УТВЕРЖДАЮ
Ректор ФГБОУ ВПО «НВГУ»
С. И. Горлов
«30» мая 2013 г.

Инструкция по организации антивирусной защиты

1. Общие положения

1.1. Настоящая инструкция по организации антивирусной защиты разработана на основании: Федерального закона Российской Федерации от 27.07.2006г. №152-ФЗ «О персональных данных»;

- Положения «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного Постановлением Правительства Российской Федерации №781 от 17 ноября 2007г.;
- Приказа №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных», утвержденного ФСТЭК России от 05.02.2010 г.;
- Приказа №140 от «27» мая 2010г. «Об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного Ректором ФГБОУ ВПО «НВГУ»;
- Положения от «30» мая 2013 г. «О разрешительной системе допуска пользователей к обрабатываемой в ИСПДн информации», утвержденного Ректором ФГБОУ ВПО «НВГУ».

1.2. Настоящая Инструкция определяет требования к организации защиты информационной системы персональных данных (ИСПДн) в ФГБОУ ВПО «НВГУ» (далее – НВГУ) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность сотрудников, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

1.3. К использованию в НВГУ допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

1.4. Установка средств антивирусного контроля на компьютерах осуществляется Администратором безопасности ИСПДн. Настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля

2.1. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.

2.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (DVD (CD)-ROM, flash-накопители и т.п.).

2.3. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в оперативную память компьютера.

2.4. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

2.5. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

2.6. Установка (изменение) системного и прикладного программного обеспечения осуществляется на основании заявки начальника отдела. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено Администратором безопасности ИСПДн на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера на автоматизированном рабочем месте (АРМ) Администратором безопасности ИСПДн должна быть выполнена антивирусная проверка.

2.7. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в электронном журнале антивирусного средства (операционной системы).

2.8. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник самостоятельно или вместе с Администратором безопасности ИСПДн должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлечь специалистов для определения ими факта наличия или отсутствия компьютерного вируса.

2.9. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего руководителя и Администратора безопасности

ИСПДн, владельца зараженных файлов, а также других сотрудников, использующих эти файлы в работе;

- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на отдельном съемном носители Администратору безопасности ИСПДн для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;
- по факту обнаружения зараженных вирусом файлов составить служебную записку Администратору безопасности ИСПДн, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

3. Ответственность

3.1. Ответственность за организацию антивирусного контроля в Организации и соблюдение требований настоящей Инструкции возлагается на Администратора безопасности ИСПДн.

3.2. Периодический контроль за состоянием антивирусной защиты в ИСПДн, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками Организации осуществляется Администратором безопасности ИСПДн.