

**Инструкция**  
**по организации антивирусной защиты в информационных системах**  
**государственного автономного учреждения Иркутской области**  
**«Институт развития образования Иркутской области»**

**1. Общие положения**

1.1. Настоящая Инструкция определяет требования к организации защиты в информационных системах государственного автономного учреждения Иркутской области «Институт развития образования Иркутской области» (далее – ИС ГАУ ДПО ИРО) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и работников ГАУ ДПО ИРО, эксплуатирующих и сопровождающих ИС ГАУ ДПО ИРО, за выполнение требований настоящей Инструкции.

1.2. Для обеспечения информационной безопасности к использованию в ИС ГАУ ДПО ИРО допускаются только лицензионные и сертифицированные Федеральной службой по техническому и экспортному контролю Российской Федерации и (или) Федеральной службой безопасности Российской Федерации антивирусные средства, закупленные у официальных разработчиков (поставщиков) указанных средств.

1.3. Установка и настройка средств антивирусного контроля, контроль за состоянием антивирусной защиты в ИС ГАУ ДПО ИРО осуществляется администратором информационной безопасности, в соответствии с руководствами по применению конкретных антивирусных средств.

1.4. После установки и настройки средств антивирусного контроля администратором информационной безопасности в обязательном порядке должно быть произведено тестирование системы антивирусной защиты.

**2. Применение средств антивирусного контроля**

2.1. ИС ГАУ ДПО ИРО подлежат обязательному антивирусному контролю, а также любая информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.).

2.2. Антивирусный контроль ИС ГАУ ДПО ИРО должен проводиться ежедневно в автоматическом режиме при начальной загрузке автоматизированного рабочего места (далее – АРМ).

2.3. Настройка средств антивирусной защиты должна реализовывать следующие функции:

1) непрерывный автоматический мониторинг информационного обмена в ИС ГАУ ДПО ИРО с целью выявления программно-математического воздействия (далее – ПМВ);

2) автоматическая проверка на наличие вредоносных программ или последствий ПМВ при импорте в ИС ГАУ ДПО ИРО всех программных модулей (прикладных программ), которые могут содержать вредоносные программы, по их типовым шаблонам и с помощью эвристического анализа;

3) реализация механизма автоматического блокирования обнаруженных вредоносных программ путем их удаления из программных модулей или уничтожения;

4) автоматическая проверка критических областей автоматизированных рабочих мест и серверов, таких как системная память, загрузочные секторы дисков, объекты автозапуска, каталоги операционной системы «system» и «system32» при каждом запуске операционной системы;

5) полная автоматическая проверка носителей информации всех автоматизированных рабочих мест и серверов не реже одного раза в неделю;



6) регулярное обновление антивирусных баз и программных модулей средств антивирусной защиты. В указанных целях администратору информационной безопасности необходимо один раз в неделю осуществлять установку пакетов обновлений вирусных баз, контроль их подключения к антивирусному пакету и осуществлять проверку АРМ на наличие вирусов;

7) автоматическое документирование состояния системы антивирусной защиты ИС.

2.4. Пользователи ИС ГАУ ДПО ИРО при работе со съемными носителями информации (flash-накопители, дискеты 3,5", CD/DVD диски, жесткие диски USB и т.д.) обязаны перед началом работы осуществить их проверку на предмет отсутствия вредоносных программ выполнив следующие действия:

- 1) подключить съемный носитель информации;
- 2) открыть значок Рабочего стола «Мой компьютер»;
- 3) установить курсор мыши на имя выбранного носителя;
- 4) по правой клавише мыши открыть контекстное меню Microsoft Windows и выбрать пункт, запускающий антивирусную проверку электронного носителя информации.

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 должна осуществляться только в присутствии администратора информационной безопасности. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) системного программного обеспечения должна проводиться антивирусная проверка. В ИС ГАУ ДПО ИРО запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

2.7. При возникновении подозрения на наличие в системе компьютерного вируса, (нетипичная работа программ, искажение данных, частое появление сообщений о системных ошибках и т.п.) работником ГАУ ДПО ИРО должен быть проведен внеочередной антивирусный контроль рабочей станции (самостоятельно или вместе с администратором информационной безопасности). Для проведения контроля должны использоваться актуальные версии антивирусных сканеров (сureit, avz и др.), запускаемых без установки в системе

2.8. В случае обнаружения при проведении антивирусной проверки наличия в ИС ГАУ ДПО ИРО компьютерного вируса работники ГАУ ДПО ИРО обязаны немедленно поставить в известность администратора информационной безопасности и прекратить какие-либо действия на персональном компьютере, приостановить работу, а также поставить в известность владельца зараженных файлов.

2.9. В случае обнаружения наличия в ИС ГАУ ДПО ИРО компьютерного вируса необходимо :

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

провести локализацию вируса в системе;

обеспечить удаление вируса из системы;

2.10. В случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, необходимо направить зараженный вирусом файл в организацию, с которой заключен договор на антивирусную поддержку;

2.11. По факту обнаружения вируса должна быть составлена служебная записка администратору информационной безопасности, в которой требуется указать предположительный источник (отправителя, владельца и т.д.) вируса, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

2.12. Пользователю ИС ГАУ ДПО ИРО запрещается использовать на СВТ съемные носители информации без предварительной проверки установленными средствами антивирусной защиты.

2.13. Пользователь ИС ГАУ ДПО ИРО обязан:

1) ежедневно при начальной загрузке АРМ убедиться в наличии резидентного антивирусного монитора и в случае его отсутствия уведомить об этом администратора информационной безопасности;

2) самостоятельно запускать внеплановую антивирусную проверку АРМ при получении уведомления о наличии в системе вируса, а также при возникновении подозрения на наличие вируса.

### 3. Ответственность

3.1. Ответственность за организацию и проведение мероприятий антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на администратора информационной безопасности.

3.2. Ответственность за ежедневный антивирусный контроль в процессе эксплуатации ИС ГАУ ДПО ИРО и своевременное информирование администратора информационной безопасности в случае обнаружения действий вредоносных программ возлагается на работников ГАУ ДПО ИРО

3.3. На администратора информационной безопасности возлагается ответственность за:

1) организацию антивирусного контроля в ИС ГАУ ДПО ИРО в соответствии с требованиями настоящей Инструкции;

2) проведение мероприятий антивирусного контроля в структурном подразделении ГАУ ДПО ИРО и соблюдение требований настоящей Инструкции всеми работниками, являющимися пользователями ИС ГАУ ДПО ИРО;

3) осуществление периодического контроля за состоянием антивирусной защиты в ИС ГАУ ДПО ИРО, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции работниками ГАУ ДПО ИРО;

4) поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля.

3.4. Работники ГАУ ДПО ИРО, нарушившие требования настоящей Инструкции, привлекаются к ответственности в соответствии с действующим законодательством Российской Федерации.