музея для выполнения непосредственных производственных функций.

Стандартное ПО – программное обеспечение рабочего места, входящее в базовый комплект установки. Состав комплекта определяется «Стандартом рабочего места пользователя».

Информационные ресурсы – компоненты ИТ-инфраструктуры Музея, информационные системы, файловые ресурсы, отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах, которые могут быть идентифицированы как отдельные сущности, и к которым может быть предоставлен доступ Пользователям.

Информационная система - набор приложений, услуг, информационно-технических активов или других компонентов для обработки информации.

3. Общие положения.

3.1. Источники разработки

Настоящая Политика разработана на базе законодательных и нормативно-методических документов Российской Федерации, касающихся вопросов защиты информации (включая, но не ограничиваясь):

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ 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».

Политика учитывает внутренние требования Музея по защите информации.

3.2. Виды информации, обрабатываемой в Музее

В Музее обрабатываются различные виды информации в электронном виде, подлежащие защите. Основные виды обрабатываемой информации:

- открытая информация;
- персональные данные (сотрудников Музея, волонтеров Музея, посетителей Музея, Контрагентов Музея);
- иная информация, защищаемая Музеем.

Музей обрабатывает как собственную информацию, так и информацию, принадлежащую контрагентам Музея. Применяемые меры защиты информации определяются видом информации безотносительно к источнику и владельцу информации.

3.3. Категории пользователей в Музее

В Музее классифицируются следующие категории пользователей информации:

- Внутренние пользователи;
- VIP – пользователи;
- Системные администраторы;
- Администраторы информационной безопасности.

В Музее действует разрешительная система доступа к информации, что предполагает явное назначение прав доступа Пользователям к Информационным ресурсам Музея.

3.4. Объекты защиты в Музее

В Музее объектами информационной защиты являются:

- информация, обрабатываемая в электронном виде;
- программно-аппаратная ИТ-инфраструктура Музея;
- информационные системы Музея;
- конфигурация компонентов ИТ-инфраструктуры и ИС Музея;
- архитектура и конфигурация Комплексной системы информационной безопасности (КСИБ) Музея;
- сотрудники Музея;
- посетители Музея;
- Контрагенты Музея (при взаимодействии с ИТ-инфраструктурой Музея).

3.5. Обеспечение информационной безопасности в Музее

Под обеспечением информационной безопасности Музея понимается совокупность организационных, правовых, технических и технологических, направленных на обнаружение, предотвращение, ликвидацию последствий нарушения информационной безопасности, а также защиту информации, информационных ресурсов и технологий обработки информации от воздействий, способных привести к ухудшению характеристик процесса функционирования Музея, создать риски субъектам персональных данных, нанести ущерб Музею и Внешним пользователям Музея.

3.5.1. Риски информационной безопасности

Деятельность по управлению рисками ИБ в Музее является одним из видов деятельности в области ИБ и включает в свой состав мероприятия по идентификации, оценке рисков ИБ, выработке мер по снижению рисков ИБ. Настоящая Политика направлена на снижение рисков ИБ в Музее.

Среди ключевых рисков можно выделить следующие:

№ п.п.	ИС	Риски	Последствия
1.	Учетно-фондовая система	Риск взлома системы (внутренний/внешний)в том числе по причине уязвимостей используемых программных и аппаратных средств, Риск кражи ПДн сотрудников Музея	Остановка деятельности Музея, Кража информации Музея, Нарушение норм ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных»

