Приложение №4
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.

ИНСТРУКЦИЯ

по применению средств антивирусной защиты

Липецк 2025

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»).

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»).

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)).

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

1.1.3. 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 в целях осуществления антивирусной защиты информации, содержащейся и обрабатываемой на автоматизированных рабочих местах пользователей (далее – АРМ), от несанкционированного копирования, модификации и разрушения данных, используемых в деятельности МУ «ДК «Матыра» (далее - Организация), а также нарушения работы используемого программного обеспечения при воздействии компьютерных вирусов и других вредоносных программ. Инструкция устанавливает требования и ответственность при организации защиты информации от разрушающего воздействия вредоносных программ – компьютерных вирусов.

1.3. Требования настоящей Инструкции являются обязательными для сотрудников Организации (далее – Пользователь) и администратора информационной безопасности.

2. Общие требования

2.1. Для реализации антивирусной защиты на всех АРМ Организации должны применяться средства антивирусной защиты. Допускается к использованию только сертифицированные ФСТЭК России лицензионные антивирусные средства общего применения

2.2. Установка (инсталляция), настройка (конфигурирование), обновление модулей средств антивирусной защиты, удаление должно осуществляться только администратором информационной безопасности.

2.3. Управление параметрами настройки функций безопасности средств антивирусной защиты должно быть доступно только администратору информационной безопасности.

2.4. Средства антивирусной защиты должны постоянно находиться в активном состоянии и обеспечивать антивирусную защиту в режиме реального времени.

3. Организация антивирусной защиты

3.1. Применение средств антивирусной защиты информации устанавливается с учетом соблюдений следующих требований:

- обязательный контроль за отсутствием программных вирусов во всех поступающих на объект информатизации со съёмных носителей информации (далее - НИ), информационных массивах, программных средств общего и специального назначения;

- обязательная проверка всех электронных писем на предмет отсутствия программных вирусов;

- периодическая проверка на предмет отсутствия программных вирусов жестких дисков АРМ и обязательная проверка НИ перед началом работы с ними;

- внеплановая проверка жестких дисков АРМ и съемных НИ в случае подозрения на наличие программных вирусов.

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

4. Требования к параметрам настроек антивирусной защиты

4.1. Периодичность поиска вредоносных компьютерных программ (вирусов) средствами антивирусной защиты должно обеспечиваться в соответствии с таблицей 1.

Таблица 1.

№ п/п	Объект проверки	Периодичность проверки
1	Оперативная и системная память средств вычислительной техники	1 раз в неделю
2	Файлы, получаемые и передаваемые через сети общего пользования	При каждом получении и отправке
3	Файлы инсталляции программного обеспечения	Каждый раз перед установкой (инсталляцией)
4	Файлы обновлений программного обеспечения	1 раз в неделю
5	Съемные машинные носители информации	При каждом подключении
6	Почтовые сообщения электронной почты	При каждом получении и отправке

4.2. Средства антивирусной защиты при обнаружении вредоносной компьютерной программы (вируса) должны выполнять следующие действия:

- удалить зараженный объект (файл);

- уведомить о масштабе времени, близком к реальному, об обнаружении вредоносной компьютерной программы (вируса).

5. Порядок обновления баз данных признаков вредоносных компьютерных программ (вирусов).

5.1. Администратор информационной безопасности должен обеспечивать обновление базы данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты.

5.2. Периодичность обновления определяется программными требованиями средств антивирусной защиты информации или устанавливается администратором безопасности.

6. Права и обязанности администратора информационной безопасности

6.1. Администратор информационной безопасности обязан обеспечивать соблюдение политики антивирусной защиты информации и выявление фактов заражения программными вирусами.

6.2. К основным задачам администратора информационной безопасности относятся организации процесса установки и обновления средств антивирусной защиты информации на АРМ пользователей и обеспечение технического сопровождения действий пользователей в случаях обнаружения программных вирусов, а также осуществление контроля за состоянием системы антивирусной защиты информации.

6.3. Администратор информационной безопасности несет ответственность:

- за своевременную установку средств антивирусной защиты информации;
- за эксплуатацию системы антивирусной защиты информации;
- за своевременное обновление лицензий на средства антивирусной защиты информации;
- за своевременное обновление баз данных средств антивирусной защиты информации.

7. Обязанности пользователей средств антивирусной защиты информации

7.1. Пользователь при работе со съёмными носителями информации обязан перед началом работы провести их проверку средствами антивирусной защиты на предмет отсутствия компьютерных вирусов и вредоносных программ.

7.2. Пользователям запрещается:

- отключать средства антивирусной защиты информации во время работы;
- без разрешения Администратора информационной безопасности копировать любые файлы, устанавливать и использовать программное обеспечение, не предназначенное для выполнения служебных задач.

8. Действия при обнаружении вредоносных компьютерных программ (вирусов)

8.1.Пользователи при обнаружении или появления подозрений на наличие компьютерных вирусов или вредоносного ПО обязаны немедленно прекратить какие-либо действия на АРМ и провести лечение зараженных файлов путем выбора соответствующего пункта меню антивирусной программы и затем провести повторный антивирусный контроль.

8.2. В случае обнаружения на АРМ не поддающегося лечению вируса или вредоносного ПО, Пользователь обязан поставить в известность Администратора информационной безопасности, прекратить работу на АРМ.

8.3. При обнаружении вредоносных компьютерных программ (вирусов) администратор информационной безопасности принимает меры по предотвращению наступления негативных последствий заражения. Меры могут включать:

-удаление вредоносной программы;
- установление причин и источника заражения;
- проведение полной антивирусной проверки.

9. Ответственность

9.1. За ненадлежащее исполнение или неисполнения своих обязанностей, предусмотренных настоящей инструкцией Пользователи и администратор информационной безопасности несут ответственность, установленную действующим законодательством Российской Федерации.