**УТВЕРЖДАЮ**

Директор МАОУ «Первомайская СОШ»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Стрижова Г.Н.

«\_\_\_» \_\_\_\_\_\_\_\_\_2014 г.

**ИНСТРУКЦИЯ**

**по организации антивирусной защиты информации**

**в МАОУ «Первомайская СОШ» Кваркенского района Оренбургской области**

**1. Общие положения**

1.1. Настоящая рабочая инструкция (далее — РИ) определяет порядок применения средств антивирусной защиты в МАОУ «Первомайская СОШ» обязанности и права администратора локальной вычислительной сети (далее — ЛВС), пользователей средств антивирусной защиты, порядок установки и применения обновлений, подключения средств антивирусной защиты, а также порядок ликвидации последствий воздействия программных вирусов.

1.2. Требования настоящей РИ обязательны для выполнения всеми пользователями и администратором ЛВС МАОУ «Первомайская СОШ», а также иными лицами, использующими средства вычислительной техники.

1.3. В настоящей РИ применены термины и определения:

а) ***антивирусная защита информации*** - система организационно-технических мероприятий, требований и условий использования электронно-вычислительной техники, предназначенная для предотвращения заражения программными вирусами информационно-вычислительных ресурсов посредством применения средств антивирусной защиты информации:

б) ***вредоносная программа*** - программа для электронно-вычислительных машин (далее — ЭВМ), заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети;

в) ***программные вирусы*** - разновидность вредоносных программ, отличительной особенностью которых является способность к размножению (саморепликации). В дополнение к этому они могут повреждать или полностью уничтожать данные, подконтрольные пользователю, от имени которого была запущена зараженная программа.

1.4. Оснащение средствами антивирусной защиты информации является видом материального обеспечения. В образовательной организации может использоваться только лицензионное антивирусное программное обеспечение.

1.5. Общее руководство обеспечением антивирусной защиты информации осуществляется директором МАОУ «Первомайская СОШ».

1.6. Руководителем ОУ назначается лицо, ответственное за антивирусную защиту (в данном случае – администратор ЛВС), которое осуществляет практическое решение задач, связанных с организацией антивирусной защиты информации и применением средств антивирусной защиты информации в МАОУ «Первомайская СОШ». В противном случае вся ответственность за обеспечение антивирусной защиты ложится на руководителя образовательного учреждения.

1.7. Средства антивирусной зашиты информации должны устанавливаться на всех единицах вычислительной техники, используемых в школе.

1.8. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, флэш-картах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

1.9. Передача средств антивирусной защиты пользователями, администратором ЛВС и другими работниками на объекты, не входящие в МАОУ «Первомайская СОШ», запрещена.

При возникновении ситуаций, не описанных в настоящей рабочей инструкции, решение принимается администратором ЛВС по согласованию с директором школы.

**2. Применение средств антивирусной защиты информации**

2.1. Применение средств антивирусной защиты информации осуществляется при соблюдении следующих требований:

а) обязательный входной контроль отсутствия программных вирусов во всех поступающих на объект информатизации электронных носителях информации, информационных массивах, программных средствах общего и специального назначения;

б) обязательная проверка всех электронных писем на предмет отсутствия программных вирусов;

в) периодическая проверка на предмет отсутствия программных вирусов жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка съемных носителей информации перед началом работы с ними;

г) внеплановая проверка жестких магнитных дисков и съемных носителей информации в случае подозрения на наличие программных вирусов;

д) восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами.

2.2. Администратор ЛВС школы обеспечивает:

а) управление установкой и обновлением лицензионных ключей средств антивирусной защиты информации;

б) управление установкой обновлений баз средств антивирусной защиты информации;

в) ограничение доступа пользователей на рабочих местах к настройкам установленных средств антивирусной защиты информации;

г) удаленное решение проблем, возникающих в процессе использования средств антивирусной защиты информации.

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

2.4. Копирование любой информации, переносимой с помощью любых съемных носителей информации, должно производиться только после проведения процедуры полного антивирусного контроля съемного носителя.

2.5. Антивирусная профилактика является необходимым элементом защиты информационных ресурсов учреждения от их модификации и уничтожения. Антивирусная профилактика состояния средств антивирусной защиты информации на сервере и рабочих станциях должна проводиться по согласованию с администратором ЛВС в нерабочее время, за исключением внештатных ситуаций.

2.6. Проведение мероприятий по антивирусной защите средств информатизации школы должно включать следующее:

а) ежедневное в начале работы при загрузке компьютера в автоматическом режиме обновление антивирусных баз и проведение антивирусного контроля всех дисков и файлов персонального компьютера;

б) обязательная проверка всех электронных писем на предмет отсутствия программных вирусов в автоматическом режиме;

в) блокирование сетевых атак из сети Интернет в автоматическом режиме;

г) периодическая проверка в автоматическом режиме на предмет отсутствия программных вирусов жестких магнитных дисков (не реже одного раза в месяц);

д) обязательная проверка съемных носителей информации перед началом работы с ними;

е) восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами.

2.7. 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), необходимо провести внеплановую проверку жестких магнитных дисков и съемных носителей информации на наличие программных вирусов.

2.8. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов ответственный за антивирусную защиту обязан совместно с пользователем зараженных вирусом файлов определить необходимость дальнейшего их использования и провести лечение или уничтожение заражённых файлов.

**3. Обновление баз данных средств антивирусной защиты информации**

3.1. Своевременное обновление баз данных средств антивирусной защиты информации является неотъемлемой частью обеспечения эффективной политики антивирусной защиты информации.

