Государственное профессиональное образовательное учреждение Тульской области «Тульский колледж профессиональных технологий и сервиса» (ГПОУ ТО «ТКПТС»)

УТВЕРЖДАЮ
Директор
_____ С.С. Курдюмов
«31» 01 2017 г.

ПОЛОЖЕНИЕ
31.01. 2017 г. № 202/1

Об антивирусной защите

1. Общие положения

1.1. Настоящее положение определяет требования к организации защиты средств информатизации от разрушающего воздействия компьютерных вирусов, порядок организации работ по антивирусной защите средств информатизации в ГПОУ ТО «ТКПТС» (далее Колледж), устанавливает ответственность пользователей и должностных лиц по антивирусной защите средств информатизации.

1.2. 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.

1.3. Средства антивирусной защиты информации должны устанавливаться на всех средствах вычислительной техники, используемых в ГПОУ ТО «ТКПТС».

1.4. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в ГПОУ ТО «ТКПТС».

1.5. Требования настоящего Положения распространяются на всех работников подразделений, использующих в работе средства вычислительной техники (включая работу в локальной вычислительной сети Колледжа) и должны применяться для всех средств вычислительной техники, эксплуатируемой в Учреждении.

1.6. Организационное обеспечение мероприятий антивирусного контроля и контроль за действиями пользователей возлагается на инженера-электроника.

2. Основные термины, сокращения и определения

2.1. **АС – автоматизированная система Колледжа** – система, обеспечивающая хранение, обработку, преобразование и передачу информации Учреждения с использованием компьютерной и другой техники.

2.2. **Компьютерный вирус** - программа, способная создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты или ресурсы компьютерных систем, сетей и так далее без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения.

2.3. **Зараженная программа** - это программа, содержащая внедренную в нее программу-вирус.

3. Организация системы антивирусного контроля

3.1. Целью мероприятий по антивирусному контролю является предотвращение потерь информации в АС Колледжа.

3.2. Задачами антивирусной защиты являются:

— определение состава и регламента запуска антивирусных диагностических средств, регламента их ревизии и обновления;

— проведение профилактических работ с применением антивирусных диагностических средств;

— непрерывное обеспечение защиты информации от действия вредоносных программ на всех этапах эксплуатации АС Учреждения.

3.3. К использованию в Учреждении допускаются только лицензионные антивирусные средства, закупленные у разработчиков (поставщиков) указанных средств.

3.4. Установка средств антивирусной защиты и настройка их параметров в соответствии с руководствами по применению конкретных антивирусных

средств на компьютерах в ГПОУ ТО «ТКПТС» осуществляется инженером-электроником.

3.5. Обновление антивирусных баз должно производиться не реже 1 раза в сутки автоматически, согласно возможностям программного обеспечения. В случае сбоя автоматического обновления обновление баз производится вручную с той же периодичностью.

3.6. Обязательному входному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация на съемных носителях и мобильных устройствах.

3.7. Файлы резервных копий, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

3.8. Мероприятия по антивирусной защите на компьютерах в ГПОУ ТО «ТКПТС» включают в себя:

— профилактику вирусного заражения;

— анализ ситуаций;

— применение средств антивирусной защиты;

— проведение расследований инцидентов связанных с вирусами.

4. Профилактика вирусного заражения

4.1. В целях исключения появления и распространения вирусов на рабочих станциях АС Учреждения должны регулярно проводится профилактические мероприятия. К основным профилактическим работам и мероприятиям относятся:

— ежедневная автоматическая проверка наличия вирусов по расписанию;

— регулярная (не реже одного раза в квартал) выборочная проверка

рабочих станций и серверов на наличие вирусов, даже при отсутствии внешних проявлений вирусов;

— проверка наличия вирусов на рабочих станциях, вернувшихся с ремонта (в том числе гарантийного) в сторонних организациях;

— создание резервной копии программного продукта сразу же после приобретения;

— установка защиты от записи на съемные носители информации, где это возможно и необходимо;

— тщательная проверка всех поступающих и купленных программ и баз данных;

— ограничение доступа к компьютеру посторонних лиц.

4.2. Создание резервной копии программного продукта равно как и остальные профилактические работы и мероприятия выполняются ответственным за антивирусный контроль.

4.3. При обнаружении вирусов на компьютере, работающем в локальной сети, проверке подлежат все компьютеры, включенные в эту сеть и работающие с общими данными и программным обеспечением.

