УТВЕРЖДАЮ

Ректор _____ Кошкин В.И.

«__» _____ 2012 г.

ПОЛИТИКА АНТИВИРУСНОЙ ЗАЩИТЫ

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 съемных носителей информации 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 при участии уполномоченных лиц по защите информации. Установка и техническая поддержка производятся совместно с подразделением ответственным за защиту информации . Проверка, настройка и тестовые испытания СВТ и программных продуктов осуществляется исключительно при участии уполномоченных лиц по защите персональных данных.

Вновь поступающее программное обеспечение должно быть подвергнуто входному контролю – проверке на отсутствие вирусов и проверке соответствия размеров файлов 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 по работе с компьютером, антивирусными пакетами программ.

4. На компьютерах может использоваться только программное и аппаратное обеспечение, необходимое для выполнения служебной деятельности и согласованное с подразделением и лицами, ответственными за защиту информации в Организации. Запрещается использовать на компьютерах программные и аппаратные средства, не согласованные с требованиями нормативных документов ФСТЭК

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 ИСПДн. Установка средств антивирусного контроля (в том числе настройка параметров средств антивирусного контроля) на автоматизированных рабочих местах (АРМ), серверах локальной вычислительной сети (ЛВС) осуществляется администратором безопасности ИСПДн 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 ИСПДн) 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 файлов, зараженных компьютерными вирусами, пользователь обязан:

- приостановить работу;

- о факте обнаружения зараженных вирусом файлов немедленно поставить в известность специалистов по антивирусной защите, по защите информации (в ИСПДн), владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

- совместно с уполномоченным лицом 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 уполномоченное лицо заносит в «Журнал учета работы антивирусных средств» (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 Политике порядка проведения антивирусного контроля возлагается на администратора безопасности ИСПДн

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