МУНИЦИПАЛЬНОЕ КАЗЁННОЕ УЧРЕЖДЕНИЕ
АНЖЕРО-СУДЖЕНСКОГО ГОРОДСКОГО ОКРУГА
«ФУНКЦИОНАЛЬНО-АНАЛИТИЧЕСКИЙ ЦЕНТР»

ПРИКАЗ

от 23.08.2018г. **№ 70**

Об утверждении инструкции по организации антивирусной защиты в муниципальном казённом учреждении Анжеро-Судженского городского округа «Функционально-аналитический центр»

В соответствии с требованиями Постановления Правительства РФ от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами":

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую инструкцию по организации антивирусной защиты в муниципальном казённом учреждении Анжеро-Судженского городского округа «Функционально-аналитический центр».
2. Главному специалисту отдела информационной и кадровой работы МКУ «ФАЦ» Белоусовой А.С. ознакомить Азанова Д.В., ведущего специалиста МКУ «ФАЦ» с данной инструкцией по организации антивирусной защиты и обеспечить её исполнение.
3. Контроль за исполнением приказа возложить на начальника юридического отдела МКУ «ФАЦ» Модель А.В.

Директор МКУ «ФАЦ» С.А. Вейс

Утверждено
приказом МКУ «ФАЦ»
от 23.08.2018г. № 70

Инструкция по организации антивирусной защиты

в муниципальном казённом учреждении Анжеро-Судженского городского округа «Функционально-аналитический центр»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция входит в комплект эксплуатационной документации по использованию автоматизированного рабочего места (далее - АРМ).

1.2. Инструкция разработана для пользователей АРМ, а также для администратора безопасности.

1.3. Рекомендации имеют общий характер. Конкретные методы выявления компьютерных вирусов (в дальнейшем - вирусов) и методы борьбы с ними отражены в эксплуатационной документации на антивирусные программные (программно-аппаратные) средства.

1.4. Защита от вирусов состоит из нескольких этапов. На первом этапе выполняются регулярные профилактические работы согласно настоящей Инструкции. На втором этапе производится анализ ситуации проявления вируса (вирусов) и причины появления. И на третьем этапе выполняется уничтожение вируса (вирусов) из АРМ.

1.5. Для обеспечения проверки программных средств на наличие вирусов создается и ведется банк характеристик существующих вирусов банк антивирусных
программ. В необходимых случаях для анализа выявленных вирусов могут привлекаться сторонние организации.

1.6. По факту выявления вирусов проводится служебное расследование специалистами подразделения безопасности информации.

1.7. Настоящая инструкция доводится под роспись всех работников структурных отделов подразделений, являющихся пользователями ЛВС.

2. НАИБОЛЕЕ ХАРАКТЕРНЫЕ ВНЕШНИЕ ПРОЯВЛЕНИЯ ВИРУСОВ

2.1. Вирус представляет собой программу, которая разрушает информацию на магнитных носителях или нарушает работу АРМ, а также обладает способностью к размножению, т.е. вирус может самостоятельно внедряться в другие программы, переносить себя на диски и дискеты, передаваться локальной компьютерной сети.

2.2 Можно выделить несколько видов воздействия вирусов на АРМ:

- вирусы разрушительного действия;
- вирусы, замедляющие работу АРМ;
- вирусы рекламного характера;

- вирусы-шутки.

2.3. Самые опасные вирусы - это вирусы разрушительного действия. Наиболее характерные внешние проявления вирусов этого вида:

- осыпание различных символов с экрана;
- появление на экране дисплея световых пятен, черных областей или символов, не запланированных рабочими программами;
- самопроизвольная перезагрузка операционной системы;
- зависание компьютера;
- появление неисправных участков (кластеров) на "винчестере";
- неожиданные действия рабочих программ (не предусмотренные документацией на программы);
- искажения данных в обрабатываемых файлах.

2.4. Вирусы, замедляющие работу АРМ, проявляют себя тем, что работа процессора может замедляется в 30-40 раз.

2.5. Вирусы рекламного характера и вирусы-шутки хотя и не портят информацию в АРМ, однако замедляют работу или навязывают пользователю ненужные диалоги, что также замедляет весь процесс решения задачи.

2.6. Некоторые вирусы проявляют себя внешне тем, что изменяют дату и время создания файла, хотя внутренние изменения могут быть и разрушительными.

2.7. Некоторые внешние неожиданные отклонения в работе АРМ, описанные выше, не обязательно являются следствием наличия вирусов. Так, появление неисправных кластеров на "винчестере" может быть вызвано действительно неисправностью устройства, что определяется анализом ситуации.

3. ПРОФИЛАКТИКА ВИРУСОВ

3.1. Регулярно проводимые профилактические работы по выявлению вирусов могут полностью исключить появление и распространение вирусов в АРМ. Поэтому целесообразно включать эти работы в планы работ подразделений. К основным профилактическим работам и мероприятиям относятся:

- ежедневная автоматическая проверка наличия вирусов при включении АРМ;
- регулярная (не реже одного раза в месяц) комплексная проверка наличия вирусов во всех АРМ, даже при отсутствии внешних проявлений вирусов;
- проверка наличия вирусов в АРМ, вернувшихся с ремонта (в том числе гарантийного) в сторонних организациях;
- изучение информации по сообщениям в компьютерных журналах и газетах о новых вирусах;
- создание резервной копии программного продукта сразу же после приобретения;
- системные дискеты и дискеты с наиболее важными программами защищаются от записи на них информации путем установки переключателя на 3-5 " дискетах в положение только чтения - тем самым вирусы не смогут проникнуть на дискеты;
- тщательная проверка всех поступающих и купленных программ и баз

данных; проверку необходимо выполнять либо на АРМ без "винчестера", либо на отдельно выделенной АРМ, не входящей в локальную сеть;

- ограничение доступа к АРМ посторонних лиц.

