

ИНСТРУКЦИЯ

по организации антивирусной защиты компьютерной техники в ПО

1. Общие положения

1.1. В ПО используется только лицензионное антивирусное программное обеспечение.

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 съёмных носителях (магнитных дисках, CD-ROM, твердотельных накопителях, картах памяти и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съёмный носитель).

1.3. Файлы, помещаемые в электронный архив, в обязательном порядке должны подвергаться антивирусному контролю.

1.4. Устанавливаемое (изменяемое) программное обеспечение предварительно проверяется на отсутствие вирусов.

1.5. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения регистрируется в специальном журнале за подписью лица, ответственного за антивирусную защиту.

2. Требования к проведению мероприятий по антивирусной защите

2.1. Ежедневно в начале работы при загрузке компьютера (для серверов локальной сети — при перезапуске) в автоматическом режиме должно выполняться обновление антивирусных баз и должен проводиться антивирусный контроль всех дисков и файлов персонального компьютера.

2.2. Периодические проверки электронных архивов проводятся не реже одного раза в неделю.

2.3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера выполняется:

— непосредственно после установки (изменения) программного обеспечения компьютера (локальной сети); факт выполнения антивирусной

проверки регистрируется в специальном журнале за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего;

– 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.).

2.4. В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов пользователи обязаны:

– приостановить работу;

– немедленно поставить в известность о факте обнаружения заражённых вирусом файлов ответственного за обеспечение информационной безопасности в учреждении;

– совместно с владельцем заражённых вирусом файлов провести анализ необходимости дальнейшего их использования;

– провести лечение или уничтожение заражённых файлов.

2.5. В случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, ответственный за антивирусную защиту направляет заражённый вирусом файл в организацию, с которой заключён договор на антивирусную поддержку, для дальнейшего исследования.

3. Ответственность

3.1. Ответственный за антивирусную защиту компьютерной техники несёт ответственность:

– за организацию антивирусной защиты;

– за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции.

3.2. Пользователь несёт ответственность:

– в случае самостоятельного, преднамеренного отключения антивирусного ПО на рабочей станции;

– в случае использования заведомо заражённого носителя информации.

3.3. Периодический контроль за состоянием антивирусной защиты в ПО осуществляется заместителем директора по информатизации.