АДМИНИСТРАЦИЯ ГОРОДА СМОЛЕНСКА

Р А С П О Р Я Ж Е Н И Е

от 03.11.2010 № 262-р/адм

Об утверждении Инструкции по
антивирусному контролю в
Администрации города Смоленска

В целях обеспечения защиты информационных ресурсов Администрации города Смоленска от вредоносных вирусных программ и сетевых атак, руководствуясь Концепцией защиты информации в Смоленской области, утвержденной постановлением Администрации Смоленской области от 20.12.2004 № 366, руководствуясь Уставом города Смоленска:

1. Утвердить прилагаемую Инструкцию по антивирусному контролю в Администрации города Смоленска.

2. Руководителям структурных подразделений Администрации города Смоленска ознакомить всех сотрудников с утверждаемой Инструкцией и обеспечить ее исполнение.

3. Комитету по информационным ресурсам и телекоммуникациям Администрации города Смоленска (С.В. Пивоваров) разместить настоящее распоряжение на сайте Администрации города Смоленска.

4. Контроль за исполнением настоящего распоряжения оставляю за собой.

Врип Главы Администрации
города Смоленска К.Г. Лазарев

УТВЕРЖДЕНА
распоряжением Администрации
города Смоленска
от 03.11.2010 № 262-р/адм

ИНСТРУКЦИЯ
по антивирусному контролю в Администрации города Смоленска

1. Антивирусный контроль проводится в целях обеспечения защиты информационных ресурсов Администрации города Смоленска от вредоносного воздействия программ-вирусов и сетевых атак.

2. Настоящая Инструкция устанавливает требования к организации антивирусной защиты и обязательна для исполнения всеми сотрудниками Администрации города Смоленска, осуществляющими обработку информации на персональных компьютерах (ПК).

3. Ответственность за организацию антивирусного контроля возлагается на комитет по информационным ресурсам и телекоммуникациям Администрации города Смоленска (далее – Комитет). Комитет определяет тип, марку и версию применяемых антивирусных средств защиты и параметры их настройки.

4. Установку и настройку антивирусных средств защиты осуществляют сотрудники Комитета, за исключением подразделений, имеющих штатных специалистов по информационным технологиям, которые должны самостоятельно осуществлять указанные мероприятия в соответствии с параметрами настройки, определенными Комитетом.

5. Антивирусные средства защиты являются техническими средствами защиты информации.

6. Не допускается использование компьютеров без установленных и настроенных антивирусных средств защиты, которые включены в Государственный реестр сертифицированных средств защиты информации. К применению допускаются только лицензионные официально поставленные разработчиками или свободно распространяемые ими средства защиты.

7. Пользователям ПК запрещается по своей инициативе останавливать работу антивирусных средств защиты, а также изменять настройки.

8. Комитет обязан раз в месяц анализировать вирусные и сетевые атаки, а также эффективность применения антивирусных средств защиты.

9. Антивирусный контроль должен осуществляться постоянно, в автоматическом режиме.

10. Обязательному антивирусному контролю подлежит любая информация, получаемая и передаваемая по телекоммуникационным каналам, файлы, сохраняемые на внешних съемных носителях (магнитных дисках, CD-дисках, USB-накопителях) или считываемые с них, а также помещаемые в электронный архив или извлекаемые из него.

11. Контроль входящей информации должен проводиться непосредственно после или в момент ее приема. Контроль входящей информации, полученной на внешнем съемном носителе, должен проводиться непосредственно после его подключения к ПК или при копировании информации с него на ПК. Запрещается открывать любые файлы на переносных носителях без проведения предварительного антивирусного контроля всего носителя. Контроль исходящей информации должен проводиться непосредственно перед архивированием и отправкой или записью на съемный носитель.

12. Периодичность и режим обновления сигнатур угроз зависит от наличия и параметров подключения ПК к компьютерной сети Администрации города Смоленска и настроенного источника обновлений:

Подключение к компьютерной сети	Пропускная способность канала, Мб/сек	Режим обновления	Периодичность, не реже, чем
Да	10 и более	Автоматический	1 раз в день
Да	менее 10	Автоматический	1 раз в неделю
Нет	-	Ручной	1 раз в месяц

13. Обновление сигнатур угроз на серверах осуществляется ежедневно, в автоматическом режиме, независимо от параметров их подключения к сети.

14. Автоматический режим обновления означает, что антивирусная программа получает обновление по расписанию без непосредственного участия пользователя. Обновление сигнатур угроз может производиться с сервера администрирования в локальной сети или с сервера обновлений производителя антивирусного программного обеспечения. Выбор конкретных параметров расписания и приоритетных источников обновления осуществляется специалистами Комитета исходя из параметров подключения ПК к компьютерной сети.

15. Ручной режим обновления означает, что обновление производится при непосредственном участии сотрудников подразделения.

16. Ответственность за нерегулярное обновление сигнатур угроз на ПК, не подключенном к локальной сети, лежит на пользователе данного компьютера.

17. Получение сотрудниками подразделения новых сигнатур угроз (обновления) возможно двумя способами:

1) если в подразделении имеется ПК с настроенным автоматическим обновлением, то обновления необходимо получать с него. В этом случае сотрудники Комитета осуществляют первоначальную настройку антивируса на данном ПК (создают папку с названием Updates, куда копируются получаемые антивирусом сигнатуры угроз) и ПК, на которых необходимо производить

обновление. Сотрудники подразделения копируют папку Updates на съемный носитель;

2) если в подразделении отсутствуют ПК с настроенным автоматическим обновлением, то обновления необходимо получать непосредственно у сотрудников Комитета в кабинете № 49 основного здания Администрации города Смоленска. Сотрудники Комитета копируют папку Updates на съемный носитель. Первоначальная настройка ПК также осуществляется сотрудниками Комитета.

18. Порядок обновления в ручном режиме: после получения новых сигнатур угроз на внешнем съемном носителе подключить его к ПК, скопировать папку Updates на том D, правой кнопкой мыши нажать на пиктограмму антивируса на панели задач и выбрать пункт «Обновление», дождаться завершения задачи. В случае если сигнатуры повреждены или обновление завершилось с ошибкой необходимо сообщить об этом в Комитет.

19. Сотрудники Комитета при необходимости осуществляют контроль актуальности антивирусных баз на ПК пользователей.

20. При обнаружении средствами антивирусного контроля вредоносного программного обеспечения пользователь из вариантов, предложенных ему антивирусной программой, должен выбрать тот, который подразумевает устранение угрозы. В первую очередь это: «лечить»; «удалить» (если лечение невозможно); «запретить». В случае выбора вариантов: «пропустить», «разрешить», «отменить» - пользователь несет всю полноту ответственности за последствия, причиненные вторгающимся вредоносным программным кодом.

21. В случае обнаружения не поддающегося лечению/удалению вируса пользователь должен: прекратить любые действия с прикладным программным обеспечением; закрыть прикладные программы; выключить ПК; сообщить о вирусе в Комитет. Специалисты Комитета обязаны: провести диагностику ПК; совместно с владельцем зараженных файлов принять решение об их удалении и удалить без возможности восстановления; по возможности, произвести восстановление данных из архивных или резервных копий.

22. Контроль за выполнением требований настоящей Инструкции в структурных подразделениях Администрации города Смоленска осуществляет Комитет.