Приложение к приказу 126-О от 25.06.2021 г.

ИНСТРУКЦИЯ

по организации антивирусной защиты автоматизированной системы управления образования администрации муниципального образования Северский район

1. Общие положения

Настоящая Инструкция определяет требования к организации защиты автоматизированной системы (далее АС) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителя и сотрудников управления образования, экспортирующих и сопровождающих автоматизированную систему, за их выполнение.

К использованию в АС допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств, рекомендованные к применению лицом, ответственным за защиту информации.

В случае необходимости использования антивирусных средств, не вошедших в перечень рекомендованных, их применение необходимо согласовать с лицом, ответственным за защиту информации.

Установка средств антивирусного контроля на ПЭВМ осуществляется уполномоченным на выполнение данных действий, приказом начальника управления образования сотрудником. Настройка параметров средств антивирусного контроля осуществляется Администратором в соответствии с руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля

Антивирусный контроль всех дисков и файлов АС после загрузки компьютера должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

Периодически, не реже одного раза в месяц, должен проводиться полный антивирусный контроль всех дисков и файлов АС (сканирование).

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация на съемных носителях (магнитных дисках. CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей

информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Установка (изменение) системного и прикладного программного обеспечения осуществляется в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств АС». Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено Администратором на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка жестких дисков ПЭВМ Администратором.

Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале за подписью Администратора, установившего (изменившего) программное обеспечение.

3. Действия сотрудников при подозрении наличия компьютерного вируса

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.) сотрудник подразделения самостоятельно или вместе с Администратором должен провести внеочередной антивирусный контроль ПЭВМ. При необходимости он должен привлечь Администратора для определения факта наличия или отсутствия компьютерного вируса.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

-приостановить работу;

-немедленно поставить в известность о факте обнаружения зараженных вирусом файлов Администратора владельца зараженных файлов;

- Администратор совместно с владельцем зараженных вирусом файлов проводит анализ необходимости дальнейшего их использования;

- провести лечение иди уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь Администратор;

- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл на гибком магнитном диске ответственному за защиту информации для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;

- по факту обнаружения зараженных вирусом файлов составить служебную записку ответственному за защиту информации, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) заражен-

ного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

4. Порядок обновления антивирусных баз

Обновление антивирусных баз должно проводиться регулярно, с периодичностью определенной технологией работы в АС.

После согласования с ответственным за защиту информации, ответственный за установку, модификацию и техническое обслуживание программного обеспечения (администратор) копирует новые антивирусные базы с гибких магнитных дисков (ГМД) или с компакт дисков, проводит внеочередной антивирусный контроль и делает отметку в журнале учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств защищенных ПЭВМ о проделанных действиях.

5. Ответственность

Ответственность за организацию антивирусного контроля в управлении образования в соответствии с требованиями настоящей Инструкции возлагается на начальника управления образования.

Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственного за АС (Администратора) и всех сотрудников управления, являющихся пользователями АС.

Периодический контроль за состоянием антивирусной защиты в АС, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками управления осуществляется ответственным за защиту информации.