МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ГИМНАЗИЯ №1»

663305, Россия, Красноярский край, город Норильск, район Центральный, улица Кирова, дом 30
тел. (приемная): (3919) 238-301, тел./факс: (3919) 238-472,
e – mail:norilsk-gim1@mail.ru

РАССМОТРЕНО
на заседании
Педагогического совета
МБОУ «Гимназия № 1»
Протокол от
«31» 08 2016г. № 1

УТВЕРЖДАЮ:
Директор МБОУ «Гимназия № 1»
_____ С.А. Савенкова
«01» сентября 2016 г.

ИНСТРУКЦИЯ
по организации антивирусной защиты информации в МБОУ «Гимназия № 1»

I. Общие положения

1.1. Настоящая инструкция по организации антивирусной защиты информации (далее – Инструкция) в муниципальном бюджетном общеобразовательном учреждении «Гимназия № 1» (далее – гимназия) является локальным нормативным актом гимназии, который определяет порядок применения средств антивирусной защиты в гимназии, обязанности и права администратора локальной вычислительной сети, пользователей средств антивирусной защиты, порядок установки и применения обновлений, подключения средств антивирусной защиты, а также порядок ликвидации последствий воздействия программных вирусов.

1.2. Требования Инструкции обязательны для выполнения всеми пользователями и администратором локальной сети, а также иными лицами, использующими средства вычислительной техники.

1.3. В Инструкции применены термины и определения:

- ***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;
- ***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;
- ***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 гимназии.

1.6. Директором гимназии назначается лицо, ответственное за антивирусную защиту (в данном случае – администратор локальной вычислительной сети), которое осуществляет практическое решение задач, связанных с организацией антивирусной защиты информации и применением средств антивирусной защиты информации в гимназии. 1.7.
1.7. Средства антивирусной зашиты информации должны устанавливаться на всех единицах вычислительной техники, используемых в гимназии.
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 локальной вычислительной сети и другими работниками на объекты, не входящие в гимназию, запрещена.
При возникновении ситуаций, не описанных в Инструкции, решение принимается администратором локальной вычислительной сети по согласованию с директором гимназии.

II. Применение средств антивирусной защиты информации

2.1. Применение средств антивирусной защиты информации осуществляется при соблюдении следующих требований:
- обязательный входной контроль отсутствия программных вирусов, во всех поступающих на объект информатизации электронных носителях информации, информационных массивах, программных средствах общего и специального назначения;
- обязательная проверка всех электронных писем на предмет отсутствия программных вирусов;
- 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;
- внеплановая проверка жестких магнитных дисков и съемных носителей информации в случае подозрения на наличие программных вирусов;
- восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами.
2.2. Администратор локальной вычислительной сети обеспечивает:
- управление установкой и обновлением лицензионных ключей средств антивирусной защиты информации;
- управление установкой обновлений баз средств антивирусной защиты информации;
- ограничение доступа пользователей на рабочих местах к настройкам установленных средств антивирусной защиты информации;
- 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 гимназии от их модификации и уничтожения. Антивирусная профилактика состояния средств антивирусной защиты информации на сервере и рабочих станциях должна проводиться по согласованию с администратором локальной вычислительной сети в нерабочее время, за исключением внештатных ситуаций.

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

- ежедневное в начале работы при загрузке компьютера в автоматическом режиме обновление антивирусных баз и проведение антивирусного контроля всех дисков и файлов персонального компьютера;
- обязательная проверка всех электронных писем на предмет отсутствия программных вирусов в автоматическом режиме;
- блокирование сетевых атак из сети Интернет в автоматическом режиме;
- периодическая проверка в автоматическом режиме на предмет отсутствия программных вирусов жестких магнитных дисков (не реже одного раза в месяц);
- обязательная проверка съемных носителей информации перед началом работы с ними;
- 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.

III. 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 локальной вычислительной сети должно осуществляться централизованно через сервер гимназии в автоматическом режиме.

3.3. На рабочем месте администратора локальной вычислительной сети могут быть установлены средства, позволяющие через локальной вычислительной сети 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 локальной вычислительной сети, обновление средств антивирусной защиты информации производится администратором локальной вычислительной сети через съемные носители информации.
3.4. Периодичность обновления определяется программными требованиями средств антивирусной защиты информации или устанавливается администратором локальной вычислительной сети. Плановые проверки средств информатизации гимназии должны проводиться не реже одного раза в месяц.

IV. Обязанности, права и порядок назначения администратора локальной вычислительной сети

4.1. Директор назначает приказом ответственного за антивирусную защиту – администратора локальной вычислительной сети.
4.2. Администратор локальной вычислительной сети обязан обеспечивать соблюдение политики антивирусной защиты информации и выявление фактов заражения программными вирусами в гимназии.
4.3. Администратор локальной вычислительной сети обязан раз в год проводить с пользователями инструктаж по работе с антивирусным программным обеспечением.
4.3. К задачам администратора локальной вычислительной сети 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 локальной вычислительной сети 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.
4.5. Администратор локальной вычислительной сети имеет право:
- вносить предложения по совершенствованию системы антивирусной защиты информации;
- принимать участие в планировании мероприятий по антивирусной защите информации;
- осуществлять контроль состояния средств антивирусной защиты информации в гимназии;
- проводить служебные проверки по фактам заражения программными вирусами автоматизированных систем обработки информации и средств вычислительной техники в гимназии;
- оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты информации в гимназии.

V. Обязанности пользователей средств антивирусной защиты информации

5.1. Пользователь обязан изучить Инструкцию. Факт ознакомления фиксируется в листе ознакомления (приложение к Инструкции).
5.2. Пользователям запрещается:
- отключать средства антивирусной защиты информации во время работы;

- использовать средства антивирусной защиты информации, отличные от установленных администратором локальной вычислительной сети.
- без разрешения администратора локальной вычислительной сети 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 локальной вычислительной сети.

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

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

VI. Действия пользователей и администраторов при обнаружении вирусов

6.1. Основными путями проникновения вирусов в локальной вычислительной сети 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:
- приостановить процесс приема-передачи информации;
- сообщить администратору локальной вычислительной сети о факте обнаружения программного вируса;
- принять по согласованию с администратором локальной вычислительной сети меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации;
- 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:
- немедленно приостановить все работы;
- сообщить администратору локальной вычислительной сети о факте обнаружения программных вирусов;
- принять по согласованию с администратором локальной вычислительной сети меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации.

6.4. При невозможности ликвидации последствий заражения программными вирусами администратору локальной вычислительной сети необходимо:
- принять решение о запросе в организацию, осуществляющую техническую поддержку средств антивирусной защиты информации;
- 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 гимназии.

VII. Ответственность

7.1. За нарушение требований Инструкции администратор локальной вычислительной сети и пользователи несут ответственность, установленную действующим законодательством Российской Федерации.

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 Инструкции, связанных с применением пользователем средств антивирусной защиты информации, пользователь несет персональную ответственность, установленную действующим законодательством Российской Федерации и внутренними нормативными документами гимназии.

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