2.	Портал Музея	Риск взлома системы в том числе по причине уязвимостей используемых программных и аппаратных средств, Риск кражи ПДн сотрудников Музея	Кража информации Музея, Нарушение норм ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных»
3.	Билетная система Музея	Риск взлома системы в том числе по причине уязвимостей используемых программных и аппаратных средств, Риск кражи ПДн посетителей Музея	Финансовые и правовые последствия, Остановка деятельности Музея, Нарушение норм ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных»
4.	Сетевая инфраструктура Музея, системные сервисы	Риск взлома системы в том числе по причине уязвимостей используемых программных и аппаратных средств, Риск кражи ПДн сотрудников Музея	Остановка деятельности Музея, Нарушение норм ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных»
5.	Система учета активов Музея	Риск взлома системы в том числе по причине уязвимостей используемых программных и аппаратных средств	Кража информации Музея,
6.	Системы ИБ, мониторинга, контроллеры	Риск взлома системы в том числе по причине уязвимостей используемых программных и аппаратных средств	Кража информации Музея,
7.	Библиотечная система	Риск взлома системы в том числе по причине уязвимостей используемых программных и аппаратных средств, Риск кражи ПДн сотрудников Музея	Кража информации Музея, Нарушение норм ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных»
8.	Системы ФХД	Риск взлома системы в том числе по причине уязвимостей используемых программных и аппаратных средств, Риск кражи ПДн сотрудников Музея, Риск кражи информации Контрагентов Музея (заказчиков, поставщиков, подрядчиков и др.)	Остановка деятельности Музея, Кража информации Музея, Нарушение норм ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных», Нарушение соглашения о неразглашении (NDA) с Заказчиками
9.	Справочно-информационные системы	Риск взлома системы в том числе по причине уязвимостей используемых программных и аппаратных средств	Финансовые и правовые последствия
10.	Система DAM	Риск взлома системы в том числе по причине уязвимостей используемых программных и аппаратных средств	Финансовые и правовые последствия
11.	Система резервного копирования	Риск взлома системы в том числе по причине уязвимостей используемых программных и аппаратных средств, Риск кражи ПДн сотрудников Музея, Риск	Кража информации Музея, Нарушение норм ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных»,

		кражи информации Контрагентов Музея (заказчиков, поставщиков, подрядчиков и др.), Риск кражи ПДн посетителей Музея	Нарушение соглашения о неразглашении (NDA) с Заказчиками
12.	Система электронного документооборота	Риск взлома системы в том числе по причине уязвимостей используемых программных и аппаратных средств, Риск кражи ПДн сотрудников Музея, Риск кражи информации Контрагентов Музея (заказчиков, поставщиков, подрядчиков и др.)	Кража информации Музея, Нарушение норм ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных», Нарушение соглашения о неразглашении (NDA) с Заказчиками
13.	Почтовая система	Риск взлома системы в том числе по причине уязвимостей используемых программных и аппаратных средств, Риск кражи ПДн сотрудников Музея	Кража информации Музея, Нарушение норм ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных», Нарушение соглашения о неразглашении (NDA) с Заказчиками

3.5.2. Цели политики информационной безопасности

Политика информационной безопасности разрабатывается со следующими целями:

- обеспечения должного уровня безопасности информации в Музее, в том числе конфиденциальной информации, персональных данных и иной защищаемой информации;
- исполнения норм действующего законодательства Российской Федерации;
- обеспечения доступности и непрерывности функционирования информационных систем Музея;
- обеспечения защиты информационных ресурсов Музея;
- обеспечения безопасности сотрудников Музея, посетителей, контрагентов в части ИБ.

3.5.3. Комплексная система информационной безопасности

Для реализации Политики в Музее функционирует Комплексная система информационной безопасности (КСИБ), включающая в свой состав технические и организационные меры обеспечения информационной безопасности.

Система защиты персональных данных в Музее (СЗПДн) является составной частью КСИБ, включающей те меры, которые применимы для защиты ПДн.

Технические меры защиты информации реализуются подсистемами и средствами информационной безопасности.

3.5.3. Управление доступом к информационным ресурсам

Управление доступом Пользователей к информационным ресурсам в Музее представляет собой совокупность процессов, обеспечивающих:

- ведение каталога УЗ внутренних пользователей, обеспечение его когерентности с реестром сотрудников Музея;
- ведение каталога внешних пользователей;
- ведение групп доступа пользователей;
- ведение реестра информационных ресурсов – объектов доступа;
- предоставление возможности Пользователям получать доступ к ресурсам;
- ведение маршрутов согласования заявок на доступ;
- осуществление согласования запросов на доступ;
- исполнение заявок на доступ: предоставление, изменение, отзыв, блокирование, разблокирование;
- смена пароля УЗ;
- контроль полного предоставленного доступа;
- формирование отчетности по операциям управления доступом;
- реализация функции однократного входа в ИС Музея (SSO);

Способ управления доступом в Музее по заявкам через корпоративный портал.

Принципы и технологии управления и предоставления доступа в Музее идентичны для всех видов информационных ресурсов.

4. Описание политики ИБ в отношении доменов

4.1. Защита персональных данных

Обеспечение защиты персональных данных в Музее осуществляется с целью выполнения требований российского законодательства, регламентирующего порядок обработки персональных данных и обеспечение их защиты.

