МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
государственное образовательное учреждение высшего профессионального образования «Мурманский государственный гуманитарный университет»
(ГОУВПО МГГУ)

УТВЕРЖДАЮ:
Ректор МГГУ _____ А.М. Сергеев
«13» декабря 2010 г.

ИНСТРУКЦИЯ
по организации антивирусной защиты

РАЗРАБОТАЛ:

Нач.отдела информатизации К.А.Приставка

СОГЛАСОВАНО:

Проректор по инф. технологиям С.В.Архипов

г. Мурманск
2010 г.

1. Общие положения

Компьютерный вирус является разрушающей программной закладкой и характеризуется значительным деструктивным потенциалом для программ, данных и любой информации, хранящейся на компьютерах и магнитных носителях. 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 магнитными носителями.

1. Приобретение средств вычислительной техники (СВТ) и программных продуктов подразделениями осуществляется исключительно по согласованию с проректором по информационным технологиям, а их установка и техническая поддержка производятся сотрудниками отдела технического развития МГГУ. 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 управлением 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 администратор безопасности подразделения. Установка средств антивирусного контроля (в том числе настройка параметров средств антивирусного контроля) на автоматизированных рабочих местах (АРМ), серверах локальной вычислительной сети (ЛВС) осуществляется системным администратором 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.

7. Пользователь (в случае необходимости совместно с администратором безопасности подразделения) обязан проводить антивирусный контроль любой электронной информации (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивируе-

мые/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 специалистов по антивирусной защите, по защите информации (в ИСПДн), 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 администратор безопасности информации 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 администратора безопасности информации.

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

Приложение 1

Форма журнала регистрации работ АС.

Дата	Наименование работ	Ф.И.О. исполнителя работ	ИСПДн _____	Роспись
1	2	3	4	5
01.06.2010	Обновление антивирусной базы, сканирование дисков		ИСПДн работников ИСПДн контрагентов	
01.06.2010	Антивирусная проверка АС Вирусов не обнаружено		ИСПДн работников ИСПДн контрагентов	
02.06.2010	Обновление антивирусной базы. Антивирусная проверка ИСПДн. Обнаружен вирус «название вируса». Лечение проведено антивирусными средствами. О заражении поставлены в известность администраторы безопасности подразделений _____.		ИСПДн работников ИСПДн контрагентов	