«УТВЕРЖДАЮ»

Директор МБОУ г. Керчи РК
«Школа № 15 им. Героя Советского Союза Е.М. Рудневой

Г.А. Спинчевская

приказ № 553
от 07 сентября 2018 года

РЕГЛАМЕНТ
организации антивирусной защиты

Муниципального бюджетного образовательного учреждения

города Керчи Республики Крым

«Школа № 15 имени Героя Советского Союза Е.М. Рудневой»

2018

I. Общие положения

1.1. Целью создания системы антивирусной защиты является обеспечение защищенности информационно-коммуникационной системы (далее ИКС) от воздействия различного рода вредоносных программ и несанкционированных массовых почтовых рассылок, предотвращения их внедрения в информационные системы, выявления и безопасного удаления из систем в случае попадания, а также фильтрации доступа пользователей МБОУ г. Керчи РК «Школа № 15 им. Героя Советского Союза Е.М.Рудневой» (далее ОО) к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

1.2. Основополагающими требованиями к системе антивирусной защиты являются:

- решение задачи антивирусной защиты должно осуществляться в общем виде;
- средство защиты не должно оказывать противодействие только конкретному вирусу или группе вирусов, противодействие должно оказываться в предположениях, что вирус может быть занесен на компьютер и о вирусе (о его структуре (в частности, сигнатуре) и возможных действиях) ничего неизвестно;
- решение задачи антивирусной защиты должно осуществляться в реальном времени.

3. Мероприятия, направленные на решение задач по антивирусной защите:
3.1. установка только лицензированного программного обеспечения либо бесплатного антивирусного программного обеспечения;
3.2. регулярное обновление и еженедельные профилактические проверки;
3.3. непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах ИКС;
3.4. ежедневный анализ, ранжирование и предотвращение угроз распространения и воздействия вредоносных программ путем выявления уязвимостей используемого в ИКС операционного программного обеспечения и сетевых устройств и устранения обнаруженных дефектов в соответствии с данными поставщика программного обеспечения и других специализированных экспертных антивирусных служб;
3.5. проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание

специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур;

3.6. проведение регулярных проверок целостности критически важных программ и данных;

3.7. наличие лишних файлов и следов несанкционированного внесения изменений должно быть зарегистрировано в журнале и расследовано: внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования;

3.8. соблюдение установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения;

3.9. наличие планов обеспечения бесперебойной работы школы для случаев вирусного заражения, в том числе планы резервного копирования всех необходимых данных и программ и их восстановления. Эти меры особенно важны для сетевых файловых серверов, поддерживающих большое количество рабочих станций.

2. Технологические инструкции.

1.Директор школы назначает лицо, ответственное за антивирусную защиту.

2. В школе может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.

3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, почтовые сообщения), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация, находящаяся на съемных носителях (CDROM, DVD, flash-накопителях и т.п.).

4. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

5. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

3. Требования к проведению мероприятий по антивирусной защите.

3.1.В начале работы при загрузке компьютера в автоматическом режиме должно выполняться обновление антивирусных баз и серверов.

3.2. Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю.

3.3.Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

- непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка на серверах и персональных компьютерах школы;
- 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.);

3.4. При отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

3.5. В случае обнаружения зараженных вирусами файлов или электронных писем пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты (в случае его отсутствия - директора) школы;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

4.Ответственность

4.1. Ответственность за организацию антивирусной защиты возлагается на директора школы или лицо, им назначенное.

4.2. Ответственность за проведение мероприятий антивирусного контроля в школе возлагается на ответственного за обеспечение антивирусной защиты, соблюдение требований настоящей Инструкции при работе на пер-

сональных рабочих станциях возлагается на пользователей данных станций или педагога, отвечающего за работу компьютерного класса.

3. Периодический контроль состояния антивирусной защиты по вопросам регламентации доступа к информации в сети Интернет два раза в год (ноябрь, апрель) и фиксируется в Журнале проверок антивирусной защиты в школе.