УТВЕРЖДЕНА
приказом по ГБУК РО
«Ростовский областной музей
изобразительных искусств»
№ 10 от 05.02.2020

ИНСТРУКЦИЯ
пользователя по работе с персональными данными

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет общие правила работы сотрудников государственного бюджетного учреждения культуры Ростовской области «Ростовский областной музей изобразительных искусств» (далее по тексту – Музей) с персональными данными.

1.2. Персональные данные в электронном виде обрабатываются в информационных системах персональных данных. Также устанавливается особый порядок обработки и хранения персональных данных, содержащихся на бумажных носителях.

1.3. Пользователем является каждый сотрудник Музея, участвующий в рамках своих функциональных обязанностей в процессах как автоматизированной обработки, так и обработки без использования средств автоматизации персональных данных, а также имеющий доступ к аппаратным средствам, программному обеспечению, носителям информации и средствам защиты.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, Правилами обработки персональных данных, законами и нормативными актами, а также нормативными документами Музея, регламентирующими обработку персональных данных.

1.5. Методическое руководство по работе пользователя осуществляет ответственный за организацию обработки персональных данных.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

2.3. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.4. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.5. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

2.7. Автоматизированное рабочее место (АРМ) – программно-технический комплекс, посредством которого пользователь выполняет свои должностные обязанности (персональный компьютер, ноутбук, терминал и т.п.)

2.8. Несанкционированный доступ (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

2.9. Посторонние лица – лица, которые не имеют права самостоятельного доступа в ИСПДн и (или) не имеют доступа к персональным данным.

2.10. Средство защиты информации от несанкционированного доступа (СЗИ от НСД) – программное, техническое или программно-техническое средство, направленное на предотвращение или существенное затруднение несанкционированного доступа к информации.

3. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

3.1. Не разглашать персональные данные, которые будут доверены или станут известны в ходе рабочего процесса во время выполнения должностных (договорных) обязанностей.

3.2. Не сообщать устно или письменно, не передавать в каком-либо виде третьим лицам и не раскрывать публично персональные данные за исключением случаев, предусмотренных законодательством РФ.

3.3. Знать и выполнять требования законодательных актов Российской Федерации, настоящей Инструкции и других внутренних документов, регламентирующих порядок обработки персональных данных.

3.4. Выполнять на АРМ только те процедуры обработки персональных данных, которые определены должностной инструкцией.

3.5. Знать и соблюдать установленные требования обработки персональных данных, по учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных.

3.6. Использовать для хранения персональных данных только определенные места хранения и учтенные носители персональных данных.

3.7. Незамедлительно, в кратчайшие сроки, сообщать руководителю об утрате или недостаче носителей информации, удостоверений, пропусков,

ключей от помещений, хранилищ, сейфов и о других фактах, которые могут привести к разглашению персональных данных.

3.8. Пользователи, имеющие выход в Интернет, обязаны соблюдать правила при работе в сетях связи общего пользования и (или) сетях международного информационного обмена.

3.9. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами.

3.10. Обо всех выявленных нарушениях, связанных с порядком обработки персональных данных, необходимо обращаться к ответственному за организацию обработки персональных данных.

3.11. **Пользователям запрещается:**

3.11.1. Нарушать установленные в Музее инструкции по работе с персональными данными.

3.11.2. Использовать компоненты программного и аппаратного обеспечения Музея в неслужебных целях.

3.11.3. Оставлять свое рабочее место без присмотра, предварительно не заблокировав (при помощи штатных средств защиты информации от несанкционированного доступа).

3.11.4. Оставлять без присмотра или неубранными в хранилища (шкаф, сейф) носители или документы, содержащие персональные данные.

3.11.5. Записывать и хранить персональные данные на неучтенных носителях информации (оптических дисках, гибких магнитных дисках, флешнакопителях и т.п.)

3.11.6. Самовольно изменять состав и конфигурацию используемых программных, аппаратных, программно-аппаратных средств, самовольно устанавливать программное обеспечение, отключать/подключать оборудование или изменять режимы его работы.

3.11.7. Самовольно подключать АРМ или другие средства, изменять IP-адрес, MAC-адрес и иные настройки сети АРМ.

