Принято педагогическим советом
протокол № 1
от «25» 01 2021 г.

Утверждено
директор _____ О.Н. Баклашова
Введено в действие
приказом № 26 от «25» 01 2021 г.

ПОЛОЖЕНИЕ
об организации антивирусной защиты
компьютеров и информационных систем

I. Общие положения.

1.1. Настоящее Положение разработано в целях осуществления антивирусной защиты информационных ресурсов, определения системы мер, направленных на защиту автоматизированных рабочих мест в МБОУ «Гимназия № 6» (далее – Учреждение) от несанкционированного копирования, модификации и разрушения, а также нарушения работы программного обеспечения Учреждении при воздействии вирусов и других вредоносных программ.

1.2. Настоящее Положение определяет порядок применения средств антивирусной защиты в Учреждении, задачи, обязанности, права и ответственность пользователей средств антивирусной защиты, порядок установки, обновления и применения средства антивирусной защиты, а также порядок ликвидации последствий воздействия программных вирусов и других вредоносных программ.

1.3. Требования настоящего Положения обязательны для выполнения всеми лицами, использующими средства вычислительной техники Учреждения.

1.4. Руководство обеспечением антивирусной защиты информации в Учреждении осуществляет руководитель. Контроль за выполнением настоящего Положения осуществляет заместитель директора по АХЧ.

1.5. Данное Положение размещается на официальном сайте МБОУ «Гимназия № 6» в информационно-телекоммуникационной сети «Интернет».

II. Цель организации антивирусной защиты.

2.1. Целью организации антивирусной защиты является:
- защита информационных ресурсов Учреждения от несанкционированного копирования, искажения и разрушения;
- минимизация риска сбоев и отказов в работе технологических и информационных процессов, при воздействии вирусов и других вредоносных программ;
- минимизация финансовых потерь и трудовых затрат при устранении последствий воздействия вредоносного кода.

III. Основные требованиями к системе антивирусной защиты.

3.1. Основными 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.

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

- установка только лицензированного программного обеспечения либо бесплатного антивирусного программного обеспечения;
- регулярное обновление и еженедельные профилактические проверки;
- 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.

3.3. Во избежание заражения АРМ вредоносным ПО всем пользователям необходимо соблюдать следующие правила:

3.3.1. В случае сомнений в наличии или в корректной работе на компьютере антивирусного ПО необходимо незамедлительно сообщить об этом непосредственному руководителю.

3.3.2. Никогда не открывать никакие файлы, находящиеся во вложениях к электронным письмам, которые отправлены с подозрительных или неизвестных Вам адресов. Не пересылайте их другим адресатам. В случае получения таких писем следует немедленно их удалить из папки «Входящие», а затем удалить их из папки «Удаленные» для того, чтобы исключить возможность их восстановления.

3.3.3. В случае возникновения подозрений на наличие зараженных файлов во вложениях к сообщениям электронной почты (к примеру, подозрительные имена или расширения файлов вложений, подозрительный источник сообщения, неизвестный отправитель с адресом электронной почты публичного почтового сервиса), которые, однако могут быть полезны пользователю, необходимо незамедлительно сообщить об этом специалисту по защите информации для проведения проверки подозрительною сообщения.

3.3.4. Никогда не загружайте файлы и не соглашаться на предложения загрузить или установить программное обеспечение с неизвестных Вам Интернет сайтов.

3.3.5. Избегайте использования на рабочих местах съемных носителей информации без служебной необходимости, особенно если эти носители получены из неизвестных или подозрительных источников или могли использоваться на других компьютерах, возможно, незащищенных антивирусными программами. Допускается самостоятельно осуществлять антивирусные проверки при помощи штатного антивирусного программного обеспечения, установленного на рабочих местах.

3.3.6. Не допускать к рабочим местам других лиц, блокируйте доступ к Вашим компьютерам при помощи комбинации клавиш Win+L или Ctrl-Alt-Del на время Вашею отсутствия на рабочем месте.

3.3.7. Для совместной работы или хранения важной, конфиденциальной информации, используйте сетевые ресурсы на файловом хранилище, специально для этого предназначенные. В случае появления сообщений антивирусного программного обеспечения об обнаружении угрозы убедитесь, что угроза успешно предотвращена.

