



УТВЕРЖДАЮ
Директор ГБПОУ
Республики Марий Эл «ЙОСТ»
И.С. Зяблицева
« » 2020г.

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ

1. Общие положения

1.1. Настоящая инструкция предназначена для организации порядка проведения антивирусного контроля в ГБПОУ Республики Марий Эл «Йошкар-Олинский строительный техникум»

и предотвращения возникновения фактов заражения программного обеспечения учреждения компьютерными вирусами.

1.2. В ГБПОУ Республики Марий Эл «Йошкар-Олинский строительный техникум» может использоваться только лицензионное антивирусное программное обеспечение.

2. Установка и обновление антивирусных средств

2.1. Установка, настройка и регулярное обновление антивирусных средств осуществляется ответственным за обеспечение антивирусной защиты.

3. Требования к проведению мероприятий по антивирусной защите

3.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

3.2. Файлы, помещаемые на сервер, должны в обязательном порядке проходить антивирусный контроль.

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

3.4. Контроль информации на съемных носителях производится непосредственно перед её использованием.

3.5. Особое внимание следует обратить на недопустимость использования съемных носителей, принадлежащих лицам, временно допущенным к работе на ЭВМ в ГБПОУ Республики Марий Эл «Йошкар-Олинский строительный техникум» (обучающиеся, участники совещаний, студенты-практиканты и т.п.). Работа этих лиц должна проводиться под непосредственным контролем сотрудника или ответственного за обеспечение антивирусной защиты, особенно если работа происходит с использованием ресурсов локальной вычислительной сети.

3.6. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС - при перезапуске) в автоматическом режиме должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех дисков и файлов персонального компьютера.

3.7. Периодические проверки компьютеров должны проводиться не реже одного раза в неделю. 3.8. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

3.8.1. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка: на серверах и персональных компьютерах ГБПОУ Республики Марий Эл «Йошкар-Олинский строительный техникум». Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего.

3.8.2. 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.) сотрудник техникума самостоятельно или вместе с ответственным за антивирусную защиту техникума, должен провести внеочередной антивирусный контроль своей рабочей станции.

4. Действия сотрудников при обнаружении компьютерного вируса

4.1. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

4.1.1. приостановить работу;

4.1.2. немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение информационной безопасности в учреждении;

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

4.1.4. провести лечение или уничтожение зараженных файлов;

4.1.5. в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, ответственный за антивирусную защиту обязан направить зараженный вирусом файл на гибком магнитном диске в организацию, с которой заключен договор на антивирусную поддержку для дальнейшего исследования;

4.2. При возникновении подозрения на наличие компьютерного вируса сотрудник или ответственный за информационную безопасность должны провести внеочередной антивирусный контроль.

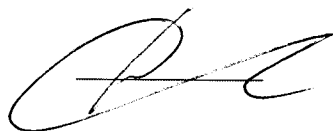
5. Ответственность при организации антивирусной защиты

5.1. Ответственность за организацию антивирусной защиты возлагается на руководителя образовательного учреждения или ответственного за обеспечение антивирусной защиты;

5.2. Ответственность за проведение мероприятий антивирусного контроля в образовательном учреждении и соблюдение требований настоящей инструкции возлагается на ответственного за обеспечение антивирусной защиты;

5.3. Периодический контроль состояния антивирусной защиты в образовательном учреждении осуществляется руководителем.

Инструкцию разработал:



/ М.В. Руденко /