3.11.8. Производить действия, направленные на получение несанкционированного доступа к АРМ и серверам, в том числе:

- действия, направленные на нарушение нормального функционирования элементов сети (компьютеров, другого сетевого оборудования или программного обеспечения);
- установка программного обеспечения, осуществляющего перехват информации, адресованной другим пользователям;
- действия, направленные на получение несанкционированного доступа к информационным ресурсам, в последующем использовании такого доступа;
- уничтожение, модификация программного обеспечения или данных без согласования с директором или владельцем этого ресурса;
- попытка подбора паролей к любым информационным ресурсам методом перебора всех возможных вариантов паролей;
- умышленные действия по созданию, использованию и распространению вредоносных программ, в том числе направленных на

получение несанкционированного доступа к любым информационным и служебным ресурсам, либо на нарушение целостности и работоспособности этих систем;

- действия по сканированию локальной сети с целью определения её внутренней структуры, списков открытых портов, наличия существующих сервисов и уязвимостей.

3.11.9. Самовольно изменять параметры средств защиты информации (в том числе и средств антивирусной защиты), а также завершать их работу и (или) самостоятельно их устанавливать.

3.11.10. Самостоятельно разрабатывать или использовать нерегламентированные программы.

3.11.11. Разрешать посторонним лицам работать под своей учетной записью в ИСПДн.

3.11.12. Пересылать персональные данные по каналам связи в открытом виде, в том числе Интернет, по телефону, факсу, электронной почте и т.п. (без использования средств шифрования).

3.11.13. Получать доступ к персональным данным с рабочих мест, не оборудованных необходимыми средствами защиты информации.

3.11.14. Самовольно создавать совместно используемые сетевые ресурсы (папки общего доступа) на своих компьютерах и файловых серверах, несанкционированно удалять или изменять права доступа к ним.

3.11.15. В случае возникновения любых механических неисправностей в оборудовании осуществлять самостоятельные попытки их устранения.

3.11.16. Препятствовать должностным лицам при проведении проверок и служебных расследований, связанных с обеспечением безопасности информации.

3.11.17. Удалять или искажать программы и файлы с персональными данными и иной важной информацией (например, системной, необходимой для функционирования ИСПДн).

3.11.18. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению внештатной ситуации. Об обнаружении такого рода ошибок – ставить в известность руководителя своего подразделения и сотрудников, ответственных за установку и (или) сопровождение программного обеспечения.

3.11.19. Подключать к ЛВС Музея личные средства вычислительной техники: ноутбуки, карманные компьютеры, смартфоны и т.п., а также личные носители и накопители информации. В случае необходимости переноса информации с личных носителей информации обращаться к ответственным.

4. ПАРОЛЬНАЯ ПОЛИТИКА

4.1. Общие требования к паролям:

- Минимальное требование: буквенно-цифровой пароль. Желательно использовать буквы в верхнем или нижнем регистрах, цифры или специальные символы.

- Минимальная длина пароля – не менее 6 (шести) символов.

- Максимальный срок действия пароля – 90 суток.

- Запрет использования трех ранее использовавшихся паролей.

- Пароль Пользователя не должен включать в себя легко вычисляемые сочетания символов, общепринятые сокращения, имена, фамилии, должности, год рождения, номер паспорта, табельный номер, иную информацию о Пользователе, доступную другим лицам.

- Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

- Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567, qwerty и т.п.)

4.2. Правила использования паролей:

- Хранить в тайне свой пароль, не сообщать его другим лицам.

- Не предоставлять доступ в ИСПДн другим лицам под своей учетной записью и паролем.

- Изменять свой пароль при первом требовании политики паролей операционной системы и/или ИСПДн.

- Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.)

- Запрещается записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе АРМ, на обратной стороне клавиатуры и т.д.

- Запрещается хранить пароли в записанном виде на отдельных листах бумаги.

4.3. Смена, удаление личного пароля любого пользователя производится в следующих случаях:

- в случае подозрения на компрометацию пароля;

- по окончании срока действия;

- в случае прекращения полномочий (увольнение, переход на другую работу внутри Музея) Пользователя после окончания последнего сеанса работы в информационных системах персональных данных;

- по указанию ответственного за организацию обработки персональных данных;

- при увольнении, переходе на новую должность сотрудника, имеющего доступ помимо своей учетной записи к другим ресурсам (межсетевые экраны, серверы, другие учетные записи и т.п.) также производится внеплановая смена паролей к таким ресурсам.

5. АНТИВИРУСНАЯ ЗАЩИТА

5.1. В случае отсутствия штатных функций антивирусной программы, предусматривающих автоматическую проверку файлов, Пользователь обязан осуществлять проверку файлов, получаемых:

- по электронной почте;
- через сеть Интернет;
- на магнитном, оптическом диске, флеш-накопителе;
- ином съемном носителе информации;
- полученных иным способом.

