Приложение 2
к Положению об информационной безопасности
при работе на персональных компьютерах в локальной
вычислительной сети ФАУ ДПО ИПКЛХ
от 13 июля 2017 года

Федеральное агентство лесного хозяйства
(Рослесхоз)
Федеральное автономное учреждение
дополнительного профессионального образования
«Институт повышения квалификации работников лесного хозяйства»
(ФАУ ДПО ИПКЛХ)

ИНСТРУКЦИИ ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ В ФАУ ДПО ИПКЛХ

1. Общие положения

1.1. Настоящая Инструкция является неотъемлемой частью Положение об информационной безопасности при работе на персональных компьютерах в локальной вычислительной сети Федерального автономного учреждения дополнительного профессионального образования «Институт повышения квалификации работников лесного хозяйства» (далее – Институт), которая определяет требования к организации защиты информационных систем персональных данных (далее – ИСПДн) Института от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

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

1.3. Установка средств антивирусного контроля на серверах и рабочих станциях ИСПДн осуществляется администратором безопасности.

1.4. Настройка параметров средств антивирусного контроля осуществляется администратором безопасности в соответствии с руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля

2.1. Антивирусный контроль всех дисков и файлов рабочих станций должен проводиться ежедневно в начале работы при загрузке компьютера (для серверов - при перезапуске) в автоматическом режиме.

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 (магнитных дисках, CD – ROM, Flash, SD и т.п.). 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 с заведомо "чистой" (не зараженной вирусами) и защищенной от записи системной дискеты. 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).

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

2.4. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка.

3. Действия при обнаружении вирусов

3.1. 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 подразделения самостоятельно или вместе с ответственным за обеспечение безопасности информации должен провести внеочередной антивирусный контроль своей рабочей станции для определения факта наличия или отсутствия компьютерного вируса.

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

3.2.1. приостановить работу;

3.2.2. немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя подразделения и ответственного за обеспечение информационной безопасности, а также смежные подразделения, использующие эти файлы в работе;

3.2.3. администратор безопасности совместно с владельцем зараженных вирусом файлов должен провести анализ необходимости дальнейшего их использования;

3.2.4. провести лечение или уничтожение зараженных файлов;

3.2.5. в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл в организацию, с которой заключен договор на антивирусную поддержку или разработчику используемого антивирусного программного обеспечения;

3.2.6. по факту обнаружения зараженных вирусом файлов составить служебную записку и передать ее ответственному за информационную безопасность сотруднику, 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.

3.3. Пользователям запрещается:

3.3.1. Отключать средства антивирусной защиты информации во время работы.

3.3.2. Открывать сомнительные эл. письма (необходимо удаление), ссылки, сайты, источники переноса информации.

4. Ответственность

4.1. Ответственность за организацию антивирусного контроля в внутренних организационных структурных подразделений Института, эксплуатирующем компьютерную технику, в соответствии с требованиями настоящей Инструкции возлагается на соответствующего руководителя структурного подразделения.

4.2. Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение безопасности информации и всех сотрудников подразделения, являющихся пользователями компьютерной техники.

4.3. Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками (пользователями ПК) внутренних организационных структурных подразделений Института осуществляется проректором и ответственным за информационную безопасность.