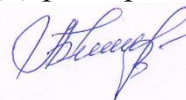


УТВЕРЖДАЮ
Директор школы



А.В.Белкина

Приказ от 27.10.2016 №281



Инструкция по организации антивирусной защиты в НРМОБУ «Усть-Юганская СОШ»

1. Общие положения

1.1. Настоящая инструкция предназначена для проведения антивирусного контроля в Нефтеюганском районном муниципальном общеобразовательном бюджетном учреждении «Усть-Юганская средняя общеобразовательная школа» (далее НРМОБУ «Усть-Юганская СОШ») и предотвращения возникновения фактов заражения программного обеспечения (далее ПО) компьютерными вирусами, а также фильтрации доступа пользователей к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

1.2. Директором школы назначается лицо, ответственное за организацию антивирусной защиты в НРМОБУ «Усть-Юганская СОШ».

1.3. В НРМОБУ «Усть-Юганская СОШ» может использоваться только лицензионное антивирусное ПО либо свободно-распространяемое ПО.

1.4. Установка, настройка и регулярное обновление антивирусных средств осуществляется только ответственным за организацию антивирусной защиты в НРМОБУ «Усть-Юганская СОШ».

1.5. 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 съёмных носителях (CD-ROM, DVD, flash-накопителях и т.п.).

1.6. Контроль информации на съёмных носителях производится непосредственно перед её использованием.

1.7. Файлы, помещаемые в электронный архив или на сервер, должны в обязательном порядке проходить антивирусный контроль.

1.8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

2. Мероприятия, направленные на решение задач по антивирусной защите

2.1. Установка только лицензированного ПО либо бесплатного антивирусного ПО.

2.2. Регулярное обновление и профилактические проверки;

2.3. Непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах информационно-коммуникационной системы (далее ИКС) НРМОБУ «Усть-Юганская СОШ».

2.4. 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.

2.5. Внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования.

2.6. Необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения.

2.7. Обеспечение бесперебойной работы НРМОБУ «Усть-Юганская СОШ» для случаев вирусного заражения, в том числе резервного копирования всех необходимых данных и программ и их восстановления.

3. Требования к проведению мероприятий по антивирусной защите

3.1. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС – при перезагрузке) в автоматическом режиме должно выполняться обновление антивирусных баз и серверов и проводиться антивирусный контроль всех дисков и файлов персонального компьютера и съёмных носителей.

3.2. Периодические проверки компьютеров 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) ПО компьютера (ЛВС) должна быть выполнена антивирусная проверка на серверах и персональных компьютерах НРМОБУ «Усть-Юганская СОШ»;

- 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.

4. Действия сотрудников при обнаружении компьютерного вируса

4.1. В случае обнаружения зараженных компьютерными 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 НРМОБУ «Усть-Юганская СОШ»;

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

- провести лечение или уничтожение зараженных файлов.

4.2. При возникновении подозрения на наличие компьютерного вируса ответственный за организацию антивирусной защиты должен провести внеочередной антивирусный контроль.

5. Ответственность

5.1. Ответственность за организацию антивирусной защиты и выполнение положений данной инструкции возлагается на лицо, назначенное директором НРМОБУ «Усть-Юганская СОШ».

5.2. Ответственность за соблюдение требований настоящей Инструкции при работе на персональных рабочих ПК возлагается на пользователей данных ПК или педагога, отвечающего за работу компьютерного класса.

