Приложение 4

к приказу от 31.08.2018 № 429

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 2» МУНИЦИПАЛЬНЫЙ ОБРАЗОВАТЕЛЬНЫЙ ОКРУГ СИМФЕРОПОЛЬ РЕСПУБЛИКИ КРЫМ

Принято на заседании
педагогического совета
Протокол № 12
От 30.08.2018 г.

УТВЕРЖДЕНО
Директор МБОУ «Средняя общеобразовательная школа № 2»
_____ В.А. Кухнина
Приказ № 429 от 31.08. 2018 г.
«Об утверждении организационно-распорядительной документации по обработке персональных данных в МБОУ «СОШ № 2» г. Симферополя»

ИНСТРУКЦИЯ

по применению средств антивирусной защиты информации в МБОУ «СОШ № 2» г. Симферополя

I. Общие положения

1. Данная Инструкция разработана в целях обеспечения антивирусной безопасности информационных систем (далее – ИС) МБОУ «СОШ № 2» г. Симферополя и регламентирует требования к организации антивирусной защиты в ИС, а также устанавливает ответственность работников МБОУ «СОШ № 2» г. Симферополя, эксплуатирующих ИС, а также администраторов информационной безопасности за выполнение этих требований.

2. Настоящая Инструкция разработана с учетом требований и рекомендаций руководящих документов ФСТЭК России.

3. Установка средств антивирусного контроля и настройка их параметров на автоматизированных рабочих местах (далее – АРМ), серверах ИС

осуществляется администратором информационной безопасности, в соответствии с эксплуатационной документацией по применению конкретных антивирусных средств.

II. Порядок установки и обновления антивирусных средств

1. К применению в ИС допускаются только антивирусные средства, имеющие действующую лицензию.

2. Установка антивирусного программного обеспечения и настройка регулярного его обновления осуществляется администратором информационной безопасности.

3. Первичная установка антивирусного программного обеспечения на персональные компьютеры пользователей осуществляется администратором информационной безопасности при подготовке АРМ пользователя.

4. Антивирусное программное обеспечение должно быть установлено на каждый элемент ИС, подверженный актуальной вирусной уязвимости.

III. Порядок проведения антивирусного контроля

1. На всех объектах вычислительной техники (АРМ, серверы), администратор информационной безопасности обеспечивает антивирусный контроль в режиме реального времени.

2. На АРМ и серверах ИС администратор информационной безопасности дополнительно обеспечивает проведение полного сканирования всех машинных носителей информации средств вычислительной техники (постоянно установленных либо съемных) антивирусными средствами не реже 1 раза в неделю (автоматическое сканирование по расписанию).

3. Кроме того, администратор информационной безопасности осуществляет обязательный антивирусный контроль:

– любой информации (текстовых файлов любых форматов, файлов данных, исполняемых файлов, файлов, помещаемых в электронный архив), получаемой и передаваемой по телекоммуникационным каналам, а также информации на съёмных носителях (магнитные диски, ленты, оптические диски, USB-накопители и т.п.), получаемой от сторонних лиц и организаций (автоматическое сканирование в режиме реального времени).

4. Администратор информационной безопасности осуществляет настройку антивирусной системы таким образом, что при обнаружении вируса (инфицированного файла) выполняются следующие действия:

– лечение (очистка) файла от обнаруженного вируса с предварительным созданием резервной копии;

– при невозможности удаления тела вируса из файла или обнаружении «троянской программы», «сетевого червя» и т.п. данный объект перемещается в специально выделенную закрытую директорию (карантинную зону);

– осуществляется оповещение администратора информационной безопасности о результатах этих операций.

5. Администратор информационной безопасности, обеспечивающий функционирование антивирусного программного обеспечения ИС обязан:

– проверять информацию о наличии обновлений версий базы вирусных сигнатур и сканирующего модуля;

– выявлять попытки инфицирования средств вычислительной техники ИС, разбираться в их причинах (при необходимости с привлечением сотрудников, ответственных за эти средства вычислительной техники). При невозможности выяснить причины простыми (штатными) действиями либо в случае, если определен злой умысел, немедленно сообщить директору МБОУ «СОШ № 2» г. Симферополя;

– принимать и обрабатывать по мере поступления все сообщения о действиях антивирусного программного обеспечения;

– при вирусной атаке с конкретного средства вычислительной техники, немедленно отключить (постоянно или временно) это средство вычислительной техники от сетевого оборудования;

– анализировать все системные журналы антивирусного программного обеспечения для составления общего отчета, после завершения мероприятий очищать данные журналы и «карантинные зоны» за истекший месяц.

IV. Действия работников МБОУ «СОШ № 2» г. Симферополя при обнаружении компьютерного вируса

1. 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 и т.п.) работник МБОУ «СОШ № 2» г. Симферополя самостоятельно или вместе с администратором информационной безопасности должен провести внеочередной антивирусный контроль АРМ.

2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов, работники МБОУ «СОШ № 2» г. Симферополя обязаны:

– приостановить работу на средствах вычислительной техники;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора информационной безопасности.

3. Администратор информационной безопасности должен провести анализ необходимости дальнейшего их использования и провести очистку или уничтожение зараженных файлов.

V. Порядок восстановления информации и работоспособности средств вычислительной техники в случае реализованного вирусного воздействия

Администратор информационной безопасности для ликвидации последствий воздействия вируса и восстановления информации обязан:

– выполнить действия, определенные настоящей Инструкцией и направленные на пресечение распространения вируса по сетевой инфраструктуре (изолировать инфицированное средство вычислительной техники);

– обеспечить получение новой базы вирусных сигнатур;

– выполнить действия по удалению тела вируса из всех зараженных файлов на всех средствах вычислительной техники, подвергшихся атаке;

– восстановить работоспособность средств вычислительной техники;

– обеспечить восстановление модифицированной (поврежденной) информации с применением системы резервного копирования и восстановления при невозможности очистки зараженных файлов.

VI. Ответственность при организации антивирусной защиты

1. Ответственность за обеспечение доступа к дистрибутивам и дополнениям антивирусных средств, своевременное обновление их версий, а также за оповещение о новых версиях несет администратор информационной безопасности.

2. Ответственность за организацию и контроль функционирования антивирусной защиты на средствах вычислительной техники ИС, обнаружение инфицированных объектов возлагается на администратора информационной безопасности.

3. Ответственность за работоспособность, корректную работу и своевременную проверку АРМ, а также поступающей и исходящей электронной почты несет администратор информационной безопасности.

4. За разработку или умышленное распространение компьютерных вирусов, троянских программ, макровирусов и других вредоносных программ работники МБОУ «СОШ № 2» г. Симферополя и сторонних организаций несут ответственность согласно действующему законодательству.

Пронумеровано, прошито и скреплено печатью

4 (четыре) листа

Директор МБОУ «СОШ №2»
Г. Симферополя ***В. А. Кухнина***