Об утверждении Инструкции по антивирусной защите информации, обрабатываемой с применением средств вычислительной техники, в органах по контролю за оборотом наркотических средств и психотропных веществ

Приказ · № 65 · от 19.08.2003 · Госнаркоконтроль · Действует без изменений

ГОСУДАРСТВЕННЫЙ КОМИТЕТ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО КОНТРОЛЮ ЗА ОБОРОТОМ НАРКОТИЧЕСКИХ СРЕДСТВ И ПСИХОТРОПНЫХ ВЕЩЕСТВ
ПРИКАЗ
от 19 августа 2003 г. № 65
Москва Об утверждении Инструкции по антивирусной защите информации, обрабатываемой с применением средств вычислительной техники, в органах по контролю за оборотом наркотических средств и психотропных веществ
С целью обеспечения антивирусной защиты информации, обрабатываемой с применением средств вычислительной техники, в органах по контролю за оборотом наркотических средств и психотропных веществ ПРИКАЗ Ы В А Ю:
1. Утвердить прилагаемую Инструкцию по антивирусной защите информации, обрабатываемой с применением средств вычислительной техники, в органах по контролю за оборотом наркотических средств и психотропных веществ.
2. Приказ довести до сотрудников, федеральных государственных служащих и работников органов по контролю за оборотом наркотических средств и психотропных веществ, обрабатывающих информацию с применением средств вычислительной техники. Председатель В.В.Черкесов
Приложение
к приказу Госнаркоконтроля России
от 19 августа 2003г. № 65
ИНСТРУКЦИЯ
по антивирусной защите информации, обрабатываемой с применением
средств вычислительной техники, в органах по контролю за оборотом
наркотических средств и психотропных веществ
I. ОБЩИЕ ПОЛОЖЕНИЯ
1. Инструкция по антивирусной защите информации, обрабатываемой с применением средств вычислительной техники, в органах по контролю за оборотом наркотических средств и психотропных веществ (далее - Инструкция) разработана с целью организации антивирусной защиты информации, обрабатываемой с применением средств вычислительной техники (далее - СВТ), в подразделениях, территориальных органах и организациях Госнаркоконтроля России (далее - органы госнаркоконтроля).
2. Инструкция разработана в соответствии с требованиями Федерального закона "Об информации, информатизации и защите информации", нормативных правовых актов федеральных органов исполнительной власти и Госнаркоконтроля России.
3. Антивирусная защита информации является составной частью комплекса мероприятий по обеспечению защиты информации в органах госнаркоконтроля.
4. В настоящей Инструкции используются следующие определения:
Компьютерный вирус (далее - вирус) - исполняемый или интерпретируемый программный код, обладающий свойством распространения и самовоспроизведения. В процессе распространения вирусный код может себя модифицировать. Вирусы могут выполнять изменение и/или уничтожение программного обеспечения и/или данных.
Машинные носители информации (МНИ) съёмные и несъёмные жесткие магнитные диски, гибкие

магнитные диски, компакт-диски, магнитные ленты, оптические диски, магнитооптические диски и т.п.
Средство вычислительной техники (СВТ) совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.
Съемные носители информации машинные носители информации, не размещенные постоянно в системном блоке СВТ.
II. ТРЕБОВАНИЯ К СРЕДСТВАМ АНТИВИРУСНОЙ ЗАЩИТЫ
5. Используемые средства антивирусной защиты должны обеспечивать:
- проверку оперативной памяти;
- возможность проверки загрузочной дискеты;
- настройку режимов проверки файлов;
- проверку файловых архивов;
- проверку почтовых файлов;
- ведение файла-отчета;
- вывод диалогового окна с описанием обнаруженного вируса;
- обнаружение вирусов в моменты открытия/закрытия файлов работающими приложениями;
- анализ проявления вирусной активности;
- возможность блокировки СВТ и настройки действий при обнаружении вируса;
- отслеживание изменений на носителях информации СВТ;
- гарантированное функционирование на СВТ, используемых для обработки информации.
III. ОРГАНИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ
6. Организация антивирусной защиты информации, обрабатываемой с применением СВТ, возлагается на начальника органа госнаркоконтроля, в ведении которого находится эта информация.
7. Ответственность за проведение мероприятий в подразделениях органов госнаркоконтроля по обеспечению антивирусной защиты СВТ и получение средств антивирусной защиты, их новых версий и обновлений (далее - средства антивирусной защиты) возлагается на сотрудников, ответственных за обеспечение безопасности информации (далее - сотрудники ОБИ).
8. Ответственность за установку и обновление средств антивирусной защиты, антивирусную защиту информации непосредственно на рабочих местах, оборудованных СВТ, возлагается на пользователя, ответственного за эксплуатацию СВТ (далее - пользователь).
9. Размещение средств антивирусной защиты на серверах автоматизированной информационной системы Госнаркоконтроля России (далее - АИС) обеспечивает ИТУ Госнаркоконтроля России.
Получение средств антивирусной защиты и их обновлений в ИТУ Госнаркоконтроля России информационно-технологическими подразделениями территориальных органов Госнаркоконтроля России осуществляется через FTP-сервис.
10. Получение средств антивирусной защиты сотрудниками ОБИ производится с ресурсов, определяемых информационно-технологическими подразделениями органа госнаркоконтроля. В случаях, когда доступ к указанным ресурсам предоставлен пользователям, получение, установка и обновление средств антивирусной защиты производится ими самостоятельно.
Пользователи, не имеющие доступ к ресурсам, содержащим средства антивирусной защиты, получают их у сотрудника ОБИ.
11. Методическое руководство работами по антивирусной защите в органах госнаркоконтроля, организация консультаций возлагается на ИТУ Госнаркоконтроля России.
IV. ПРОВЕДЕНИЕ ПРОФИЛАКТИЧЕСКИХ МЕРОПРИЯТИЙ ПО
АНТИВИРУСНОЙ ЗАЩИТЕ
12. В целях предупреждения заражения вирусами необходимо:
- установить средство антивирусной защиты на все СВТ, используемые для обработки, хранения и