3.2. Обновление баз данных средств антивирусной защиты информации на рабочих станциях школьной ЛВС должно осуществляться централизованно через сервер школы в автоматическом режиме.

3.3. На рабочем месте администратора ЛВС могут быть установлены средства, позволяющие через ЛВС управлять компонентами системы антивирусной защиты, установленными на рабочих станциях и сервере, а также проводить обновления баз средств антивирусной защиты информации.

В случае если рабочая станция пользователя не подключена к ЛВС, обновление средств антивирусной защиты информации производится администратором ЛВС через съемные носители информации.

3.4. Периодичность обновления определяется программными требованиями средств антивирусной защиты информации или устанавливается администратором ЛВС. Плановые проверки средств информатизации школы должны проводиться не реже одного раза в месяц.

**4. Обязанности, права и порядок назначения администратора ЛВС**

4.1. Приказом по школе руководитель ОУ назначает ответственного за антивирусную защиту — администратора ЛВС.

4.2. Администратор ЛВС обязан обеспечивать соблюдение политики антивирусной защиты информации и выявление фактов заражения программными вирусами в школе.

4.3. Администратор ЛВС обязан раз в год проводить с пользователями инструктаж по работе с антивирусным программным обеспечением.

4.3. К задачам администратора ЛВС относятся организация процесса установки и обновления средств антивирусной защиты информации на рабочих станциях пользователей и обеспечение технического сопровождения действий пользователей в случаях обнаружения программных вирусов, а также осуществление контроля за состоянием системы антивирусной защиты информации.

4.4. Администратор ЛВС несет ответственность:

а) за своевременную установку средств антивирусной защиты информации;

б) за эксплуатацию системы антивирусной защиты информации;

в) за своевременное обновление лицензий на средства антивирусной защиты информации;

г) за своевременное обновление баз данных средств антивирусной защиты информации.

4.5. Администратор ЛВС имеет право:

а) вносить предложения по совершенствованию системы антивирусной защиты информации;

б) принимать участие в планировании мероприятий по антивирусной защите информации;

в) осуществлять контроль состояния средств антивирусной защиты информации в ОУ;

г) проводить служебные проверки по фактам заражения программными вирусами автоматизированных систем обработки информации и средств вычислительной техники в ОУ;

д) оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты информации в ОУ.

**5. Обязанности пользователей средств антивирусной защиты информации**

5.1. Пользователь обязан изучить настоящую рабочую инструкцию. Факт ознакомления фиксируется в листе ознакомления (приложение к настоящей рабочей инструкции).

5.2. Пользователям запрещается:

а) отключать средства антивирусной защиты информации во время работы;

б) использовать средства антивирусной защиты информации, отличные от установленных администратором ЛВС.

в) без разрешения администратора ЛВС копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

5.3. Копирование информации на рабочую станцию пользователя с флэш-карт, магнитных, оптических и любых других съемных носителей информации неслужебного характера должно осуществляться пользователем только с разрешения администраторов ЛВС.

5.4. В случае появления подозрений на наличие программных вирусов в ЛВС пользователи должны немедленно проинформировать об этом администратора ЛВС.

В случае выявления инцидентов (фактов и т.п.), связанных со сбоями в работе средств антивирусной защиты, пользователь обязан незамедлительно сообщить об этом администратору ЛВС или директору школы.

**6. Действия пользователей и администраторов при обнаружении вирусов**

6.1. Основными путями проникновения вирусов в ЛВС являются: съемные накопители информации, электронная почта, файлы, получаемые из сети Интернет, ранее зараженные рабочие станции.

6.2. В случае обнаружения программных вирусов при входном контроле съемных носителей информации, файлов или почтовых сообщений, пользователь обязан:

а) приостановить процесс приема-передачи информации;

б) сообщить администратору ЛВС о факте обнаружения программного вируса;

в) принять по согласованию с администратором ЛВС меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации;

г) сообщить о факте обнаружения программного вируса и организации, из которой поступили зараженные съемные электронные носители информации, файлы или почтовые сообщения.

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

а) немедленно приостановить все работы;

б) сообщить администратору ЛВС о факте обнаружения программных вирусов;

в) принять по согласованию с администратором ЛВС меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации.

6.4. При невозможности ликвидации последствий заражения программными вирусами администратору ЛВС необходимо:

а) принять решение о запросе в организацию, осуществляющую техническую поддержку средств антивирусной защиты информации;

б) осуществить полную переустановку программного обеспечения на зараженном компьютере.

6.5. Все факты модификации и разрушения данных на сервере в случае заражения его вирусами, а также обнаружения других вредоносных программ классифицируются как значимые нарушения информационной безопасности и должны анализироваться посредством проведения служебного расследования, проводимого по приказу директора школы.

**7. Ответственность**

7.1. За нарушение требований настоящей рабочей инструкции администратор ЛВС и пользователи несут ответственность, установленную действующим законодательством РФ.

7.2. Непосредственную ответственность за соблюдение установленных норм обеспечения антивирусной защиты информации на своих рабочих местах, в том числе за своевременное обновление антивирусных баз средств антивирусной защиты информации, несут пользователи, за которыми закреплены средства вычислительной техники.

7.3. В случае нарушения требований настоящей рабочей инструкции, связанных с применением пользователем средств антивирусной защиты информации, пользователь несет персональную ответственность, установленную действующим законодательством РФ и внутренними нормативными документами школы.

7.4. Периодический контроль за состоянием антивирусной защиты в образовательном учреждении осуществляется директором школы.