СОГЛАСОВАНО
Начальник сервисного центра
в г.Мурманск ЗАО «Гринатом»
«06» октября 2015 г.

_____ В.Б. Удин

УТВЕРЖДЕНО
Приказом № 68-02 от 06.10.2015 г.
ректор Мурманской академии
экономики и управления
д-р экон. наук, профессор

_____ Н.Н. Щебарова

ИНСТРУКЦИЯ
по организации антивирусной защиты

Мурманск
2015 г.

1. Общие положения

Компьютерный вирус является разновидность компьютерных программ, отличительной особенностью которых является способность к размножению (саморепликации). В дополнение к этому они могут повреждать или полностью уничтожать данные, подконтрольные пользователю, от имени которого была запущена заражённая программа. Особую опасность представляет то обстоятельство, что компьютерные вирусы могут скрытно и постепенно уничтожать, либо мгновенно разрушать хранящуюся в компьютере и магнитных носителях информацию, при этом также могут пострадать аппаратные средства.

Основными путями вирусного вторжения являются неквалифицированное обращение пользователей с компьютерной техникой при использовании ими зараженных дискет и программ, либо целенаправленное спланированное воздействие извне с использованием компьютерных вирусов.

2. Порядок, обеспечивающий безопасную работу на компьютере и с магнитныминосителями.

1. Приобретение средств вычислительной техники (СВТ) и программных продуктов подразделениями осуществляется исключительно по согласованию с ректором, а их установка и техническая поддержка производятся сотрудниками центра информационных технологий МАЭУ. Там же осуществляется проверка, настройка и тестовые испытания СВТ и программных продуктов.

Вновь поступающее программное обеспечение должно быть подвергнуто входному контролю - проверке на отсутствие вирусов и проверке соответствия длины и контрольных сумм, если таковые указаны в сопроводительных документах, полученным длинам и контрольным суммам.

2. Каждый компьютер решением начальника структурного подразделения персонально закрепляется за ответственным за его эксплуатацию подготовленным работником.

3. Допуск сотрудников к самостоятельной работе на компьютерах и с внешними носителями осуществляется только после овладения ими навыками в работе с компьютером, антивирусными пакетами программ.

4. На компьютерах может использоваться программное и аппаратное обеспечение, необходимое только для выполнения служебной деятельности и согласованное с центром информационных технологий.

5. На любом работающем компьютере в обязательном порядке должен быть установлен и активирован пакет антивирусных программ. Ответственность за это несет конкретный, отвечающий за его работоспособность сотрудник, а также техник ЦИТ. Установка средств антивирусного контроля (в том числе настройка параметров средств антивирусного контроля) на автоматизированных рабочих местах (АРМ), серверах локальной вычислительной сети (ЛВС) осуществляется техником ЦИТ в соответствии с руководствами по применению конкретных антивирусных средств. Антивирусные средства устанавливаются при вводе в эксплуатацию автоматизированной системы или при их плановой замене.

6. Периодически, не реже 1 раза в неделю, работник, ответственный за компьютер, проверяет его дисковое пространство с использованием антивирусного пакета программ на возможное наличие компьютерного вируса.

Пользователь (в случае необходимости совместно с техником ЦИТ) обязан проводить антивирусный контроль любой электронной информации (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивируемые/разархивируемые файлы и т.д.), получаемой и передаваемой по телекоммуникационным каналам, а также

информации на съемных носителях (магнитных дисках, оптических носителях, Flash - память и т.п.).

8. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов техника ЦИТ, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно со специалистом по антивирусной защите провести анализ необходимости дальнейшего использования зараженных вирусом файлов;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов по информационным технологиям, по защите информации);

Все факты обнаружения зараженных вирусом файлов техник ЦИТ заносит в «Журнал учета работы АС» (приложение 1), где отображается тип зараженного файла, характер содержащейся в файле информации, название вируса, тип вируса и выполненные антивирусные мероприятия.

3. Ответственность

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на техника ЦИТ МАЭУ.

Пользователь и техник ЦИТ несут ответственность за качество и своевременность выполнения задач и функций, возложенных на них в соответствии с настоящей Инструкцией.

Приложение 1
к Инструкции по организации
антивирусной защиты
Утверждена
Приказом № 68-02 от 06.10.2015 г.

Форма журнала регистрации работ АС

Дата	Наименование работ	ФИО исполнителя работ	ИСПДн	Роспись
1	2	3	4	5
01.06.2014	Обновление антивирусной базы, сканирование дисков		ИСПДн работников ИСПДн контрагентов	
04.07.2014	Антивирусная проверка АС Вирусов не обнаружено		ИСПДн работников ИСПДн контрагентов	
05.09.2014	Обновление антивирусной базы. Антивирусная проверка ИСПДн. Обнаружен вирус «название вирус». Лечение проведено антивирусными средствами. О заражении поставлены в известность техник ЦИТ.		ИСПДн работников ИСПДн контрагентов	