МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное образовательное учреждение
высшего образования
«Алтайский государственный гуманитарно-педагогический университет
имени В.М. Шукшина»
(ФГБОУ ВО «АГГПУ им. В.М. Шукшина»)

УТВЕРЖДАЮ:
Ректор
_____ Л.А. Мокрецова
«11» апреля 2016г.

ИНСТРУКЦИЯ
по антивирусной защите компьютеров ФГБОУ ВО «АГГПУ им. В.М. Шукшина»

1. Общие положения

1.1 Инструкция по организации антивирусной защиты компьютеров и информационных систем (далее - Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Доктриной информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации от 09.09.2000 г. №Пр-1895.

1.2 Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля ФГБОУ ВО «АГГПУ им. В.М. Шукшина» (далее по тексту – образовательного учреждения или ОУ) с целью предотвращения несанкционированных вредоносных воздействий на информационные ресурсы подразделения и возникновения фактов заражения программного обеспечения (далее по тексту - ПО) образовательного учреждения компьютерными вирусами.

1.3 В настоящей Инструкции использованы следующие термины и определения:

Антивирусное ПО - набор программ для обнаружения компьютерных вирусов и других вредоносных программ и лечения инфицированных файлов, а также для предотвращения заражения файлов или операционной системы вредоносным кодом.

Антивирусные базы - файлы, используемые антивирусным ПО при поиске вредоносных программ, периодически обновляемые разработчиком антивирусного ПО.

Антивирусный контроль - проверка информации (файла, сообщения и т.п.) на предмет наличия вредоносных программ.

Вредоносная программа - компьютерная программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информационные ресурсы.

Защищаемый компьютер - электронно-вычислительная машина (персональный компьютер или сервер), используемая для обработки данных.

Пользователь — работник ОУ или другое лицо, использующее в работе средства электронно-вычислительной техники ОУ, назначенный приказом ректора ОУ.

Съемный носитель информации - носитель информации, предназначенный для ее автономного хранения и независимого от места записи использования (съемные винчестеры, флэш- память, CD, DVD, дискеты и др.).

1.4 Требования настоящей Инструкции обязательны для выполнения всеми пользователями, обрабатывающими персональные данные посредством электронно-вычислительной техники ОУ.

1.5 Общее и методическое руководство обеспечением антивирусной защиты в ОУ осуществляется программистом управления информатизации, ответственным за наличие/обновление антивирусного программного обеспечения.

1.6 Пользователь отвечает за обеспечение устойчивой работоспособности и информационной безопасности вверенного ему объекта вычислительной техники и выполнения других видов работ.

1.7 Техническое обслуживание средств вычислительной техники, уборка помещения и т.п. проводятся под контролем пользователя или уполномоченного лица.

2. Установка антивирусного ПО

2.1 Установку антивирусного ПО производит программист, ответственный за наличие/обновление антивирусного программного обеспечения.

2.2 В ОУ могут использовать только лицензионное антивирусное ПО.

2.3 Установка антивирусного ПО производится индивидуально на каждый защищаемый компьютер с обязательным предохранением настроек от изменения паролем.

2.4 Пользователям запрещается отключать средства антивирусной защиты и самостоятельно вносить изменения в настройки антивирусного ПО.

2.5. Антивирусное ПО запускается автоматически при запуске системы.

3. Порядок обновления антивирусных баз

3.1 Актуализация антивирусных баз на защищаемых компьютерах, подключенных к локальной сети ОУ, должна осуществляться ежедневно в автоматическом режиме через специальный сервер обновлений (по рабочим дням).

3.2 Обновление антивирусных баз на защищаемых компьютерах, не подключенных к локальной сети, должно осуществляться с использованием маркированных съемных носителей информации, в обязательном порядке проверяемых антивирусным ПО перед их использованием или принудительным подключением к локальной сети в ОУ.

3.3 Проверка критических областей защищаемого компьютера, заражение которых вредоносными программами может привести к серьезным последствиям, должна проводиться автоматически при каждой его загрузке.

3.4 Актуализация антивирусных баз на защищаемых компьютерах, подключенных к локальной сети, контролируется пользователем самостоятельно ежедневно и в случае нарушения пользователь должен не принимать никаких мер и срочно сообщить администратору по обеспечению защиты информации.

3.5 На корпоративном сервере обновлений аккумулируются базы обновлений для всех версий используемого антивирусного и предоставляются в доступ для компьютеров сети.

4. Требования к проведению антивирусного контроля

4.1 Пользователь осуществляет контроль за целевым использованием автоматизированного рабочего места, а также всех его внешних устройств

4.2 Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, файлы данных, сообщения электронной почты и т.д.), получаемая и передаваемая по телекоммуникационным каналам, а также данные на съемных носителях информации. Контроль входящей и исходящей информации на защищаемых компьютерах должен осуществляться непрерывно посредством постоянно работающего компонента антивирусного ПО («монитора»).

4.3 Все программное обеспечение, устанавливаемое на защищаемые компьютеры, должно предварительно проверяться на наличие вредоносных программ.

4.4 Не реже одного раза в две недели должна проводиться полная проверка всех файлов, хранящихся на жестких дисках защищаемого компьютера.

4.5 Внеочередной антивирусный контроль всех дисков и файлов защищаемого компьютера должен выполняться:

- сразу после установки или изменения ПО;
- после подключения автономного компьютера к локальной сети;
- при возникновении подозрения на наличие вредоносных программ (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

4.6 В сомнительных случаях для определения факта наличия или отсутствия вредоносных программ к проверке необходимо привлечь ответственного за обеспечение /обновление антивирусных программ и/или ответственного за безопасность систем обработки ПДн ОУ.

5. Действия пользователей при обнаружении вредоносных программ

5 . 1 В случае обнаружения при проведении антивирусной проверки вредоносных программ пользователи обязаны:

- приостановить все операции, связанные с обработкой файлов на защищаемом компьютере;
- немедленно поставить в известность о факте обнаружения вредоносных программ руководителя структурного подразделения, владельцев зараженных или поврежденных вредоносными программами файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение зараженных файлов (при необходимости привлечь ответственного за обеспечение /обновление антивирусных программ);
- в случае обнаружения не поддающегося лечению вируса, пользователь обязан удалить инфицированный файл в соответствующую папку антивирусного ПО, и проверить работоспособность компьютера (при необходимости привлечь ответственного за обеспечение /обновление антивирусных программ).

6. Ответственность за выполнение требований Инструкции

6.1 Ответственность за организацию антивирусной защиты информации на компьютерах, эксплуатируемых работниками в структурном подразделении, их ознакомление с настоящей Инструкцией несет начальник структурного подразделения, в котором базируются данные компьютеры и состоит в штате материально-ответственное за них лицо.

6.2 Ответственность за соблюдение требований Инструкции на своих рабочих местах несут пользователи.

6.3 Ответственность за своевременное обновление антивирусных баз и получение новых лицензионных ключей при истечении их срока действия несет лицо, ответственное за обеспечение /обновление антивирусных программ АГАО в ОУ.

11.04.2016 Составил: программист ЦА УИНФ Ларионов С.М.