УТВЕРЖДАЮ: директор МБУК
Дома культуры имени В.П. Ногина
_____ Д.В. Рачков
Приказ от 29 декабря 2018 г. № 70

И Н С Т Р У К Ц И Я
пользователя информационных систем персональных данных МБУК Дом культуры имени В.П. Ногина

1. Общие положения.

1.1. Пользователь информационных систем персональных данных (ИСПДн) (далее-Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.2. Пользователь является каждый сотрудник учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами РФ и регламентирующими документами учреждения.

1.5. Методическон руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2. Должностные обязанности.

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных актов , а также внутренних инструкций руководства по защите информации и распоряжений, регламентирующих порядок действий по защите персональных данных.

2.2. Выполнять на автоматизированном рабочем месте(АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики.

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешены (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью, в а также для получения консультаций по вопросам информационной безопасности, необходимо обратиться в администрации. Учреждения по электронной почте или по телефону, указанным на официальном сайте.

2.8. Для получения консультаций по вопросам настройки и работы элементов ИСПДн необходимо обращаться к Администратору ИСПДн.

2.9. Пользователям запрещается:

- разглашать защищаемую информацию третьим лицам;
- копировать защищаемую информацию на внешние носители без разрешения своего руководства;
- самостоятельно устанавливать, тиражировать, или модефицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к папкам на своей рабочей станции;
- запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;
- сообщать (или передавать) посторонним лицам личные ключи к атрибутам доступа к ресурсам ИСПДн;
- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.10. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию «Блокировка».

2.11. Принимать меры по реагированию в случае возникновения нештатных и аварийных ситуаций, с целью ликвидации их последствий в пределах возложенных на него функций.

3. Организация парольной защиты.

3.1. Личные пароли доступа к элементам ИСПДн выдаются пользователем Администратором информационной безопасности, Администратором ИСПДн или создаются самостоятельно.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в полгода.

3.3.Правила формирования пароля:

- пароль не сможет содержать имя учетной записи пользователя или какую-либо его часть;
- пароль должен состоять не менее чем из 8 символов;
- в пароле должны присутствовать символы трех категорий из числа следующих четырех:

1) прописные буквы английского алфавита от A до Z;
2) строчные буквы английского алфавита от a до z;
3) десятичные цифры (от 0 до 9);
4) символы, не принадлежащие алфавитно-цифровому набору (например, ! &, ?, %) и т.д.;

- запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123у», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, на основании информации о пользователе;
- 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 и т.п.)
- запрещается выбирать пароли, которые уже использовались ранее.

3.4. Правила ввода пароля:

- запрещается записывать пароль на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
- запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.6. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;
-своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Правила работы в сетях общего доступа и (или) международного обмена.

4.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее-Сеть), на элементах ИСПДн, должна проводиться при служебной необходимости.

4.2. При работе в сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус и других);
- передавать по сети запрещенную информацию без использования средств шифрования;
- запрещается скачивать из сети программное обеспечение и другие файлы;

- запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое ПО и другие;
- запрещается нецелевое использование подключение к Сети.

5. Права и ответственность пользователей ИСПДн

5.1. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

5.2. Пользователи, виновные в несоблюдении Настоящей Инструкции, расцениваются как нарушит ели Федерального закона РФ 27.07.2006г. № 152-ФЗ «О персональных данных» и несут гражданскую, административную и уголовную ответственность в пределах, предусмотренных действующим законодательством Российской Федерации.