?????????? ??
??????????
????????????? ??????

- ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ УЧРЕЖДЕНИЯ «SDU UNIVERSITY»

?????????? ?? ????????? ????????? ?????? ?????????? «SDU UNIVERSITY»

СОДЕРЖАНИЕ

1. Общие положения

2. Установка и обновление антивирусных средств

3. Порядок проведения антивирусного контроля

1. ????? ?????????

1. Настоящая Инструкция определяет требования к организации антивирусной защиты информационных ресурсов локальной вычислительной сети Учреждения «SDU University» (далее – Университет) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность сотрудников Университета - пользователей персональных компьютеров, подключенных к информационным ресурсам локальной вычислительной сети Университета, специалистов Отдела информационно-технической поддержки (далее – ОИТП).

2. ????????? ? ?????????? ???????????? ???????

2.1. К использованию в Университете допускаются только лицензионные антивирусные средства, рекомендованные отделом информационной

безопасности инженерного центра и централизованно закупленные Университетом у разработчиков (поставщиков) указанных средств.

2.2. Антивирусные программы устанавливаются специалистами ОИТП на все персональные компьютеры и сервера локальной вычислительной сети Университета. На почтовом сервере и (или) специально выделенном сервере устанавливается почтовый антивирусный шлюз, который осуществляет антивирусную обработку почтовых сообщений, проходящих по SMTP протоколу.

2.3. Настройка антивирусных средств должна обеспечивать:

1) При каждой перезагрузке компьютера (для серверов – при перезапуске) автоматический запуск антивирусного монитора;

2) В определенное время дня полную антивирусную проверку (сканирование) локальных дисков, установленных на компьютере;

3) Обновление антивирусных баз в определенное время дня;

4) Лечение зараженных вирусов файлов или удаление при невозможности лечения.

3. ??????? ?????????? ????????????? ????????

3.1. Установка (изменение) системного и прикладного обеспечения компьютеров и локальной вычислительной сети должна осуществляться только в присутствии специалиста ОИТП.

3.2. Устанавливаемое (изменяемое) на компьютер программное обеспечение должно быть проверено на отсутствие компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка.

3.3. Обязательному антивирусному контролю подлежит любая информация (тестовые файлы любых форматов, файлы данных, исполняемые файлы),

получаемая и передаваемая по телекоммуникационным каналам.

Пользователю на своем персональном компьютере запрещено:

- изменять настройки и конфигурацию антивирусных приложений;
- удалять или добавлять какие-либо антивирусные программы;

Пользователь обязан:

1) ежедневно в начале работы при загрузке компьютера убедиться в наличии резидентного антивирусного монитора (справа на панели задач должен быть значок с логотипом программы антивирусной защиты и всплывающим над ним наименованием этой программы), и в случае его отсутствия уведомить об этом сотрудников ОИТП;
2) самостоятельно запускать внеплановую антивирусную проверку локальных дисков своего персонального компьютера при получении уведомления от ОИТП о наличии вируса в локальной вычислительной сети Университета, а также 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.);
3) в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, незамедлительно сообщить об этом в отдел сервисного системно-технического обслуживания.

Сотрудник ОИТП обязан:

1) устанавливать антивирусные программы на персональных компьютерах и серверах и инструктировать пользователей по произведенным настройкам;
2) при установке программных продуктов предварительно производить их проверку на наличие вирусов;

3) непосредственно после установки программных продуктов выполнять внеплановую антивирусную проверку компьютера;

4) контролировать состояние серверов и локальной сети от проникновения вирусов;

5) должен рассылать всем пользователям предупреждение о проникновении в корпоративную сеть вирусов и указания по проведению мер антивирусной защиты;

6) не реже одного раза в день производить мониторинг обновлений антивирусных баз на сайтах поставщиков систем антивирусной защиты;

7) установить на антивирусном шлюзе блокировку на входящую почту пользователей для получения исполняемых файлов (файлов с расширением exe, com, bat);

8) проводить не реже двух раз в день анализ работы антивирусного шлюза;

9) составлять расписания и порядок работы модулей антивирусной программы.