Приложение №6__
к Приказу от «16» декабря 2025 г.№315

У Т В Е Р Ж Д А Ю

Директор
Муниципального учреждения
«Дом культуры «Матыра»
_____ Л.Л. Черепахина
«16» декабря 2025 г.

МП

ИНСТРУКЦИЯ

пользователя по обеспечению информационной безопасности

Липецк 2025

Термины, определения и сокращения

Автоматизированная система (АС) – Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (Межгосударственный стандарт ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Автоматизированное рабочее место (АРМ) – программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида (Межгосударственный стандарт ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Администратор безопасности – лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Безопасность информации [данных] – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами и системами или в защищаемых помещениях (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Защита информации от несанкционированного доступа (ЗИ от НСД) – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Защита информации от разглашения – защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Носитель защищаемой информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Носитель информации (НИ) – материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин ("Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008)).

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Персональные данные, разрешенные субъектом персональных данных для распространения – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Система защиты информации (СЗИ) – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Средство защиты информации (СрЗИ) – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

1. Общие положения

1.1. Настоящая инструкция разработана на основании следующих нормативных документов:

1.1.1. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

1.1.2. Федеральный закон от 27 июня 2006 № 152-ФЗ «О персональных данных»;

1.1.3. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

1.1.4. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

1.1.5. Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

1.2. Настоящая инструкция определяет основные задачи, функции, обязанности, права и ответственность пользователей по обеспечению безопасности в информационных системах (далее – Пользователь) МУ «ДК «Матыра» (далее – Организация).

1.3. Пользователями являются сотрудники МУ «ДК «Матыра» (далее-Организация), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной

2.10.6. Обрабатывать информацию с выключенным или нефункционирующими устройствами защиты информации.

2.10.7. Производить какие-либо изменения в электрических схемах, монтаже и размещении ОТСС и ВТСС.

2.10.8. Самостоятельно устанавливать, тиражировать или модифицировать ПО, изменять установленный алгоритм функционирования ОТСС и ВТСС.

2.10.9. Обрабатывать на ПЭВМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам обработки информации.

2.10.10. Сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам ПЭВМ.

2.10.11. Записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.

2.10.12. Работать на ПЭВМ при обнаружении каких-либо неисправностей.

2.10.13. Осуществлять электропитание и заземление ОТСС от нештатных сетей электропитания и заземления.

3.Идентификация и аутентификация пользователей

3.1.Настройки средств защиты от несанкционированного доступа должны осуществлять идентификацию и аутентификацию при доступе в ИС пользователей, являющихся работниками в Организации (внутренних пользователей), пользователей, не являющихся работниками оператора (внешних пользователей) и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

3.2.В качестве внутренних пользователей рассматриваются должностные лица (пользователи, администраторы), выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств ИС в соответствии с должностными регламентами (инструкциями) утвержденными Руководителем Организации и которым в ИС присвоены учетные записи, и, дополнительно, должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной ИС, а также лица, привлекаемые на договорной основе для обеспечения функционирования ИС (ремонт, гарантийное обслуживание, регламентные и иные работы) и которым в ИС также присвоены учетные записи.

3.3.К пользователям, не являющимся работникам оператора (внешним пользователям), относятся все остальные пользователи ИС, не указанные в качестве внутренних пользователей.

3.4.Пользователи ИС должны однозначно идентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до прохождения ими процедур идентификации и аутентификации.

3.5.Ответственность за создание, присвоение и уничтожение идентификаторов и средств аутентификации пользователей и устройств несет Администратор информационной безопасности. Администратор информационной безопасности проверяет на СВТ пользователя заданные возможности доступа и выдает пользователю под расписку в соответствующем журнале учета его персональный идентификатор.

3.5.Функционал, доступный до прохождения процедур идентификации и аутентификации

3.5.1.При предоставлении доступа к персональным данным и любой иной конфиденциальной информации пользователям запрещены любые действия до прохождения ими процедур идентификации и аутентификации.

3.5.2.При предоставлении пользователям доступа к общедоступной информации (веб-сайтам, порталам, иным общедоступным ресурсам) до прохождения процедур идентификации и аутентификации доступны функции чтения и копирования.

3.6.Пользователи ИС должны однозначно аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до прохождения ими процедур идентификации и аутентификации.

