**Областное государственное бюджетное образовательное учреждение дополнительного профессионального образования "Томский областной институт повышения квалификации и переподготовки работников образования"**

**Утверждаю**
Ректор ТОИПКРО
_____ О.М. Замятина
«29» апреля 2016г.

# Инструкция по организации антивирусной защиты

## 1. Общие положения

1.1. Настоящая Инструкция определяет требования к организации защиты автоматизированных систем Областного государственного бюджетного образовательного учреждения дополнительного профессионального образования «Томский областной институт повышения квалификации и переподготовки работников образования» (далее – ТОИПКРО) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих автоматизированные системы (в том числе информационные системы персональных данных), за их выполнение.

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

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

## 2. Применение средств антивирусного контроля

2.1. Ежедневно в начале работы при загрузке компьютера (для серверов локальной вычислительной сети при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов рабочей станции.

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 дисках, USB-флэш-накопителях 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, - на любом другом компьютере. 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. Установка (изменение) системного и прикладного программного обеспечения осуществляется в соответствии с эксплуатационной и технической документацией к ним. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), администратором безопасности должна быть выполнена антивирусная проверка на защищаемых серверах и рабочих станциях.

2.5. 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 администратором безопасности должен провести внеочередной антивирусный контроль своей рабочей станции для определения факта наличия или отсутствия компьютерного вируса.

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

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя своего подразделения, администратора безопасности, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь администратора безопасности);
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл администратору безопасности для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку (при необходимости, для выполнения требований данного пункта привлечь специалистов по защите информации сторонних организаций – лицензиатов ФСТЭК, имеющих разрешение на осуществление деятельности по технической защите конфиденциальной информации);
- по факту обнаружения зараженных вирусом файлов составить служебную записку, 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 подразделениях, эксплуатирующих автоматизированные системы, в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности.

3.2. Ответственность за проведение мероприятий антивирусного контроля в подразделениях и соблюдение требований настоящей Инструкции возлагается на администратора безопасности и всех сотрудников подразделения, являющихся пользователями автоматизированных систем.

3.3. Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками подразделений ТОИПКРО осуществляется администратором безопасности.