5.2. Перед открытием вложения (ссылок) убедиться в том, что отправитель действительно послал вам этот файл, даже если он и должен был это сделать. Позвоните ему сами. Не доверяйте имени отправителя и указанным в тексте письма номерам телефонов, а также лицам, позвонившим вам самостоятельно с просьбой открыть файлы и пройти по ссылкам.

5.3. При возникновении подозрений в отправителе либо при одном из следующих форматов файла запрещается его открывать: .exe, .pif, .application, .gadget, .msi, .msp, .com, .scr, .hta, .cpl, .msc, .jar, .bat, .cmd, .js, .psi, .ws, .scr, .lnk, .inf, .reg.

5.4. Пользователю запрещается:

5.4.1. Осуществлять действия, направленные на выключение антивирусной программы.

5.4.2. Самостоятельно устанавливать на АРМ программное обеспечение.

5.4.3. Запускать файлы, полученные по сетям связи (электронная почта, Интернет), со съемных носителей, даже если они получены у проверенного адресата, без предварительной их проверки антивирусной программой.

5.4.4. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) Пользователь самостоятельно или вместе с ответственным (специалистом по защите информации) должен провести внеочередной антивирусный контроль своего рабочего места.

5.4.5. В случае обнаружения при проведении антивирусной проверки вирусного заражения Пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения вирусного заражения ответственного (специалиста по защите информации);
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

6. ПОРЯДОК РАБОТЫ В ИСПДн И СЕТИ ИНТЕРНЕТ

6.1. Подключение к ИСПДн и сети Интернет:

6.1.1. Целью работы Пользователя в ИСПДн и сети Интернет является сбор, обработка, хранение персональных данных, обмен электронными сообщениями в служебных целях.

6.1.2. Доступ в ИСПДн и сети Интернет предоставляется Пользователям только в том случае, если это не противоречит требованиям настоящей Инструкции и иных нормативных документов в области защиты информации.

6.1.3. Доступ Пользователя в ИСПДн для обработки персональных данных производится только с рабочих мест, на которых установлены средства защиты информации.

6.1.4. Основанием для подключения сотрудника Музея к ИСПДн и сети Интернет является мотивированная заявка ответственному за организацию обработки персональных данных от непосредственного руководителя Пользователя с указанием полномочий доступа к таким ресурсам и сервисам.

6.1.5. Ответственный за организацию обработки персональных данных, либо сотрудник, выполняющий его функции, организует подключение к ИСПДн или сети Интернет Пользователей в установленном порядке, осуществляет контроль над использованием данных ресурсов и сервисов.

6.1.6. Основанием для отключения Пользователя от ИСПДн и сети Интернет являются следующие события:

- нарушение инструкции и иных локальных нормативных актов в области защиты информации Музея;
- увольнение Пользователя, либо перевод его в другое подразделение.

6.2. Порядок работы в сети Интернет:

6.2.1. Использование сотрудниками Музея сети Интернет должно осуществляться исключительно для выполнения должностных обязанностей.

6.2.2. Информация, образованная (образующаяся) в процессе трудовой деятельности работника Музея является собственностью Музея и не подлежит использованию (в том числе использованию в сети Интернет или с помощью сети Интернет) в личных целях и (или) в корыстных интересах других лиц (организаций).

6.2.3. При проведении технических работ, связанных с настройкой оборудования, в случае обнаружения попыток несанкционированного доступа к Интернет-шлюзу, АРМ Пользователей может проводиться временное отключение Пользователей от сервисов сети Интернет.

6.2.4. При работе в сети Интернет Пользователям запрещается:

- умышленное распространение и получение материалов в/из сети Интернет, противоречащих законодательству Российской Федерации, в том числе материалов, пропагандирующих насилие или экстремизм, разжигающих расовую, национальную или религиозную вражду, разъясняющих порядок изготовления и/или применения наркотиков, взрывчатых веществ, оружия и т.п., материалов порнографического характера, компьютерных вирусов и других вредоносных программ;
- передавать в сеть Интернет информацию, к которой в соответствии с законодательством ограничен доступ (персональные данные, служебная информация) без соответствующего разрешения;

- предоставлять доступ в сеть Интернет со своего АРМ кому-либо, в том числе программно-техническими способами через локальную вычислительную сеть Музея (например, путем несанкционированной установки локального Интернет-шлюза на рабочее место);

- осуществлять несанкционированный доступ к ресурсам и сервисам сети Интернет;

- выполнять действия, направленные на нарушение функционирования элементов сети Интернет (коммуникационного оборудования, серверов, рабочих станций, программного обеспечения).

