МИНОБРНАУКИ РОССИИ
ОГУ

ОРСКИЙ ГУМАНИТАРНО-ТЕХНОЛОГИЧЕСКИЙ ИНСТИТУТ (ФИЛИАЛ)
федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Оренбургский государственный университет»
(Орский гуманитарно-технологический институт (филиал) ОГУ)

УТВЕРЖДАЮ
_____ Г.А. Мелекесов
«_____» _____ 2012 г.

ИНСТРУКЦИЯ

_____ № _____

Об организации антивирусной защиты компьютерных информационных систем в Орском гуманитарно-технологическом институте (филиале) ОГУ

1. Общие положения

1.1. Инструкция «Об организации антивирусной защиты компьютерных информационных систем в Орском гуманитарно-технологическом институте (филиале) ОГУ» (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; Концепцией информационной безопасности Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Оренбургский государственный университет»; Регламентом процедур по использованию и обслуживанию программного обеспечения в Орском гуманитарно-технологическом институте (филиале) ОГУ, утвержденным решением Ученого совета от 02.03.2012 г. № 109 – юр.

1.2. Настоящая Инструкция предназначена для определения порядка по вопросам организации антивирусной защиты в Орском гуманитарно-технологическом институте (филиале) ОГУ (далее – Институт) с целью предотвращения несанкционированных вредоносных воздействий на компьютерные информационные ресурсы Института и возникновения фактов заражения программного обеспечения (далее – ПО) Института 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 профилактики – 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.

Защищаемый компьютер – электронно-вычислительная машина (персональный компьютер или сервер), используемая для передачи, хранения и обработки информации.

Вредоносная программа – компьютерная программа, предназначенная для осуществления несанкционированного доступа к информации, хранимой на персональном компьютере или сервере с целью причинения вреда Институту и (или) пользователю электронно-вычислительной машины.

Лицензионное антивирусное программное обеспечение – программа, на использование которой имеется лицензия (разрешение) правообладателя (обладателя исключительных прав).

Компьютерная информационная система (далее – КИС) – информационная система, представляющая собой совокупность сведений, содержащихся на машинных носителях, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких сведений с использованием средств автоматизации на базе электронно-вычислительной техники.

Пользователь – работник Института или другое лицо, использующее в работе средства электронно-вычислительной техники Института.

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

Маркированный съемный носитель информации – съемный носитель, на корпус которого изготовителем и (или) пользователем нанесен уникальный текст, условное обозначение или рисунок, позволяющие идентифицировать данный съемный носитель и отличать его от других подобных носителей.

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

1.5. Общее руководство обеспечением антивирусной защиты КИС в Институте осуществляется отделом информационных систем и прикладного программного обеспечения (далее – ОИСППО) совместно с информационно-коммуникационым центром (далее – ИКЦ).

2. Установка антивирусного ПО

2.1. Установку антивирусного ПО производят по решению ОИСППО либо его сотрудники, либо специалисты, обслуживающие ПО в структурных подразделениях Института.

2.2. В Институте должно использоваться только лицензионное антивирусное ПО, рекомендованное к применению в Институте.

2.3. Установка антивирусного ПО производится на каждый защищаемый компьютер Института с обязательным предохранением настроек этого ПО от несанкционированного изменения со стороны пользователя.

3. Порядок обновления антивирусных баз

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

3.2. Обновление антивирусных баз на защищаемых компьютерах, не подключенных к локальной сети Института, должно осуществляться либо через подключение к специальным серверам обновлений разработчика используемого лицензионного антивирусного ПО, либо с использованием маркированных съемных носителей информации, в обязательном порядке проверяемых перед каждым их использованием антивирусным ПО на одном из защищаемых компьютеров, подключенных к локальной сети Института.

3.3. Обновление антивирусных баз на защищаемых компьютерах, не подключенных к локальной сети Института, должно производиться не реже одного раза в две недели.

4. Требования к проведению антивирусного контроля

4.1. 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»).

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

4.3. Все ПО, устанавливаемое на защищаемые компьютеры, должно предварительно проверяться на наличие вредоносных программ специалистами, обслуживающими ПО в структурных подразделениях Института.

4.4. Проверка критических областей защищаемого компьютера, заражение которых вредоносными программами может привести к серьезным последствиям, должна проводиться в автоматическом режиме не реже одного раза в неделю.

4.5. Внеочередной антивирусный контроль всех дисков и файлов защищаемого компьютера после обновления антивирусных баз должен выполняться специалистом, обслуживающим ПО в данном структурном подразделении:

– сразу после ввода в эксплуатацию нового или ранее уже использовавшегося компьютера, не проходившего антивирусный контроль более одного месяца;

– после подключения автономного компьютера к локальной сети Института;

– при возникновении подозрения на наличие вредоносных программ (нетипичная работа программ, появление ранее не имевших место 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 специалисты ОИСППО могут инициировать и непосредственно участвовать в антивирусной проверке любых защищаемых компьютеров Института.

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 ответственного за использование ПО в структурном подразделении, владельцев зараженных вредоносными программами файлов;

– совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

– провести лечение или уничтожение зараженных файлов (при необходимости привлечь специалистов, обслуживающих ПО в структурном подразделении);

– по решению специалиста, обслуживающего ПО в структурном подразделении, изменить пароль на доступ к используемым КИС.

6. Ответственность за выполнение требований Инструкции

6.1. Ответственность за организацию антивирусного контроля на компьютерах, эксплуатируемых работниками Института, и их ознакомление с Инструкцией несет ответственный за использование ПО в соответствующем структурном подразделении.

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

6.3. Ответственность за своевременное обновление антивирусных баз на серверах обновлений Института при наличии технической возможности несут обслуживающие их системные администраторы. Ответственность за предоставление доступа к серверам обновлений антивирусных баз разработчика лицензионного антивирусного ПО через внешние телекоммуникационные каналы несет системный администратор ИКЦ.

6.4. Ответственность за своевременное обновление антивирусных баз компьютеров, не подключенных к локальной сети Института, и получение для них новых лицензионных ключей при истечении их срока действия несет отдел ОИСППО.

7. Заключительные положения

Настоящая Инструкция вступает в силу со дня введения ее в действие приказом ректора Института.

Начальник отдела информационных
систем и прикладного программного
обеспечения М.В. Сапрыкин

Согласовано:

Проректор по информатизации С.Е. Крылова

Директор информационно-
коммуникационного центра Е.А. Гамов

Начальник юридического отдела В.В. Панкратова