Приложение
к приказу Государственного комитета
Республики Узбекистан по статистике
от «20» февраля 2014 г. № 14

Положение
об организации защиты от вредоносных программ в системе Государственного комитета Республики Узбекистан по статистике

I. Область применения

1. Настоящее Положение определяет порядок организации защиты от вредоносных программ в системе Государственного комитета Республики Узбекистан по статистике.

II. Термины и определения

2. В настоящем документе применены следующие термины и определения:

Единая информационная система (ЕИС) Госкомстата – организационно упорядоченная совокупность информационных ресурсов, информационных систем, программно-аппаратного обеспечения и телекоммуникационных средств органов государственной статистики, обеспечивающая сбор, обработку, хранение и использование статистической информации;

вредоносная программа - программа, реализованная аппаратным, программно-аппаратным или программным способом и предназначенная для выполнения каких-либо несанкционированных или злоумышленных действий;

вирус – программа, которая самопроизвольно размножается путем вставления своих возможно измененных копий в другие программы и модификации их при этом, и которая выполняется при вызове инфицированной программы.

Примечание. Вирус часто является причиной искажений или разрушений и в некоторых случаях может активизироваться при наступлении определенной даты;

антивирусный монитор – часть антивирусного программного обеспечения, предназначенная для непрерывного контроля ситуаций, при которых может произойти заражение вредоносной программой. Антивирусный монитор, как правило, работает постоянно, в режиме реального времени отслеживая потенциально опасные операции;

антивирусный сканер – часть антивирусного программного обеспечения, предназначенная для антивирусной проверки различных объектов;

Hyper Text Transfer Protocol (HTTP) – протокол передачи гипертекста (протокол передачи данных прикладного уровня);

Simple Mail Transfer Protocol (SMTP) – простой протокол передачи почты (протокол передачи электронной почты в сетях TCP/IP);

Post Office Protocol Version 3 (POP3) – протокол почты версии 3 (протокол прикладного уровня, используемый программами электронной почты для извлечения электронного сообщения с удаленного сервера по TCP/IP-соединению);

Internet Message Access Protocol (IMAP) – протокол доступа к Интернет-сообщению (протокол прикладного уровня для доступа к электронной почте).

III. Общие положения

3. В системе Госкомстата должно применяться только официально приобретенное лицензионное антивирусное программное обеспечение.

4. Обновление сигнатурных баз антивирусного программного обеспечения должно осуществляться регулярно и автоматически.

IV. Требования по защите от вредоносных программ с помощью антивирусного программного обеспечения

5. Для защиты ЕИС Госкомстата от вредоносных программ на все рабочие станции и серверы устанавливается антивирусное программное обеспечение:

а) рабочие станции защищаются стандартными однопользовательскими антивирусными сканерами и антивирусными мониторами;

б) защита файловых серверов осуществляется с использованием антивирусных мониторов, способных автоматически проверять все файлы сервера, к которым обращаются по сети передачи данных;

в) для защиты почтовых серверов используется антивирусное программное обеспечение, способное фильтровать трафик HTTP, SMTP, POP3 и IMAP и исключающее попадание зараженных сообщений на рабочие станции пользователей.

6. Установка и поддержка антивирусного программного обеспечения производится:

а) в центральном аппарате Госкомстата – Отделом администрирования и безопасности информационных систем Управления информационной безопасности;

б) в территориальных Управлениях статистики – системными администраторами;

в) в Центре переподготовки кадров и статистических исследований – лицом, ответственным за обслуживание локальной вычислительной сети Центра.

7. Обновление сигнатурных баз поддерживается Отделом администрирования и безопасности информационных систем Управления информационной безопасности и должно производиться автоматически на каждом компьютере, включенном в корпоративную сеть передачи данных Госкомстата, минимум один раз в день,

а на отдельно стоящих компьютерах – минимум один раз в неделю пользователем или, при необходимости, администратором.

8. Антивирусное программное обеспечение, установленное на компьютере, должно быть настроено таким образом, чтобы обеспечивать автоматический антивирусный контроль при каждой перезагрузке компьютера, а также проверку:

а) файлов и разделов при доступе к ним;

б) электронной почты при наличии почтового клиента;

в) всей информации, считываемой веб-браузерами из сети Интернет.

9. Антивирусное программное обеспечение, установленное на рабочих станциях, должно позволять проводить антивирусную проверку по требованию.

10. Антивирусное программное обеспечение, установленное на серверах, должно быть настроено таким образом, чтобы дополнительно обеспечивать:

а) проверку любых файлов и директорий при любом доступе к ним, в том числе по локальной сети;

б) проверку электронной почты на корпоративном почтовом сервере;

в) проверку библиотек SharePoint.

11. Изменение стандартных настроек антивирусного программного обеспечения, установленного на рабочих станциях, допускается только в исключительных случаях по согласованию с системным администратором.

12. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы):

а) получаемая и передаваемая по телекоммуникационным каналам;

б) находящаяся на полученных электронных и оптических носителях информации.

13. Антивирусный контроль файлов производится непосредственно работниками системы Госкомстата, использующими эти файлы. Антивирусный контроль производится перед использованием файлов по их содержимому, а не по типу (расширению).

14. При возникновении подозрения на наличие вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, удаление файлов, частые сообщения о системных ошибках) пользователь ЕИС Госкомстата обязан:

а) остановить все работы на компьютере;

б) немедленно сообщить об инциденте системному администратору.

15. При обнаружении признаков компьютерного вируса системный администратор обязан:

а) отсоединить компьютер от ЕИС Госкомстата;

б) совместно с пользователем заражённых вирусом файлов провести анализ необходимости дальнейшего их использования, запустить процесс очистки заражённых вирусом файлов штатным антивирусным программным обеспечением;

в) при невозможности или неэффективности очистки:

уничтожить заражённые вирусом файлов способом, исключающим их восстановление;

встроенными в антивирусное программное обеспечение механизмами сообщить производителю об имеющейся проблеме;

начать первичные мероприятия по разработке альтернативных методов удаления вируса (в исключительных случаях – с применением специальных программ других производителей или самостоятельно написанных программ и программных сценариев);

при опасности массового заражения и до появления выявленной сигнатуры в обновлениях сигнатурной базы взять на ручной контроль основные узлы распространения информации в корпоративной сети передачи данных Госкомстата;

г) оповестить по локальной сети или каким-либо другим способом о факте обнаружения заражённых вирусом файлов пользователя этих файлов, начальника структурного подразделения и другие структурные подразделения, использующие эти файлы в работе;

д) если эти файлы были получены из органа государственной статистики (отправлены в орган государственной статистики), то оповестить отправителя (получателя) по электронной почте или другим способом о наличии вируса в этих файлах;

е) провести дополнительные мероприятия по выявлению в ЕИС Госкомстата компьютеров с неустановленным или необновляемым антивирусным программным обеспечением.

V. Ответственность за нарушение требований настоящего Положения

16. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с установленным законодательством Республики Узбекистан порядком.