6.3. Правила работы Пользователей с электронной почтой:

6.3.1. Пользователи обязаны использовать электронную почту только для выполнения служебных обязанностей.

6.3.2. Запрещается отправлять файлы, содержащие персональные данные в открытом виде (не зашифрованные).

6.3.3. Запрещается использовать не свой обратный адрес при отправке электронной почты.

6.3.4. Корпоративные рекомендации использования электронной почты:

- Вы должны оказывать то же уважение, что и при устном общении.
- Вы должны проверять правописание, грамматику и дважды перечитывать свое сообщение перед отравлением.
- Вы не должны участвовать в рассылке посланий, пересылаемых по цепочке (чаще всего это письма религиозно-мистического, развлекательного содержания).
- Вы не должны по собственной инициативе пересылать по произвольным адресам незатребованную информацию.
- Вы не должны рассылать сообщения, которые являются зловредными, раздражающими или содержащими угрозы другим пользователям.
- Вы не должны отправлять никаких сообщений противозаконного или неэтичного содержания.
- Вы должны помнить, что электронное послание является эквивалентом почтовой открытки и не должно использоваться для пересылки персональных данных без использования средств защиты (шифрование).
- Вы не должны использовать корпоративную электронную почту для посланий личного характера.

7. ПОРЯДОК РАБОТЫ СО СЪЕМНЫМИ НОСИТЕЛЯМИ ИНФОРМАЦИИ

7.1. Под использованием носителей информации в ИСПДн понимается их подключение к инфраструктуре ИСПДн с целью обработки, приема/передачи информации между информационными системами и носителями информации.

7.2. Допускается использование только учтенных носителей информации, которые являются собственностью Музея.

7.3. Возможность подключения носителей информации, а также получение учтенных носителей информации предоставляется Пользователям по инициативе руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;

- возникновения у Пользователя служебной необходимости.

7.4. При использовании носителей информации необходимо:

- использовать носители информации исключительно для выполнения своих служебных обязанностей;

- бережно относиться к носителям персональных данных;

- обеспечивать физическую безопасность носителей информации всеми разумными способами;

- извещать ответственного за организацию обработки персональных данных о фактах утраты (кражи) носителей информации.

7.5. При использовании носителей персональных данных запрещено:

- использовать носители персональных данных в личных целях;

- передавать носители персональных данных другим лицам;

- хранить съемные носители с персональными данными на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

- выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому и т.п.

7.6. Любое взаимодействие (обработка, прием/передача информации), инициированное Пользователем между информационной системой и неучтенными (личными) носителями информации, рассматривается как несанкционированное.

7.7. В случае выявления фактов несанкционированного и/или нецелевого использования носителей информации инициируется служебная проверка, проводимая комиссией, состав которой определяется ответственным за организацию обработки персональных данных. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю структурного подразделения для принятия мер.

7.8. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные.

7.9. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

7.10. Съемные носители персональных данных, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с персональными данными осуществляется комиссией, состав которой определяется ответственным за организацию обработки персональных данных. По результатам уничтожения носителей составляется акт.

7.11. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители персональных данных изымаются и делаются соответствующие пометки в журнале учета машинных носителей.

8. ПРАВА ПОЛЬЗОВАТЕЛЯ

8.1. Использовать ИСПДн Музея для выполнения должностных обязанностей.

8.2. Обращаться к ответственному за организацию обработки персональных данных для консультаций по поводу использования программного обеспечения и АРМ, по вопросам обработки персональных данных.

8.3. Направлять предложения по установке новых версий существующего программного обеспечения (с обоснованием необходимости замены старых версий на новые).

8.4. Направлять предложения по модернизации АРМ (замены на новые аналоги) с обязательным обоснованием замены и указанием преимуществ перед существующими аналогами.

8.5. Получать консультации и разъяснения по нормативным документам, регламентирующим работу с персональными данными в Музее.

9. ОТВЕТСТВЕННОСТЬ

9.1. Пользователь несет персональную ответственность за свои действия или бездействие, которые могут повлечь за собой разглашение персональных данных, а также за нарушение нормального функционирования ИСПДн или их отдельных компонентов, несанкционированный доступ к информации в соответствии с законодательством Российской Федерации.