3.3.8. При заражении компьютера вредоносным ПО характерны следующие признаки:
- значительное увеличение времени отклика компьютера на Ваши действия в любых программах;
- появление сообщений об ошибках;
- необъяснимая потеря файлов, изменение дат обновления и увеличение размера файлов;
- системные сбои (включая случаи, когда операционная система перестает загружаться);
- любые другие необычные явления в работе компьютера.

3.3.9. Если у пользователя возникают подозрения в заражении Вашего компьютера вирусом, следует незамедлительно сообщать об этом в обслуживающую организацию. Это позволит минимизировать ущерб, наносимый компьютерным вирусом, и принять необходимые меры ятя предотвращения повторною заражения.

3.3.10. Пользователю средствами антивирусной защиты запрещается отключать средства антивирусной защиты информации.

3.3.11. Каждый работник Учреждения несет ответственность за невыполнение или недобросовестное выполнение перечисленных выше обязанностей.

IV. Порядок применения средств антивирусной защиты информации.

4.1. Средства антивирусной защиты устанавливаются на всех средствах вычислительной техники, эксплуатируемой в Учреждении. При технологической необходимости на отдельные средства вычислительной техники средства антивирусной защиты могут не устанавливаться. Лучшей практикой считается централизованная установка, настройка и контроль работы средства антивирусной защиты.

4.2. Все средства антивирусной защиты работают в режиме мониторинга в реальном времени. Проверяются все файлы на локальных и сетевых жестких дисках, съемных носителях, в приложениях к письмам электронной почты, загружаемые из Интернета и др. Не допускается отключение работы средства антивирусной защиты.

4.3. Производится еженедельная, по централизованно установленному расписанию, полная проверка жестких магнитных дисков.

4.4. В случае подозрения на наличие вредоносных программ проводится внеплановая проверка жестких магнитных дисков и съемных носителей

4.5. Обновление антивирусных баз производится автоматически по централизованно установленному расписанию. Не допускается отключение автоматического обновления средства антивирусной защиты.

4.6. Выполнение предварительной проверки на отсутствие вредоносного кода программного обеспечения, устанавливаемого или изменяемого на средствах вычислительной техники, включая банкоматы и платежные терминалы, а также проверки на отсутствие вредоносного кода после установки или изменения программного обеспечения.

4.7. При обнаружении вредоносного кода средства антивирусной защиты должны немедленно известить об этом пользователя и удалить вредоносный код или заблокировать его работу.

V. Порядок инсталляциии настройки средств антивирусной защиты информации.

5.1. Установка средств антивирусной защиты на автоматизированных рабочих местах осуществляется системными администраторами обслуживающей организации. Регулярное обновление осуществляется пользователем АРМ.

5.2. Инсталляция и настройка средства антивирусной защиты производится в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.

5.3. После инсталляции средства антивирусной защиты конфигурируются в соответствии со следующими требованиями:

- загрузка средства антивирусной защиты должна выполняться автоматически при включении компьютера;
- средства антивирусной защиты должно постоянно работать в режиме фонового монитора;
- периодически средства антивирусной защиты должно запускаться на сканирование всех жестких дисков;
- обновление антивирусных баз производится автоматически;
- при обнаружении вируса пользователь должен быть немедленно извещен об этом антивирусной программой;
- протоколы работы средства антивирусной защиты должны храниться не мене 30 суток.

5.4. Каждый компьютер, работающий в Учреждении, должен быть настроен следующим образом:

- отключена функция автозапуска съемных носителей;
- настроено автоматическое обновление операционной системы;
- пользователь в домене не должен иметь администраторских прав на локальном компьютере.

При технологической необходимости на отдельные средства вычислительной техники средства антивирусной защиты могут быть настроены иным образом.

VI. Заключительные положения.

6.1. Положение вступает в силу с момента его утверждения.

6.2. Положение является локальным актом образовательного учреждения. Внесение изменений и дополнений в Положение осуществляется в порядке его принятия.

6.3. Настоящее Положение может быть изменено (дополнено) локальным актом образовательного учреждения.