Вологодская государственная
молочнохозяйственная академия
им. Н. В. Верещагина

Руководство пользователя
[Инструкция по организации антивирусной защиты]

Центр ИСТ, 2015

Содержание

Общие положения

1. Настоящая инструкция предназначена для организации проведения антивирусного контроля в академии и предотвращения возникновения фактов заражения программного обеспечения компьютерными вирусами и другими вредоносными программами.
2. Инструкция регламентирует действия персонала подразделений при организации антивирусной защиты электронных технологий академии.

Установка и обновление антивирусных средств

1. К применению в академии допускаются только лицензионные профессиональные антивирусные средства, сертифицированные ФСТЭК. Применение антивирусных средств, предназначенных для домашнего использования, не допускается.
2. Установка и настройка антивирусных средств осуществляется сотрудниками Центра ИСТ.
3. Антивирусные средства устанавливаются на все рабочие станции локальной вычислительной сети академии с учётом конкретных особенностей их эксплуатации.
4. Обновление антивирусных баз средств антивирусной защиты должно производиться по возможности не реже 1 раза в день силами пользователей ЭВМ или автоматически.

Порядок проведения антивирусного контроля

1. Устанавливаемое (изменяемое) на ЭВМ программное обеспечение должно быть проверено на отсутствие компьютерных вирусов и других вредоносных программ и закладок. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети) должна быть выполнена антивирусная проверка лицом, установившим (изменившим) программное обеспечение.
2. Настройка антивирусных средств должна обеспечивать постоянный автоматический антивирусный контроль (для серверов ЛВС – при перезапуске).
3. Дополнительный антивирусный контроль электронных архивов, находящихся на серверах, должен проводиться системным администратором локальной вычислительной сети не реже 1 раза в неделю.
4. Обязательному полному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, электронной почтой, а также информация со съёмных носителей (магнитные диски, ленты, флеш-накопителей, CD-ROM и т.п.), получаемых от сторонних лиц и организаций.
5. Контроль информации на съёмных носителях производится перед её использованием непосредственно в подразделениях академии.
6. Особое внимание следует обратить на недопустимость использования съёмных носителей, принадлежащих лицам, временно допущенным к работе на ЭВМ в академии (студенты, практиканты, временно замещающие и т.п.). Работа этих лиц должна проводиться под непосредственным контролем ответственных лиц, особенно если работа происходит с использованием ресурсов локальной вычислительной сети.

Действия сотрудников при обнаружении вредоносных программ или подозрении на их наличие

1. При возникновении подозрения на наличие вредоносных программ сотрудник подразделения, администратор информационной безопасности, или сотрудник, уполномоченный руководителем данного подразделения, должны провести внеочередной полный антивирусный контроль, или при необходимости привлечь специалистов Центра ИСТ для определения ими факта наличия или отсутствия вредоносных программ.
2. При обнаружении вредоносных программ или закладок сотрудник подразделения, администратор информационной безопасности, или сотрудник, уполномоченный руководителем данного подразделения, обязаны: приостановить работу, поставить в известность о факте обнаружения заражённых или испорченных вредоносной программой файлов руководителя подразделения, владельца этих файлов, а также смежные подразделения, использующие эти файлы в работе. Совместно с владельцем заражённых или испорченных файлов провести анализ необходимости дальнейшего их использования, провести лечение их штатными антивирусными средствами. При невозможности или неэффективности лечения уничтожить заражённые или испорченные файлы способами, исключающими их восстановление.

Ответственность при организации антивирусной защиты

1. Ответственность за организацию антивирусной защиты в подразделениях академии и установление порядка её введения возлагается на администратора информационной безопасности.
2. Ответственность за выполнение положений данной инструкции возлагается на администраторов информационной безопасности в подразделениях.
3. Периодический контроль за соблюдением положений данной инструкции возлагается на начальника Центра ИСТ.