МИНИСТЕРСТВО ФИНАНСОВ УДМУРТСКОЙ РЕСПУБЛИКИ

ПРИКАЗ

От 30 августа 2012г № 105

г. Ижевск

Об утверждении Инструкции по организации антивирусной защиты в Министерстве финансов Удмуртской Республики

В целях обеспечения защиты информации, программного обеспечения и средств электронно – вычислительной техники в Министерстве финансов Удмуртской Республики:

1. Утвердить прилагаемую Инструкцию по организации антивирусной защиты в Министерстве финансов Удмуртской Республики.
2. Контроль за исполнением настоящего приказа возложить на начальника управления автоматизации Рязапова Р.И.

Заместитель Председателя Правительства
Удмуртской Республики –
министр финансов Удмуртской Республики В.В.Богатырёв

Приложение
к приказу Министерства финансов
Удмуртской Республики
от «30» августа 2012 года № 105

Инструкция по организации антивирусной защиты в Министерстве финансов Удмуртской Республики

1. Общие положения

1.1. Настоящая Инструкция определяет требования к организации защиты информационных систем Министерства финансов Удмуртской Республики (далее - Министерство) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников структурных подразделений, эксплуатирующих и сопровождающих информационные системы, за их выполнение.

1.2. К использованию в Министерстве допускаются только лицензионные антивирусные средства, используемые на основании лицензионного договора, рекомендованные к применению контролирующими органами в области защиты информации.

1.3. Настройка параметров средств антивирусного контроля осуществляется Администратором безопасности, назначенным приказом Министерства, в соответствии с руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля

2.1. Антивирусный контроль всех дисков и файлов рабочих станций должен проводиться ежедневно в начале работы при загрузке компьютера (для серверов - при перезапуске) в автоматическом режиме.

2.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD - ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в оперативную память компьютера с заведомо «чистой» (не зараженной вирусами) и защищенной от записи системной дискеты, - на любом другом компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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

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

3. Действия при обнаружении вирусов

3.1. 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 Администратором безопасности должен провести внеочередной антивирусный контроль своей рабочей станции, при необходимости - привлечь специалистов Управления автоматизации Министерства для определения ими факта наличия или отсутствия компьютерного вируса.

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

3.2.1. Приостановить работу;

3.2.2. Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и Администратора безопасности, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

3.2.3. Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

3.2.4. Провести «лечение» или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов Управления автоматизации Министерства);

3.2.5. В случае обнаружения нового вируса, не поддающегося «лечению» применяемыми антивирусными средствами, передать зараженный вирусом файл на съемном диске в Управление автоматизации для дальнейшей отправки его в организацию, осуществляющую антивирусную поддержку;

3.2.6. По факту обнаружения зараженных вирусом файлов направить в Управление автоматизации Министерства служебную записку, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и перечень выполненных антивирусных мероприятий.

4. Ответственность

4.1. Ответственность за организацию антивирусного контроля в структурном подразделении, эксплуатирующем подсистему информационной системы, в соответствии с требованиями настоящей Инструкции возлагается на руководителя структурного подразделения.

4.2. Ответственность за проведение мероприятий антивирусного контроля в структурном подразделении и соблюдение требований настоящей Инструкции возлагается на Администратора безопасности и всех сотрудников структурного подразделения, являющихся пользователями информационной системы.

4.3. Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками структурных подразделений Министерства осуществляется Администратором безопасности.