передачи информации;
- изучить инструкцию на установленное антивирусное средство, используя информацию из справочной системы средства;
- обновлять антивирусные средства не реже одного раза в месяц;
- проводить проверку несъемных МНИ в режиме проверки всех типов файлов не реже 1 раза в месяц.
13. Для обеспечения контроля за состоянием информации в СВТ, обнаружения вирусов в моменты открытия (закрытия) файлов работающими приложениями, а также анализа проявления вирусной активности, необходимо применять антивирусную "программу-сторож" (например, SplDer из антивирусного пакета АО "ДиалогНаука").
14. При невозможности применения антивирусной "программы-сторож", в целях предупреждения заражения вирусами проводить проверку МНИ на наличие вирусов:
14. 1. Жесткие магнитные диски, размещенные постоянно в системном блоке СВТ - один раз в неделю.
14. 2. Съемные перезаписываемые носители информации, зарегистрированные за пользователем - один раз в неделю. Не перезаписываемые носители - один раз при первом использовании.
14. 3. Съемные носители информации других пользователей каждый раз при помещении их в СВТ для считывания или записи на них информации.
15. При организации работ по антивирусной защите в вычислительной сети администратор сети обязан проводить установку средств антивирусной защиты на сервера АИС не реже одного раза в месяц и обеспечивать постоянный мониторинг информационных потоков и ресурсов информации на наличие вирусов.

V. ОБНАРУЖЕНИЕ И УНИЧТОЖЕНИЕ ПРОГРАММНЫХ ВИРУСОВ

16. Компьютерные вирусы в зависимости от типа воздействуют на программное обеспечение СВТ, на операционную среду, на вычислительные ресурсы СВТ, при этом модифицируя загрузочные записи и системные области магнитных дисков, разрушая содержимое оперативной памяти СВТ, изменяя или уничтожая файлы, содержащие исполняемый код и информацию пользователя.
17. Признаками возможного "заражения" СВТ может быть нештатная работа устройств СВТ и программного обеспечения (изменение режимов работы контроллеров монитора, дисководов, клавиатуры, "зависание" операционной системы и пользовательских программ, отображение на экране монитора нерегламентированных сообщений и т. п.) или предупреждающие сообщения антивирусных программ.
18. При появлении признаков возможного "заражения" СВТ пользователь обязан немедленно прекратить работу и проверить СВТ на наличие вирусов в режиме проверки всех типов файлов.
19. В случае обнаружения факта "заражения" информационных ресурсов СВТ вирусом необходимо принять меры по уничтожению вируса, действуя в строгом соответствии с инструкцией на данное антивирусное средство.
При невозможности удаления вируса, необходимо сообщить о факте заражения вирусом сотруднику ОБИ. Сотрудник ОБИ составляет на имя начальника своего подразделения рапорт о факте обнаружения вируса, с приложением протокола (журнала) проверки, создаваемого антивирусной программой, и о немедленном прекращении работ на данном СВТ и принятии мер по антивирусной защите.
20. Начальник органа госнаркоконтроля обязан организовать проверку по факту нарушения требований антивирусной защиты и по результатам ее проведения сообщить в подразделение режима и информационной безопасности о причинах появления программного вируса и принятых мерах.

VI. КОНТРОЛЬ ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

21. Контроль за выполнением требований Инструкции возлагается на подразделения режима и информационной безопасности органов госнаркоконтроля.