УТВЕРЖДЕНО:
Директор МАОУ «Косулинская СОШ №8»
_____И.А.Храмцова
Приказ № ___ от «__» ____2022 г

Регламент работы по организации антивирусной безопасности компьютеров в МАОУ «Косулинская СОШ № 8»

1. 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 муниципального автономного общеобразовательного учреждения «Косулинская СОШ № 8»» (далее – Школа) к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

1.2. Основополагающими требованиями к системе антивирусной защиты Школы являются:

– решение задачи антивирусной защиты должно осуществляться в общем виде. Средство защиты не должно оказывать противодействие 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 не известно;

– решение задачи антивирусной защиты должно осуществляться в реальном времени.

1.3. Мероприятия, направленные на решение задач по антивирусной защите:

– установка только лицензированного программного обеспечения либо бесплатное антивирусное программное обеспечение, идущее в комплекте с подлинной операционной системой;

– регулярное обновление и ежедневные профилактические проверки (желательно в нерабочее ночное время);

– непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах ИКС;

– 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.

– 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.

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

– необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения;

– следует иметь планы 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.

1.4. Запрещается использование компьютеров «точки доступа к Интернет» Школы без установленного на них антивирусного программного обеспечения с регулярно обновляемыми антивирусными базами.

1.5. Для большей степени защиты от вирусов и других вредоносных программ необходимо совместное использование антивирусного программного обеспечения, брандмауэра, обнаруживающего сетевые атаки и «шпионское» программное обеспечение, и регулярного резервного копирования пользовательских данных.

1.6. В случае наличия в Школе других компьютеров кроме автоматизированного рабочего места «точки доступа к Интернету» необходимо принять меры к обеспечению и их антивирусной защиты.

2. Технологические инструкции

2.1. В Школе руководителем назначается лицо, ответственное за антивирусную защиту, в должностную инструкцию для которого прописаны порядок действия в период вирусных эпидемий, порядок действий при возникновении внештатных ситуаций, связанных с работоспособностью средств антивирусной защиты, порядок действий для устранения последствий заражений.

2.2. В Школе может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.

2.3. 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 (магнитных дисках, лентах, CD-ROM, DVD, flash- накопителях и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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

3. Подготовка к работе «точки доступа к Интернет»

3.1. Перед вводом в эксплуатацию «точки доступа к Интернет» необходимо проверить не только факт наличия на компьютерах антивирусного программного обеспечения, но и правильность его настроек. В частности, корректность настроек для обновления антивирусных баз с веб-сайта производителя антивирусной программы, запуск при загрузке компьютера резидентного антивирусного монитора (программы-сторожа), настройки резидентного антивирусного монитора на сканирование наиболее уязвимых типов файлов и электронной почты.

3.2. Подготовить и разместить на видном месте краткую памятку для ответственного за «точку доступа к Интернет» и ее пользователей по работе антивирусной защиты. В памятке указать возможные действия антивирусной программы (появляющиеся диалоговые окна) в случае заражения вирусом или появления подозрительных объектов и соответствующие действия

пользователя компьютера.

3.3. Не допускать к самостоятельной работе на компьютерах «точки доступа к Интернет» лиц не прошедших предварительного инструктажа по антивирусной безопасности. Факт прохождения инструктажа фиксировать в специальном журнале учета.

4. В процессе работы «точки доступа к Интернет»

4.1. Проводить регулярное обновление антивирусных баз не реже двух раз в неделю на всех компьютерах Школы.

4.2. Проводить регулярное резервное копирование на внешние носители памяти (CD-ROM, DVD-ROM) всей важной пользовательской информации не реже 1 раза в месяц на всех компьютерах Школы.

4.3. Перед использованием внешних носителей информации (дискет, CD-ROM, флеш-накопителей и т.п.) проверять их на наличие вирусов и опасных программ.

4.4. В случае корректной работы резидентного антивирусного монитора (программы-сторожа) полученная из Интернета информация (документы, программы и т.п.) будет проверяться на вирусы автоматически. В противном случае проверку всех скачиваемых файлов необходимо провести вручную.

5. Действия при обнаружении вируса

5.1. При обнаружении антивирусной защитой «точки доступа к Интернет» вируса или вредоносной программы необходимо выполнить:

1. лечение зараженного файла;
2. удаление зараженного файла, если лечение невозможно;
3. блокирование зараженного файла, если его невозможно удалить.

5.2. В случае блокирования зараженного файла необходимо принять меры к его удалению. Например, при перезагрузке компьютера или при загрузке операционной системы в «Безопасном режиме».

5.3. Если устранение вирусной опасности своими силами не получается, то необходимо связаться с технической поддержкой производителя антивирусной программы (по электронной почте, телефону или через специальный форум на веб-сайте производителя) для получения консультаций.

6. Обеспечение антивирусной безопасности по прошествии срока действия лицензии, входящей в комплект поставки автоматизированного рабочего места «точки доступа к Интернет»

6.1. Необходимо продлить срок действия лицензии на антивирусное программное обеспечение, предусмотрев на следующий год оплату ее стоимости из бюджетных или внебюджетных средств Школы.

6.2. Школа имеет право, самостоятельно решить будет ли продлеваться лицензия на текущую антивирусную программу или же будет приобретена другая программа, в большей степени удовлетворяющая потребности данного конкретного учреждения. Выбор антивирусной программы может производиться как среди коммерческих (платных) программ, так и среди распространяемых бесплатно.

6.3. В случае использования коммерческих антивирусных программ необходимо учитывать, что практически все производители предоставляют, во-первых, скидки для

образовательных учреждений, а, во-вторых, скидки при продлении лицензии.

7. Требования к проведению мероприятий по антивирусной защите

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

7.2. Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю, данные, расположенные на рабочих станциях пользователей — ежедневно, в ночное время по расписанию.

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

7.3.1. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка на серверах и персональных компьютерах учреждения.

7.3.2. 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.).

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

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

2 приостановить работу;

3 немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты (в случае его отсутствия — директора) Школы;

4 совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

5 провести лечение или уничтожение зараженных файлов.

8. Ответственность

8.1. Ответственность за организацию антивирусной защиты возлагается на руководителя Школы или лицо, им назначенное.

8.2. Ответственность за проведение мероприятий антивирусного контроля в Школе возлагается на ответственного за обеспечение антивирусной защиты, соблюдение требований настоящего Регламента при работе на персональных рабочих станциях возлагается на пользователей данных станций или педагога, отвечающего за работу компьютерного класса.

8.3. Периодический контроль за состоянием антивирусной защиты в Школе осуществляется ответственным лицом и фиксируется Актом проверки (не реже 1 раз в квартал).