




МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ САМАРСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ
«ТОЛЬЯТТИНСКИЙ ХИМИКО-ТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»

УТВЕРЖДАЮ

и. о. директора ГБПОУ «Тольяттинский
химико-технологический техникум»


Т. А. Михайленко

Приказ от «23» января 2019 г. № 6/1-од

Инструкция

**по организации антивирусной защиты информационных систем
ГБПОУ «Тольяттинский химико-технологический техникум»**

СОГЛАСОВАНО

Советом Учреждения
протокол от 22.01.2019 г. № 1

1. Общие положения

- 1.1. Инструкция по проведению антивирусного контроля информационных систем ГБПОУ «Тольяттинский химико-технологический техникум» (далее - Инструкция) регламентирует порядок проведения антивирусного контроля в информационных системах.
- 1.2. Правила, устанавливаемые положениями настоящей Инструкции обязательны для исполнения всеми пользователями информационных систем.
- 1.3. Организационное и техническое обеспечение проведения антивирусного контроля информационных систем Учреждения возлагается на администратора безопасности информационных систем.

2. Порядок проведения антивирусного контроля информационных системах

- 2.1. На рабочих местах информационных систем Учреждения запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации для каждой информационной системы. К использованию в информационных системах допускаются только лицензионные антивирусные средства.
- 2.2. Установка, конфигурирование, управление средствами антивирусной защиты проводится исключительно администратором безопасности информационных систем Учреждения.
- 2.3. Администратор безопасности информационных систем Учреждения еженедельно осуществляет проверку статистики обновлений вирусных баз, обновляет базу вручную в случае необходимости, проводит проверку жестких дисков технических средств, входящих в состав защищаемых информационных систем, на наличие вирусов не реже 1 раза в две недели.
- 2.4. В случае возникновения ошибок при автоматическом обновлении средств антивирусной защиты (появлении диалоговых окон, сообщений об ошибке) пользователь сообщает данную информацию администратору безопасности информационных систем Учреждения.
- 2.5. Администратор безопасности информационных систем Учреждения в случае обнаружения вирусов или сообщения об обнаружении от пользователей принимает меры по выявлению и уничтожению вредоносных программ и недопущению их дальнейшего распространения. При этом в обязательном порядке устанавливает источник (носитель) заражения для принятия соответствующих мер.
- 2.6. Настройка параметров, режимов и функций средств антивирусного контроля осуществляется администратором безопасности информационных систем Учреждения в соответствии с руководствами по применению конкретных антивирусных средств. Должна обеспечиваться периодическая (не реже 1 раза в неделю) автоматическая проверка на предмет наличия вредоносных программ критических областей: корневого раздела системного

жесткого диска, разделов операционной системы (папки: Windows, Program Files), папок средств защиты информации.

2.7. В случае обнаружения не поддающегося лечению вируса, администратор безопасности информационных систем Учреждения обязан удалить инфицированный файл и проверить работоспособность технического средства. В случае отказа технического средства - произвести восстановление соответствующего программного обеспечения.

2.8. Ответственность за организацию антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на руководителя подразделения, эксплуатирующего информационную систему.

2.9. Ответственность за проведение мероприятий антивирусного контроля на своих рабочих станциях и соблюдение требований настоящей Инструкции возлагается на всех пользователей информационных систем Учреждения.

2.10. Перед эксплуатацией средства антивирусной защиты информации, на своих автоматизированных рабочих местах, пользователи знакомятся с «Руководством пользователя», поставляемым в комплекте эксплуатационной документации на средство антивирусной защиты.

2.11. Периодический контроль за состоянием антивирусной защиты в информационных системах Учреждения, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции пользователями осуществляется ответственным за организацию обработки персональных данных в информационных системах.