3.7. Аутентификация пользователей осуществляется с использованием паролей, аппаратных средств, или - определенной комбинации указанных средств.

3.8. Администратор информационной безопасности устанавливает и реализует следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств:

3.8.1. Владельцы паролей должны быть ознакомлены с требованиями к организации парольной защиты и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации (личный пароль пользователь не имеет права сообщать никому).

3.8.2.Внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, переход на другую работу внутри территориального органа) должна производиться Администратором информационной безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

3.9. Хранение пользователем значений своих паролей на бумажном носителе допускается только в личном опечатанном сейфе, либо в сейфе у ответственного за организацию обработки персональных данных.

4. Порядок подключения рабочих станций к сети общего пользования

4.1. Сеть общего пользования является открытой системой передачи данных, при работе в которой могут возникнуть следующие основные угрозы:

– заражение СВТ программными вирусами;

– внедрение программных закладок;

– загрузка трафика нежелательной корреспонденцией (спамом);

– несанкционированная передача конфиденциальной информации, в т.ч. ПДн пользователями ОИ в сети общего пользования.

4.2. Для предотвращения указанных угроз реализуется:

– разграничение доступа пользователей к ресурсам сетей путём использования средств межсетевого экранирования защищённого сегмента локальной вычислительной сети, в котором происходит обработка конфиденциальной информации, в т.ч. ПДн;

– осуществление контроля за конфиденциальной информацией, в т.ч. ПДн, выходящими из ОИ Организации в сети общего пользования;

– применение средств криптографической защиты информации при использовании сетей связи общего пользования для передачи конфиденциальной информации, в т.ч. ПДн.

4.3. Пользователям, рабочие станции которых подключены к сети общего пользования для доступа к ресурсам Интернет и электронной почты, разрешается использовать лишь те ресурсы, которые необходимы для выполнения их функциональных обязанностей.

4.4.Подключение рабочих станций пользователей Организации к сети общего пользования для доступа к ресурсам Интернет и электронной почты, осуществляется по решению директора.

4.5. После получения разрешения производится:

– установка и настройка необходимого программного обеспечения для доступа к ресурсам сетей общего пользования;

– конфигурирование системы контроля доступа в соответствии с политикой безопасности;

– присвоение пользователям персональных идентификаторов;

– выработка каждому пользователю пароля, при этом пароль должен быть индивидуален для каждого пользователя, быть трудно подбираемым и не сочетаться с именем пользователя.

5. Порядок применения средств антивирусной защиты информации

5.1. В организации обеспечивается антивирусная защита ИС, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной

информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

5.2. Средства антивирусной защиты информации должны устанавливаться на всех автоматизированных рабочих местах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), мобильных технических средствах и иных точках доступа ИС, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы).

5.3. Инсталляция и настройка средств антивирусной защиты информации осуществляются в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.

5.4. В ИС права по управлению (администрированию) средствами антивирусной защиты предоставляются только Администратору информационной безопасности информации.

5.5.Пользователям запрещается:

5.5.1 отключать средства антивирусной защиты информации во время работы;

5.5.2 без разрешения Администратора информационной безопасности копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

5.6.В случае появления подозрений на наличие программных вирусов в ЛВС пользователи должны немедленно проинформировать об этом Администратора информационной безопасности. В случае выявления инцидентов (фактов и т.п.), связанных со сбоями в работе средств антивирусной защиты, пользователь обязан незамедлительно сообщить об этом Администратору информационной безопасности

5.7. В случае обнаружения программных вирусов при входном контроле отчуждаемых носителей информации, файлов или почтовых сообщений пользователь должен:

5.7.1.приостановить процесс приема-передачи информации;

5.7.2.сообщить Администратору информационной безопасности о факте обнаружения программного вируса;

5.7.3.принять по согласованию с Администратором информационной безопасности меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации.

5.8.При обнаружении программных вирусов в процессе обработки информации пользователь обязан:

5.8.1.немедленно приостановить все работы;

5.8.2.сообщить Администратору информационной безопасности о факте обнаружения программных вирусов;

5.8.3. принять по согласованию с Администратором информационной безопасности меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации.

6. Ответственность пользователя

Пользователь несет персональную ответственность за соблюдение правил эксплуатации, требований по безопасности информации, сохранность защищаемой информации, документов и электронных носителей информации, персональных идентификаторов, с которыми он работает.