Вопросы обработки и защиты персональных данных в Музее регламентируются локальными нормативными правовыми актами и документами Музея по вопросам обработки персональных данных.

Подсистемы КСИБ, входящие в СЗ ПДн, реализуют политики защиты информации, адекватные угрозам безопасности информации в Музее.

4.2.Безопасность корпоративной информационной сети

Под корпоративной информационной сетью понимают совокупность серверной ИТ- инфраструктуры Музея, сети обмена данных (ядро, сеть распределения), обще инфраструктурных ИТ-сервисов (коммутация, маршрутизация, корпоративный домен AD, DNS, WINS, NTP, СРК, ВРМП и проч.), инфраструктуры КСИБ.

Аппаратные компоненты корпоративной информационной сети размещаются в контролируемой зоне Музея, исключительно в серверных и кроссовых помещениях Музея. В Музее организован пропускной режим, используется СКУД для управления доступом, система видеонаблюдения. Серверные аппаратные средства размещаются в запираемых шкафах. Обеспечиваются нормальные климатические условия эксплуатации серверных компонентов корпоративной информационной сети.

В корпоративную информационную сеть входят компоненты Музея, а также региональных филиалов. Защита трафика при взаимодействии с региональными филиалами осуществляется при помощи VPN.

4.2.1. Обеспечение информационной безопасности на сетевом уровне

При планировании и построении сети осуществляется ее зонирование с учетом защиты информации. Зонирование осуществляется при планировании IP-пространства и выделении VLAN (*Virtual Local Area Network*) — виртуальная локальная компьютерная сеть. Представляет собой группу хостов с общим набором требований).

Корпоративная сеть отделена от сети общего доступа (Интернет) при помощи межсетевого экрана (программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами). Сеть Музея делится на следующие основные функциональные сегменты:

- DMZ-сегмент (демилитаризованная зона, ДМЗ) — сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных), в котором размещаются ИР, к которым может быть организован доступ из сети интернет. Данный сегмент, в свою очередь, делится на зоны по функциональному назначению;
- внутренний серверный сегмент, в котором размещаются серверные компоненты ИС Музея, а также размещаются различные производственные ИС и базы данных;
- пользовательский сегмент, в котором размещаются АРМП конечных Пользователей, работающих в рамках корпоративной сети Музея;
- Пользователей по радиоканалу с разделением сетей;

- сегмент управления, который обеспечивает доступ к интерфейсам управления компонентов ИТ-инфраструктуры и ИС;
- сегмент ИБ, в котором размещаются серверные компоненты КСИБ.

Взаимодействие сетей и VLAN, фильтрация трафика осуществляются на межсетевом экране ядра. Правила межсетевого экранирования формируются на базе политик информационной безопасности и технологии взаимодействия ИС в информационной среде Музея. Политика безопасности по умолчанию – всем все запрещено, что явно не разрешено – запрещено.

В сети осуществляется натирование (от англ. *Network Address Translation* — «преобразование сетевых адресов) сетевых адресов и проксирование (технология, в которой сервер позволяет клиентам выполнять косвенные запросы к другим сетевым службам) доступа, что обеспечивает сокрытие структуры и реальных IP-адресов при доступе из Интернет.

Взаимодействие с региональными филиалами осуществляется путем организации VPN-соединения по схеме сайт-сайт.

Все компоненты сети настроены и автоматически контролируются с точки зрения информационной безопасности, при этом:

- проводится инвентаризация сетевых ресурсов, хостов, портов, протоколов;
- выявляются уязвимости хостов;
- контролируется наличие небезопасных настроек и конфигураций.

Все компоненты сети настроены для централизованного сбора событий безопасности с передачей их в Систему мониторинга событий и расследования инцидентов ИБ. Указанные события протоколируются, нормализуются, коррелируются, сопоставляются с журналами мониторинга защищенности и при выявлении аномалий формируются инциденты ИБ.

Управление сетью осуществляется из выделенной подсети с контролем администраторов.

4.3 Безопасность электронной почты

В Музее функционирует система корпоративной электронной почты. Основными доменами являются arts-museum.ru/pushkinmuseum.art. В Музее возможно создание отдельных почтовых доменов, необходимых для функционирования отдельных продуктовых направлений.

Детализированные требования по использованию электронной почты в Музее содержатся в документе «Информационно-технический регламент Музея».

Все почтовые ящики в Музее персонализированы за исключением служебных (технологических) и маркетинговых почтовых ящиков.

