СОГЛАСОВАНО
председателем профсоюзного
комитета -Кормилицин В.В.
«19» 08 2014 года

УТВЕРЖДАЮ :
Директор МОУ «ВСОШ №2»
_____ Н.А.Корсакова
Приказ от 19 августа 2014 год №92 О

ИНСТРУКЦИЯ
о применении средств антивирусной защиты информации
И О Т - 068 – 2014

В Инструкции о применении средств антивирусной защиты информации (далее - Инструкция) использованы следующие термины и определения:

Пользователи - должностные лица, а также все другие лица, использующие в работе средства электронно-вычислительной техники.

Администраторы антивирусной защиты информации (далее - администраторы) -должностные лица, назначенные ответственными за эксплуатацию средств антивирусной защиты информации и обеспечивающие организацию и эффективное использование системы антивирусной защиты информации.

Локально-вычислительная сеть - группа ЭВМ, объединенные одним или несколькими автономными высокоскоростными .

Антивирусная защита информации - система организационно-технических мероприятий, требований и условий использования электронно-вычислительной техники, предназначенная для предотвращения заражения программными вирусами посредством применения средств антивирусной защиты информации.

Вредоносная программа - программа для электронно-вычислительных машин (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.

I. Общие положения

1. Настоящая Инструкция разработана в целях осуществления антивирусной защиты информации, содержащейся и обрабатываемой от несанкционированного копирования, модификации и разрушения сведений, используемых в работе, а также нарушения работы при воздействии вирусов и других вредоносных программ посредством комплекса организационно-технических мероприятий по обеспечению информационной безопасности в школе.
2. Настоящая Инструкция определяет порядок применения средств антивирусной задачи, обязанности и права администраторов, пользователей средств антивирусной защиты информации, порядок установки и применения обновлений, подключения к Антивирусному центру, а также порядок ликвидации последствий воздействия программных вирусов.
3. Настоящая Инструкция разработана на основании Положения о системе антивирусной защиты информации в Российской Федерации и в организациях, находящихся в ведении ФТС России, утвержденного приказом ФТС России от 28.05.2007 N 660 "О системе антивирусной защиты информации Российской Федерации".
4. Требования настоящей Инструкции обязательны для выполнения всеми пользователями и администраторами, а также иными лицами, использующими средства вычислительной техники.
5. Практическое решение задач, связанных с организацией антивирусной защиты информации и применением средств антивирусной защиты информации, осуществляется системным администратором.

II. Порядок применения средств антивирусной защиты информации

1. Средства антивирусной защиты информации должны устанавливаться на всех средствах вычислительной техники.
2. 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 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.

3. Инсталляция и настройка средств антивирусной защиты информации осуществляются в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.
4. Копирование любой информации, переносимой с помощью любых съемных носителей информации, должно производиться только после проведения процедуры полного антивирусного контроля съемного носителя.
5. Антивирусная профилактика является необходимым элементом защиты информационных от их модификации и уничтожения. Антивирусная профилактика состояния средств антивирусной защиты информации должна проводиться по согласованию с администраторами в нерабочее время, за исключением внештатных ситуаций.

III. Порядок обновления баз данных средств антивирусной защиты информации

1 Своевременное обновление баз данных средств антивирусной защиты информации является неотъемлемой частью обеспечения эффективной политики антивирусной защиты информации.
2. Обновление баз данных средств антивирусной защиты информации осуществляется в автоматическом режиме.

IV. Обязанности, права и порядок назначения системного администратора

1. Администратор обязан обеспечивать соблюдение политики антивирусной защиты информации и выявление фактов заражения программными вирусами.
2. К основным задачам администратора относятся организация процесса установки и обновления средств антивирусной защиты информации, а также осуществление контроля за состоянием системы антивирусной защиты информации

3. Администратор 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. Администратор имеет право:
-вносить предложения по совершенствованию системы антивирусной защиты информации ;
-принимать участие в планировании мероприятий по антивирусной защите информации в таможне и планировании оснащения средствами антивирусной защиты информации;
- осуществлять контроль состояния средств антивирусной защиты информации;
-проводить служебные проверки по фактам заражения программными вирусами автоматизированных систем обработки информации и средств вычислительной техники;
-оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты информации .

V. Обязанности пользователей средств антивирусной защиты информации

1. Пользователь обязан изучить настоящую Инструкцию и ознакомиться с необходимостью несения ответственности за выполнение ее требований под роспись.
2. Пользователям запрещается:
-отключать средства антивирусной защиты информации во время работы;
-использовать средства антивирусной защиты информации, без разрешения администратора;
-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 администратора.
4. В случае появления подозрений на наличие программных вирусов пользователи должны немедленно проинформировать об этом администратора

VI. Порядок действий пользователей и администраторов при обнаружении вирусов

1. Основными путями проникновения вирусов в информационно - вычислительную сеть таможни 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 отчуждаемых носителей информации, файлов или почтовых сообщений, пользователь должен:
приостановить процесс приема-передачи информации;
сообщить администратору АВЗ или ответственному за информационную безопасность и техническую защиту информации о факте обнаружения программного вируса;
принять по согласованию с администратором 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 обнаружении программных вирусов в процессе обработки информации пользователь обязан:
немедленно приостановить все работы;
сообщить администратору о факте обнаружения программных вирусов;
принять по согласованию с администратором меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации.
3. При невозможности ликвидации последствий заражения программными вирусами администратору необходимо:
заархивировать зараженные файлы с внедренными программными вирусами и направить с приложением соответствующего сопроводительного документа
осуществить полную переустановку программного обеспечения на зараженном компьютере.
4. Все факты модификации и разрушения данных на серверах, заражение их вирусами, а также обнаружение других вредоносных программ классифицируются как значимые нарушения информационной безопасности и должны анализироваться посредством проведения служебного расследования.

VII. Ответственность за выполнение требований Инструкции

1. За нарушение настоящей Инструкции администратор и пользователи несут ответственность, установленную действующим законодательством Российской Федерации
2. В случае нарушения требований настоящей Инструкции, связанных с применением пользователем средств антивирусной защиты информации, пользователь несет персональную ответственность, установленную действующим законодательством Российской Федерации.

Ответственный за соблюдение охраны труда _____ (Фролова Е.В.)
С инструкцией ознакомлены: Загородняя О. С.