РАССМОТРЕНО И РЕКОМЕНДОВАНО
к утверждению на заседании
педагогического совета
протокол № 6
от «11» ноября 2019 г.

УТВЕРЖДАЮ:
Директор МАОУ «Школа №5»
«СОШ №5» В.Н. Новиков
Приказ № 467/4 «11» 11 2019 г.

Положение
по антивирусной защите
Муниципальное автономное общеобразовательное учреждение
« Школа №5»

1. Общие положении

1.1 Настоящее положение разработано в соответствии с Федеральным законом РФ «О персональных данных» от 27 июля 2006 г. № 152-ФЗ (ред. от 29.07.2017 № 223-ФЗ), Постановлением Правительства РФ от 07.10.2017 г. N 1235 "Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства образования и науки Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства образования и науки Российской Федерации, и формы паспорта безопасности этих объектов (территорий)», Постановлением Правительства Российской Федерации от 02.08.2019 №1006 «Об утверждении требований к антитеррористической защищенности объектов (территории) Министерства просвещения Российской Федерации и объектов (территории), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)»., приказами Управления образования, МАОУ «Школа № 5» и регламентирует порядок организации и осуществления контрольно-пропускного режима в учреждении.

2. Мероприятия по антивирусной защите информационных ресурсов учреждения:

- целью создания системы антивирусной защиты является обеспечение защищенности информационно-коммуникационной системы учреждения 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 учреждения к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

Основополагающими требованиями к системе антивирусной защиты учреждения 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.

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

3.1. Необходимо проводить политику, требующую установки только лицензированного программного обеспечения;

3.2. Антивирусные программные средства должны регулярно обновляться и использоваться для профилактических проверок (желательно ежедневных);

3.3. Непрерывный контроль над всеми возможными путями проникновения вредоносных программ в ИТКС Учреждения, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах ИТКС;

3.4 Ежедневный анализ, ранжирование и предотвращение угроз распространения и воздействия вредоносных программ путем выявления уязвимостей используемого в ИТКС программного обеспечения ОС и сетевых устройств и устранения обнаруженных дефектов в соответствии с данными поставщика ПО 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.

Необходимо проводить регулярную проверку целостности критически важных программ и данных. Наличие лишних файлов и следов несанкционированного внесения изменений должно быть зарегистрировано в журнале и расследовано;

- дискеты, диски, дисковые накопители любого типа неизвестного происхождения следует проверять на наличие вирусов до их использования;

- необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения АИС компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения;

- следует иметь планы обеспечения бесперебойной работы организации 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.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат 220231410850983616603994243094623231406491098 35

Владелец Новиков Виктор Николаевич

Действителен С 19.09.2022 по 19.09.2023