Доступ к почте возможен только для пользователей, аутентифицированных в корпоративном домене AD Музея.

Подключение внутренних пользователей к почте допускается только с использованием защищенных протоколов.

Для защиты почты используются цифровые сертификаты.

Вся переписка со служебных адресов является собственностью Музея. Музей оставляет за собой право проверять весь почтовый трафик. Весь почтовый трафик протоколируется на шлюзах, на серверах Exchange дополнительно включается система трэкинга писем.

Входящие почтовые сообщения проверяются антивирусной и антиспам системами. Сообщения, содержащие вредоносное ПО, спам-сообщения, рекламу, недопустимый контент - блокируются. Сообщения, содержащие зашифрованные архивы, которые невозможно проверить, блокируются. Антиспам система проверят почтовое сообщение на предмет:

- наличия PTR и SPF записи для хоста отправителя;
- наличия динамического адреса отправителя;
- соответствия текста сообщения признакам спама;
- корректности сформированных заголовков письма;
- нахождению адреса отправителя в черных списках.

Каждому признаку назначается свой вес, при достижении суммы весов больше критического письмо может быть отфильтровано на АРМП пользователя настройками почтового клиента. Антиспам и антивирусные базы обновляются регулярно, по мере выпуска обновлений производителем соответствующих систем.

Для всех почтовых серверов производится еженедельное резервное копирование, с возможностью восстановления как сервиса в целом, так и отдельных почтовых ящиков.

На почтовом сервере блокируются небезопасные сервисы POP3 и IMAP. На всех шлюзах блокируется функция relay для учетных записей, не прошедших аутентификацию.

4.4 Безопасность информационных систем Музея

Для реализации бизнес-процессов в Музее используются внутренние информационные системы (ИС). В данных ИС обрабатывается как открытая

информация, так и КИ, КТ, ПДн. В ИС не обрабатываются сведения, составляющие государственную тайну.

ИС размещаются в корпоративной сети Музея. Большинство ИС размещается в виде виртуальных машин в корпоративном пространстве виртуализации.

ИС тесно интегрированы друг с другом и с корпоративным порталом.

Доступ к ИС предоставляется только для идентифицированных и аутентифицированных внутренних Пользователей Музея. Доступ внешних Пользователей к ИС Музея предоставляется в рамках договорных (или иных) отношений Контрагента с Музеем.

Доступ к ИС Музея осуществляется на базе смешанной (ролевой и мандатной) модели доступа, когда полномочия определяют право пользователя на доступ и выполнение определенных операций в системе, но при этом есть возможность предоставления доступа к отдельным объектам данных (документам, операциям и проч.).

Идентификация и аутентификация пользователей для доступа к ИС может осуществляться одним из способов: по логину и паролю, с использованием мультифакторной аутентификации.

Доступ к ИС из внешних сетей предоставляется внутренним Пользователям при подключении по VPN. Доступ внешних ИТ Подрядчиков к ИС Музея предоставляется в рамках договорных (или иных) отношений И Т Подрядчика с Музеем.

4.5 Безопасность WiFi

В помещениях Музея для подключения мобильных АРМП используется корпоративная сеть WiFi. При построении WiFi сети должны быть реализованы следующие принципы обеспечения информационной безопасности:

- в Музее разворачиваются сети WiFi для корпоративного и гостевого доступа. WiFi сеть Музея является защищенной беспроводной сетью;
- гостевой доступ допускается только в интернет в контролируемом режиме, трафик контролируется. Местоположение абонентского оборудования на территории Музея контролируется;
- доступ корпоративных пользователей в сеть через WiFi допускается с ограничениями: запрещен доступ в защищенный аттестованный сегмент для работы с сетями заказчиков;
- любая передача данных в сети WiFi шифруется. Для аутентификации и авторизации пользователей и сети используется SSID, WPA2-PSK, WPA3 и другие защищенные протоколы;

- настройка АРМП для WiFi доступа осуществляется сотрудником ИТ службы;

5. Лицензионная политика в отношении программного обеспечения

В целях обеспечения лицензионной чистоты ПО, устанавливаемого в Музее, обеспечивается:

- сотрудникам следует использовать только ПО, установленное с комплектов дистрибутивов, полученных Музеем из легальных источников: от производителя ПО или официальных дистрибуторов;
- для инсталляции / активации ПО необходимо использовать действующие лицензии или номера корпоративных лицензий на ПО, полученные Музеем от производителя ПО или официальных дистрибуторов;
- в случае инсталляции ПО с использованием номера корпоративной лицензии - уведомлять сотрудников ИТ-службы с целью учета количества используемых лицензий на ПО
- Музей оставляет за собой право защищать свою репутацию и свои инвестиции в ПО, используя внутренние средства контроля за использованием ПО, для предотвращения создания, установки и использования сотрудниками Музея неправомочных (нелегальных) копий ПО.