3.3. Автоматическая проверка наличия вирусов при включении АРМ осуществляется централизовано под управлением антивирусной программы NOD32. Это включение и другие дополнительные настройки выполняет специалист отдела ИТ.

3.4 Регулярную комплексную проверку наличия вирусов выполняет администратор безопасности.

3.5. При обнаружении вирусов в АРМ, работающей в локальной сети, проверке подлежат все АРМ, включенные в эту сеть.

3.6. Создание резервной копии программного продукта выполняет специалист, ответственный за внедрение этого программного продукта.

3.7. Проверку всех поступающих для эксплуатации программных средств выполняет отдел ИТ.

4. АНАЛИЗ СИТУАЦИЙ

4.1. Если антивирусные программы выдают на экран дисплея сообщения о подозрении на наличие вирусов в АРМ, то прежде всего необходимо убедиться в действительном наличии вирусов. Возможны ситуации, при которых эти сообщения являются следствием неисправности компьютера.

Также появление сообщений антивирусных программ может быть вызвано разрушением программного обеспечения вследствие каких-либо аномальных электрических процессов.

4.2. Анализ ситуации наличия вирусов или неисправности какого-либо устройства АРМ выполняет администратор безопасности. При анализе должны использоваться специальные программы проверки исправности АРМ. В результате анализа делается вывод либо об уничтожении вирусов, либо о необходимости ремонта АРМ.

4.3. В Управлении образования администрации Анжеро-Судженского городского округа использование любых съемных носителей запрещено приказом начальника Управления образования городского округа №373 от «30» апреля 2014г. «О запрете использования съемных носителей».

4.4. В случае действительного наличия вирусов привлекаются специалисты функционально-аналитического центра отдела ИТ для проведения служебного расследования.

5. УНИЧТОЖЕНИЕ ВИРУСОВ

5.1. Уничтожение вирусов выполняется специалистом функционально-аналитического центра отдела ИТ.

5.2. Если вирус поразил какие-либо программы, то уничтожение вируса выполняется путем уничтожения программы на винчестере либо на дискете. После уничтожения зараженной программы необходимо восстановить программу, используя резервную копию программы.

5.3. Если вирус поразил файлы, то вирус уничтожается либо путем стирания этих файлов, либо путем использования специальных лечащих программ. Использование лечащих программ не дает полной гарантии восстановления файла. Поэтому после лечения необходима проверки

восстановления данного файла. Лечащие программы используются лишь в тех случаях, когда отсутствует резервная копия зараженной программы либо файла с данными, либо восстановление уничтоженного файла с помощью резервной копии очень трудоемко.

5.4. В любом случае после уничтожения вирусов и восстановления зараженных программ и файлов с данными необходимо еще раз выполнить проверку наличия вирусов, используя антивирусные программы. Перед повторной проверкой необходимо перезагрузить АРМ через выключение и последующее включение АРМ. Если повторная проверка не выявила вирусов, то можно быть уверенным в отсутствии вирусов.

5.5. Для восстановления зараженной загрузочной записи винчестера необходимо использовать специальную системную дискету, на которой записана загрузочная запись.

6. ПРИМЕНЕНИЕ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ

6.1. Антивирусный контроль всех файлов, к которым обращается пользователь или программа, запущенная пользователем рабочей станции, осуществляется автоматически с помощью резидентного модуля антивирусного ПО, загруженного в оперативную память при старте операционной системы.

6.2. Антивирусный контроль электронной почты на рабочих станциях пользователей осуществляется автоматически с помощью резидентного модуля контроля электронной почты, интегрируемого в резидентный модуль антивирусного ПО.

6.3. Рекомендуется проводить периодический антивирусный контроль всех дисков и файлов рабочих станций с помощью сканера антивирусного ПО. Контроль должен проводиться автоматически не реже, чем одного раза в месяц. Настройка параметров средств антивирусной защиты на проверку в автоматическом режиме проводится специалистами отдела ИТ при установке антивирусного программного обеспечения (ПО). Обязательному антивирусному контролю в автоматическом режиме с помощью антивирусного программного обеспечения подлежит любая информация (текстовые файлы любых форматов, исполняемые файлы, архивы, файлы данных, содержимое оперативной памяти рабочих станций и серверов, системные каталоги рабочих станций и серверов, электронная почта), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях.

6.4. Обновление антивирусных баз проводится автоматически ежедневно через антивирусную программу NOD32.

6.5. Установка (изменение) системного и прикладного программного обеспечения проводится по заявкам пользователей ЛВС после согласования с администратором безопасности.

6.6. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов администратором безопасности. Антивирусная проверка (на серверах и рабочих станциях) должна быть выполнена непосредственно после установки (изменения) программного обеспечения компьютера.