№5

МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
СВЕРДЛОВСКОЙ ОБЛАСТИ
государственное автономное профессиональное образовательное учреждение
Свердловской области
«Серовский техникум сферы обслуживания и питания»

Утверждаю:
директор техникума
_____ И.П. Новикова
«01» апреля 2015 г.

Регламент организации антивирусной защиты
ГАПОУ СО «Серовский техникум сферы обслуживания и питания»

I. Общие положения

1. Настоящий Регламент организации антивирусной защиты в ГАПОУ СО «Серовский техникум сферы обслуживания и питания»(далее - техникум) разработан в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных», Федеральным законом Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Трудовым кодексом Российской Федерации (далее – ТК РФ), Федеральным Законом РФ от 29.12.2012 года №273-ФЗ «Об образовании в РФ», Положением об обработке и защите персональных данных в ГАПОУ СО «Серовский техникум сферы обслуживания и питания».

2. 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 техникума к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

II. Основные положения

1.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.

2.Основополагающими требованиями к системе антивирусной защиты техникума являются:

- решение задачи антивирусной защиты должно осуществляться в общем виде.
- решение задачи антивирусной защиты должно осуществляться в реальном времени.

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 (типа MicrosoftSecurityEssentials (сеть до 10 рабочих станций) или MicrosoftForefrontEndpointProtection (сеть более 10 рабочих станций)), поддерживающее работу с пользовательскими профилями.
- 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;
- имеются планы обеспечения бесперебойной работы техникума 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.

4.Технологические инструкции

4.1. В техникуме директором назначено лицо, ответственное за антивирусную защиту, в должностные инструкции 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.

4.2. В техникуме используется только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.

4.3. 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).

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

5. Требования к проведению мероприятий по антивирусной защите

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

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

5.3. 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 учреждения.

-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.).

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

5.4. 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 техникума).

- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.

- провести лечение или уничтожение зараженных файлов.

6. Ответственность за организацию антивирусной защиты.

6.1. Ответственность за организацию антивирусной защиты возлагается на лицо, назначенное директором техникума по приказу.

6.2. Ответственность за проведение мероприятий антивирусного контроля в техникуме возлагается на ответственного за обеспечение антивирусной защиты, соблюдение требований настоящей Инструкции при работе на персональных рабочих станциях возлагается на пользователей данных станций или педагога, отвечающего за работу компьютерного класса.

6.3. Периодический контроль за состоянием антивирусной защиты в техникуме осуществляется директором и фиксируется Актом проверки (не реже 1 раз в квартал).

III.Заключительные положения

1. Настоящий Регламент вступает в силу с момента его утверждения директором техникума и действует бессрочно, до замены его новым Регламентом.

2. Все изменения в Регламент вносятся приказом директора техникума.