6. Описание обязанностей

Положения настоящей Политики являются обязательными для выполнения всеми сотрудниками во всех подразделениях Музея. Настоящая политика является базовым документом для разработки последующих документов, регламентирующих вопросы управления ИТ и ИБ в Музее.

Ниже определена ответственность подразделений и сотрудников Музея в части исполнения настоящей Политики.

ИТ служба отвечает за:

- проектирование, построение и развитие ИТ-инфраструктуры Музея с учетом исполнения положений настоящей Политики;
- обеспечение функционирования ИТ-инфраструктуры с учетом исполнения положений настоящей Политики;
- обеспечение поддержки Пользователей Музея с учетом исполнения положений настоящей Политики;
- обеспечение должного уровня подготовки системных администраторов и Пользователей Музея с учетом положений настоящей Политики;
- контроль действий системных администраторов с целью недопущения нарушений исполнения положений настоящей Политики;
- обеспечение бесперебойного функционирования ИТ-инфраструктуры,

используемой для функционирования КСИБ.

- проектирование, построение и развитие ИС Музея с учетом исполнения положений настоящей Политики;
- обеспечение функционирования ИС с учетом исполнения положений настоящей Политики;
- своевременное информирование ИТ-службы и ГИБ о фактах, которые могут рассматриваться как индикаторы компрометации ИС.
- проектирование, построение и развитие КСИБ в рамках ИТ-инфраструктуры Музея для реализации настоящей Политики;
- обеспечение функционирования, осуществление администрирование и эксплуатации КСИБ;
- обеспечение контроля защищенности и мониторинга событий ИБ с целью недопущения и выявления инцидентов ИБ, их расследования и совершенствования КСИБ;
- своевременное информирование ОЭВСиС о выявленных недостатках ИТ и ИС с целью их устранения;
- проведение расследований инцидентов ИБ по поручению руководства Музея;
- контроль действий системных администраторов с точки зрения выполнения настоящей Политики при изменении конфигурации ИТ-инфраструктуры и ИС;
- контроль модернизируемого ПО на предмет выявления критических уязвимостей;
- периодический контроль надежности функционирования КСИБ;
- своевременное информирование руководства ИТ-службы о выявленных инцидентах ИБ;
- обеспечение должного уровня подготовки своих сотрудников (в том числе прохождение обучения и сертификации по продуктам КСИБ) для обеспечения поддержки Пользователей с учетом требований настоящей Политики;
- осуществление поддержки Пользователей с учетом требований настоящей Политики.

Ответственные за информационную безопасность обязаны:

- периодически производить проверку надежности КСИБ, а также

компонентов ИТ-инфраструктуры и ИС с точки зрения реализации требований настоящей Политики;

- инициировать экстренную блокировку доступов, учетных записей, разрешений на межсетевых экранах, ключей и сертификатов в случае выявления их компрометации или атак на ИТ- инфраструктуру и ИС Музея;

- выходить на руководство Музея с предложениями по совершенствованию КСИБ;

- осуществлять развитие и совершенствование КСИБ в рамках выделенного бюджета ИБ.

Владельцы ИС (начальники структурных подразделений ИТ службы) несут ответственность за:

- согласование доступа Пользователей к своим ИС с учетом требований по информационной безопасности, исключение избыточности доступа к информации, которая не требуется Пользователям в рамках решаемых ими задач;

- обеспечение поддержки и развития ИС с учетом требований по ИБ, изложенных в нормативных документах Музея.

Руководители других структурных подразделений несут ответственность за:

- исполнение своими подчиненными требований нормативных документов Музея по вопросам обеспечения ИБ;

- согласование доступа своих сотрудников к ИР Музея с учетом требований нормативных документов Музея.

Внутренние и внешние пользователи отвечают за:

- соблюдение обязательств, принятых на себя в рамках соглашений, регулирующих правоотношения с Музеем;

- соблюдение положений внутренних локально-нормативных актов Музея, а также норм действующего законодательства РФ.

