Согласовано с
председателем профкома

Утверждено
Директор МБОУ "СОШ №1 п.Гикало"
_____ / Р.Ш. Гелаева /

Инструкция о применении средств антивирусной защиты информации

1. Общие положения

1. Настоящая Инструкция разработана в целях осуществления антивирусной защиты информации, содержащейся на электронных носителях МБОУ «СОШ № 1 п. Гикало » от несанкционированного копирования, а также нарушения работы используемого программного обеспечения при воздействии вирусов и других вредоносных программ посредством комплекса организационно-технических мероприятий по обеспечению информационной безопасности.

2. Настоящая Инструкция определяет порядок применения средств антивирусной защиты в школе, задачи, обязанности и права ответственных лиц за организацию антивирусной защиты, порядок установки и применения обновлений, подключения средств антивирусной защиты, а также порядок ликвидации последствий воздействия программных вирусов. Ответственное лицо за организацию антивирусной защиты назначается приказом директора школы.

3. Требования настоящей Инструкции обязательны для выполнения всеми участниками образовательного процесса.

4. В образовательной организации может использоваться только лицензионное программное обеспечение.

5. Ответственный за антивирусную защиту информации осуществляет непосредственное руководство организацией проведения работ по антивирусной защите информации в школе: установку нового программного обеспечения, проверку электронных архивов компьютеров и съемных носителей на вирусы.

6. Факт выполнения антивирусной проверки программного обеспечения должен регистрироваться в журнале за подписью лица, ответственного за антивирусную защиту.

2. Порядок применения средств антивирусной защиты информации в образовательном учреждении

1. Средства антивирусной защиты информации должны устанавливаться на всех средствах вычислительной техники, эксплуатируемых в образовательном учреждении.

2. Обновление антивирусных программ должно проводиться ежедневно при загрузке компьютеров в автоматическом режиме.

3. Антивирусная проверка и контроль файлов на съёмных носителях должна проводиться в каждом случае подключения этих носителей к школьным компьютерам.

4. Порядок применения средств антивирусной защиты информации устанавливается с учетом соблюдения следующих требований:

- обязательный входной контроль за отсутствием 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 месяц) 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.

5. Уполномоченное лицо организации по антивирусной защите информации обеспечивает:

- управление конфигурацией и логической структурой всего программного обеспечения системы антивирусной защиты информации;

- управление установкой и обновлением лицензионных ключей средств антивирусной защиты информации;

- управление рассылкой и установкой обновлений баз средств антивирусной защиты информации;

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

- настройку рассылки сообщений об обнаружении вирусов, о сбоях в работе средств антивирусной защиты и т.п.

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

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

3. Обязанности, права и порядок назначения

ответственного за антивирусную защиту

1. Ответственный за антивирусную защиту в школе обязан обеспечивать соблюдение в учреждении политики антивирусной защиты информации и выявление фактов заражения программными вирусами.

2. К основным его задачам относятся организация процесса установки и обновления средств антивирусной защиты информации на рабочих компьютерах пользователей и обеспечение технического сопровождения в случаях обнаружения программных вирусов, а также осуществление контроля за состоянием системы антивирусной защиты информации.

3. Ответственный за антивирусную защиту несет ответственность: за своевременную установку средств антивирусной защиты информации;

- за эксплуатацию системы антивирусной защиты информации;

- за своевременное обновление средств антивирусной защиты информации.

4. Ответственный за антивирусную защиту имеет право:

- вносить предложения по совершенствованию системы антивирусной защиты информации;

- осуществлять контроль состояния средств антивирусной защиты информации;

- проводить служебные проверки по фактам заражения программными вирусами средств вычислительной техники в образовательном учреждении;

- оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты информации.

5. Обязанности ответственного за антивирусную защиту могут совмещать должностные лица, назначенные директором школы.

4. Обязанности пользователей средств антивирусной

защиты информации

1. Пользователь обязан изучить настоящую Инструкцию и ознакомиться с необходимостью несения ответственности за выполнение ее требований.

2. Пользователям запрещается:

- отключать средства антивирусной защиты информации во время работы;

- использовать средства антивирусной защиты информации, отличные от поддерживаемых школьными компьютерами;

- без разрешения ответственного за антивирусную защиту копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

3. Ввод информации с магнитных, оптических, магнитооптических и любых других съемных носителей информации неслужебного характера должен осуществляться пользователем только с разрешения ответственного лица.

4. В случае появления подозрений на наличие программных вирусов в ЛВС пользователи должны немедленно проинформировать об этом ответственного за антивирусную защиту.

5. Порядок действий пользователей и администраторов АВЗ при обнаружении вирусов

1. Основными путями проникновения вирусов в информационно - вычислительную сеть организации являются: гибкие магнитные диски, компакт-диски, иные съемные накопители информации, электронная почта, файлы, получаемые из сети Интернет. В случае обнаружения программных вирусов при входном контроле пользователь должен:

- приостановить процесс приема-передачи информации;

- сообщить ответственному лицу о факте обнаружения программного вируса;

- принять меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации;

- сообщить о факте обнаружения программного вируса в структурное подразделение, из которого поступили зараженные съемные электронные носители информации, файлы или почтовые сообщения.

2. При невозможности ликвидации последствий заражения программными вирусами необходимо:

- заархивировать зараженные файлы с внедренными программными вирусами и направить с приложением соответствующего сопроводительного документа в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;

- осуществить полную переустановку программного обеспечения на зараженном компьютере.

5. При получении информации о возможном нарушении либо выявлении факта нарушения требований настоящей Инструкции работа на рабочей станции данного пользователя незамедлительно блокируется по решению администратора АВЗ.

6. Все факты модификации и разрушения данных на серверах или рабочих станциях, заражение их вирусами, а также обнаружение других вредоносных программ классифицируются как значимые нарушения информационной безопасности и должны анализироваться посредством проведения служебного расследования, проводимого по приказу директора школы.

6. Ответственность за выполнение требований Инструкции

1. За нарушение настоящей Инструкции администратор АВЗ и пользователи несут ответственность, установленную действующим законодательством Российской Федерации, нормативными правовыми актами и локальными актами школы.

2. Непосредственную ответственность за соблюдение в повседневной деятельности 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.

3. В случае нарушения требований настоящей Инструкции, связанных с применением пользователем средств антивирусной защиты информации, пользователь несет персональную ответственность, установленную действующим законодательством Российской Федерации и локальными нормативными актами образовательного учреждения.

7. Порядок оснащения организации средствами антивирусной

защиты информации

1. Оснащение средствами антивирусной защиты информации является видом материального обеспечения и осуществляется в образовательном учреждении централизованно.

2. Передача полученных средств антивирусной защиты на объекты, не входящие в состав организации, запрещена. За несанкционированное распространение средств антивирусной защиты информации виновные несут ответственность в соответствии с законодательством Российской Федерации.