Инструкция

организации антивирусной защиты

1 Общие положения

1.1 Настоящие правила определяют требования к организации защиты сегмента государственной информационной системы от разрушающего воздействия компьютерных вирусов и устанавливают ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих информационные системы (далее - ИС), за их выполнение.

1.1 Настоящие правила разработаны на основе:

- методического документа «Меры защиты информации в государственных информационных системах», утвержденного Федеральной службой технического и экспортного контроля России 11 февраля 2014 года.
- Постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2 К использованию в ИС допускаются только сертифицированные лицензионные антивирусные средства, рекомендованные к применению администратором информационной безопасности (далее - АИБ).

1.3 В случае необходимости использования антивирусных средств, не вошедших в перечень рекомендованных, их применение необходимо согласовать с ответственным за информационную безопасность.

2 Установка средств антивирусного контроля на автоматизированное рабочее место (далее - АРМ) и сервера ИС осуществляется уполномоченными сотрудниками. Настройка параметров средств антивирусного контроля осуществляется АИБ в соответствии с руководствами по применению конкретных антивирусных средств. Назначение и область действия

2.1 Настоящие правила предназначены для АИБ ИС.

Настоящие правила распространяются на объект информатизации:

- Государственные информационные системы.

3. Применение средств антивирусного контроля

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

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

3.3. 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).

3.4 В случае установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка жестких дисков ИС лицом, установившим (изменившим) программное обеспечение, под контролем.

4 Действия сотрудников при подозрении наличия компьютерного вируса

4.1. 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 АИБ должен провести внеочередной антивирусный контроль АРМ или серверов ИС. При необходимости он должен привлечь АИБ для определения ими факта наличия или отсутствия компьютерного вируса.

4.2. 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 руководителя подразделения и АИБ, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

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

провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь АИБ);

в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл на гибком магнитном диске ответственному за информационную безопасность для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку (при необходимости для выполнения требований данного пункта привлечь АИБ);

по факту обнаружения зараженных вирусом файлов составить служебную записку АИБ, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

5. Порядок обновления антивирусных баз

5.1. Обновление антивирусных баз должно проводиться регулярно с периодичностью определенной технологией работы в ИС.

5.2. После согласования с АИБ ответственные за установку, модификацию и техническое обслуживание программного обеспечения обновляют антивирусные средства.

6. Ответственность

6.1. Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящие правила возлагается на АИБ и всех сотрудников подразделения, являющихся пользователями ИС.

6.2. Периодический контроль за состоянием антивирусной защиты в ИС, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящие правила сотрудниками подразделений осуществляется АИБ.