Пользователи обязаны:

- знать и соблюдать нормативные документы и процедуры, принятые в Музее для обеспечения информационной безопасности;

- использовать по назначению средства защиты информации, установленные на АРМП

- не записывать пароли и PIN–коды на бумаге, не хранить их в открытом (явном) доступе в текстовых или иных документах, не сообщать их другим лицам;

- незамедлительно информировать работников ИТ службы о событиях, позволяющих предположить компрометацию учетных данных, АРМП или информационных систем Музея;

- работать, используя только свою аутентификационную информацию. Работа от имени других пользователей категорически запрещается;

- использовать почту Музея в соответствии с Информационно-техническим регламентом Музея»;

6.1.Ответственность за нарушение правил ИБ в Музее

Пользователи несут ответственность за нарушение правил информационной безопасности. В зависимости от типа Пользователя, типа нарушения, масштаба и тяжести последствий, ответственность может быть дисциплинарной, гражданской, административной и уголовной. Ответственность может наступать как за преднамеренные, так и за непреднамеренные (случайные) действия или бездействие, если недопустимость таких действий (бездействия) явно указана в действующем законодательстве РФ или/и локально-нормативных актах Музея.

Ответственность несут как внутренние Пользователи Музея, так и внешние Пользователи, которым легитимным образом предоставлен доступ к ИТ-инфраструктуре и информационным ресурсам Музея.

Ответственность за локальное хранение рабочей документации возлагается на пользователя. Музей не несет ответственности за утерю данных, находящихся на локальных дисках АРМП. Всю рабочую документацию необходимо хранить на сетевых ресурсах Музея (общих папках).

Пользователи несут ответственность за:

- разглашение сведений, составляющих персональные данные, а также другие виды защищаемой в Музее информации, в соответствии с локальными нормативными правовыми актами и документами Музея по вопросам обработки персональных данных, заключенными соглашениями о неразглашении конфиденциальной информации и другими документами, в том числе, но не ограничиваясь: должностной инструкцией, трудовым договором, договором гражданско-правового характера и прочее;

- нарушение действующего законодательства РФ или/и внутренних

нормативных документов Музея, регламентирующих вопросы информационной безопасности;

- осуществление (или способствование) компьютерным атакам на ИТ-инфраструктуру и ИС Музея или ее Контрагентов.

Настоящая Политика вступает в силу с момента утверждения директором Музея и действует до даты ее отмены, изменения или утверждения в новой редакции.

Приложение №1
к Политике информационной безопасности

Требования по Информационной безопасности к Контрагента Музея (Внешним ИТ-подрядчикам) при удаленном доступе к информационным системам Музея

1. Доступ к информационным системам Музея осуществляется через vpn канал, настроенный на оборудовании Музея. Параметры подключения к vpn каналу – учетная запись, адрес входа, предоставляются ИТ подрядчику. Учетная запись ИТ подрядчика имеет доступ только к тем системам и информационным ресурсам, которые необходимы для выполнения текущих работ. Музей вправе использовать механизмы двухфакторной аутентификации при подключении к корпоративной сети и/или при авторизации в корпоративных системах музея для ИТ подрядчиков.

2. Параметры подключения к vpn каналу Музея являются конфиденциальной информацией. Запрещается передавать параметры подключения к vpn каналу Музея третьим лицам. В случае компрометации ИТ подрядчиком учетной записи vpn канала, ИТ подрядчик в течении одного рабочего дня обязан сообщить об этом представителю Музея, для блокировки учетной записи vpn канала.

3. Все средства вычислительной техники ИТ подрядчика, с которой осуществляется доступ к информационным системам Музея должны быть оснащены средствами защиты информации, в том числе средствами антивирусной защиты, современным программным обеспечением, должны устанавливаться актуальные обновления безопасности на операционные системы и программное обеспечение.

4. Работники ИТ подрядчика, осуществляющие администрирование информационных системам Музея обязаны подключаться к vpn каналу Музея используя исключительно средства вычислительной техники ИТ подрядчика.

5. ИТ подрядчик должен организовать доступ средств вычислительной техники к сети Интернет через защищенные сети, находящиеся на территории Российской Федерации.

6. ИТ подрядчик обязан провести инструктаж/обучение работников, осуществляющих удаленный доступ к информационным системам Музея о правилах безопасного удаленного взаимодействия с такими объектами.

7. ИТ подрядчик должен обеспечивать оперативное реагирование и принятие мер защиты информации при возникновении компьютерных инцидентов.