5. Анализ ситуаций

5.1. При сообщении антивирусных программы о подозрении на наличие вирусов на рабочей станции, необходимо приостановить работу и немедленно известить об этом ответственного за антивирусный контроль, а также других пользователей и подразделения, использующие эти файлы в работе, если зараженные файлы являются совместно используемыми.

5.2. Анализ ситуации наличия вирусов выполняется ответственным за антивирусный контроль в Учреждении. При анализе могут дополнительно использоваться специальное программное обеспечение для обнаружения вирусов.

5.3. В ходе анализа ситуации обязательно требуется определить источник

заражения. Если источником заражения является съемный носитель либо другая рабочая станция, то необходимо проверить на наличие вирусов рабочую станцию - источник заражения. В случае заражения через глобальную сеть Интернет или по электронной почте следует немедленно заблокировать ресурс или адрес электронной почты – источник заражения.

6. Применение средств антивирусной защиты

6.1. Уничтожение вирусов выполняется ответственным за антивирусный контроль в Учреждении.

6.2. После уничтожения вирусов и восстановления зараженных программ и файлов с данными необходимо еще раз выполнить проверку наличия вирусов, используя антивирусные программы.

7. Ответственность

7.1. Ответственность за выполнение мероприятий по антивирусной защите информации на средствах вычислительной техники, эксплуатируемых подчиненными лицами в подразделении в соответствии с требованиями настоящего Положения, возлагается на руководителя подразделения.

7.2. Ответственность за выполнение мероприятий по антивирусной защите информации на средствах вычислительной техники на рабочем месте, в соответствии с требованиями настоящего Положения, возлагается на пользователя средств вычислительной техники.

7.3. Ответственность за проведение профилактических мероприятий по обеспечению антивирусной защиты в АС Колледжа, а также уничтожение выявленных вирусов возлагается на ответственного за антивирусный контроль.

7.4. Периодический контроль за состоянием антивирусной защиты в АС Учреждения, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящего Положения сотрудниками подразделений осуществляется инженером-электроником.

Приложение 1

Инструкция пользователя по антивирусной защите

Характерные проявления вирусов

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:

— прекращение работы или неправильная работа ранее успешно функционировавших программ;

— медленная работа компьютера;

— невозможность загрузки операционной системы;

— исчезновение файлов и каталогов или искажение их содержимого;

— изменение даты и времени модификации файлов;

— изменение размеров файлов;

— неожиданное значительное увеличение количества файлов на диске;

— существенное уменьшение размера свободной оперативной памяти;

— вывод на экран непредусмотренных сообщений или изображений;

— подача непредусмотренных звуковых сигналов;

— частые зависания и сбои в работе компьютера.

Основные источники вирусов:

— съемный носитель (дискета, флеш-карта, CD-ROM, DVD-ROM, мобильное дисковое устройство) на котором находятся зараженные вирусом файлы;

— компьютерная сеть, в том числе система электронной почты и Интернет;

— жесткий диск, на который попал вирус в результате работы с зараженными программами.

Пользователь обязан:

— ежедневно при начальной загрузке рабочей станции убедиться в загрузке антивирусного программного обеспечения и в случае его отсутствия уведомить ответственного за антивирусный контроль;

— проводить антивирусный контроль всех внешних носителей информации, поступающих со стороны (из внешних организаций, других подразделений Колледжа и т.п.) или полученных по компьютерным сетям (скопированных на общедоступный ресурс локального компьютера другими пользователями.

Во всех случаях возможного проявления действия вирусов, обнаружения файлов, пораженных вирусом или подозрении на наличие вируса сотрудник должен:

— без попытки какого-либо лечения незамедлительно сообщить об этом ответственному за антивирусный контроль и оценить с ним возможные пути заражения и распространения данного вируса;

— совместно с ним провести лечебно-восстановительные мероприятия.

Сотрудник обязан делать резервные копии файлов, содержащих ценную служебную информацию.

Сотрудник не должен самостоятельно устанавливать программное обеспечение, если это не входит в его обязанности. Запрещается устанавливать и запускать нелицензионное или не относящееся к выполнению им своих должностных обязанностей программное обеспечение.

Пользователю запрещается:

— изменять настройки и конфигурацию средств антивирусной защиты;

— удалять или добавлять в систему какие-либо другие средства антивирусной защиты;

— отключать антивирусное программное обеспечение;

— останавливать проверку компьютера и других сменных носителей информации.