

## Инструкция

по работе при подключении к сетям общего пользования и (или) международного обмена в государственном автономном учреждении дополнительного профессионального образования Иркутской области «Институт развития образования Иркутской области»

### 1. Общие положения

1.1. Настоящая Инструкция по работе при подключении к сетям общего пользования и (или) международного обмена в государственном автономном учреждении дополнительного профессионального образования Иркутской области «Институт развития образования Иркутской области» (далее соответственно – ГАУ ДПО ИРО, Инструкция) предназначена для работников ГАУ ДПО ИРО, выполнение должностных обязанностей которых связано с использованием персональных компьютеров (далее – пользователи), и определяет их полномочия, обязанности и ответственность при использовании информационных ресурсов информационно-вычислительных сетей общего пользования (далее – ИВС ОП), в том числе информационно-телекоммуникационной сети Интернет (далее – сеть Интернет), а также основные требования по обеспечению безопасности информации.

1.2. Доступ к ИВС ОП осуществляется с рабочей станции пользователя (далее – РС). Ответственность за действия на компьютере другого человека несет пользователь РС, с которого совершено такое действие.

1.3. Основными угрозами безопасности информации при использовании ИВС ОП в ГАУ ДПО ИРО являются:

1.3.1. Заражение информационно-вычислительных ресурсов ГАУ ДПО ИРО программными вирусами;

1.3.2. Несанкционированный доступ внешних пользователей к информационно-вычислительным ресурсам ГАУ ДПО ИРО (в т.ч. сетевые атаки);

1.3.3. Внедрение в информационные системы (далее – ИС) ГАУ ДПО ИРО программных закладок;

1.3.4. Загрузка трафика нежелательной корреспонденцией (спамом);

1.3.5. Несанкционированная передача служебной информации ограниченного доступа работником ГАУ ДПО ИРО в сеть Интернет (внутренний нарушитель);

1.3.6. Блокировка межсетевого взаимодействия с ИВС ОП путем нарушения целостности данных о настройках коммуникационного оборудования, обеспечивающего взаимодействие с ИВС ОП;

1.3.7. Нарушение целостности и достоверности открытых и общедоступных информационных ресурсов ГАУ ДПО ИРО, размещаемых в ИВС ОП.

1.4. Основными методами обеспечения безопасности информации при использовании ИВС ОП для предотвращения указанных угроз являются:

1.4.1. Межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов;

1.4.2. Использование сертифицированных средств защиты информации, в том числе антивирусных и криптографических;

1.4.3. Мониторинг вторжений (атак) из ИВС ОП, нарушающих или создающих предпосылки к нарушению установленных требований по защите информации, и анализ защищенности, предполагающий применение специализированных программных средств (сканеров безопасности);

1.4.4. Контроль информации, загружаемой или передаваемой в ИВС ОП;

1.4.5. Запрет обращения к нежелательным ресурсам ИВС ОП;



1.4.6. Шифрование информации при обмене с другими организациями при ее передаче по ИВС ОП, а также использование электронно-цифровой подписи для контроля целостности и подтверждения подлинности отправителя и/или получателя информации.

## 2. Обеспечение доступа к информационно-вычислительным сетям общего пользования

2.1. ГАУ ДПО ИРО обеспечивает доступ пользователей своей ИС к ресурсам ИВС ОП.

2.2. Открытие и контроль доступа регулируется администратором информационной безопасности (далее – администратор ИБ). Подключение работников ГАУ ДПО ИРО к ИВС ОП осуществляется только на основании списка лиц, допущенных к ресурсам ИВС ОП.

2.3. Доступ к ресурсам ИВС ОП предоставляется работниками ГАУ ДПО ИРО только для выполнения ими прямых должностных обязанностей.

2.4. Самостоятельная организация дополнительных точек доступа к ИВС ОП (удаленный доступ, канал по локальной сети, GPRS и пр.) запрещена.

## 3. Основные ограничения при работе в сети Интернет

3.1. Пользователям запрещается:

3.1.1. Загружать, самостоятельно устанавливать прикладное, операционное, сетевое и другие виды программного обеспечения, а также осуществлять обновления, если эта работа не входит в его должностные обязанности;

3.1.2. Нецелевое использование подключения к ИВС ОП;

3.1.3. Осуществлять работу при отключенных средствах защиты информации, установленных на РС;

3.1.4. Допускать к работе с РС посторонних лиц;

3.1.5. Передавать по сети ИВС ОП защищаемую информацию без использования средств шифрования;

3.1.6. Совершать любые попытки деструктивных действий по отношению к нормальной работе внутренней сети ГАУ ДПО ИРО и ИВС ОП (рассылка вирусов, сетевые атаки и т.п.);

3.1.7. Применять имена пользователей и пароли, используемые в ГАУ ДПО ИРО в ИС за пределами ГАУ ДПО ИРО;

3.1.8. Использовать электронную служебную почту ГАУ ДПО ИРО в личных целях;

3.1.9. Использовать для служебной переписки иную электронную почту отличную от служебной электронной почты ГАУ ДПО ИРО;

3.1.10. Посещать игровые, социальные, развлекательные и прочие сайты, не имеющие отношения к деятельности работника ГАУ ДПО ИРО;

3.1.11. Посещать сайтов сомнительной репутации (сайты, содержащие нелегально распространяемое ПО и другие);

3.1.12. Посещать ресурсы трансляции потокового видео и аудио (веб-камеры, трансляция ТВ и музыкальных программ в сети Интернет, создающих большую загрузку сети и мешающих нормальной работе остальных пользователей);

3.1.13. Играть на компьютере автономно и в сети;

3.1.14. Производить какие-либо действия с информацией, зараженной вирусом;

3.1.15. Подключаться к ресурсам ИВС ОП, используя РС ГАУ ДПО ИРО через не служебный канал доступа, сотовый телефон, модем, и др. устройства;

3.1.16. Создавать личные веб-страницы и хостинг (размещение web- или ftp-сервера) на компьютере пользователя;

3.1.17. Нарушать закон об авторском праве: копировать и использовать материалов и программ, защищенных законом об авторском праве;

3.1.18. Совершать действия, противоречащие законодательству, а также настоящей Инструкции.



### 3.2. Пользователь обязан:

3.2.1. Знать и уметь пользоваться антивирусным ПО. При обнаружении вируса он должен сообщить об этом администратору ИБ;

3.2.2. Информировать администратора ИБ о любых нарушениях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети;

3.3. Пользователи несут персональную ответственность за содержание передаваемой, принимаемой и печатаемой информации.

### 3.4. Администратор ИБ обязан:

3.4.1. Производить подключение к сети ИВС ОП только через специализированное устройство (Firewall) для обеспечения защиты информационной сети;

3.4.2. Знать и правильно использовать аппаратно-программные средства защиты информации и обеспечивать сохранность информационных ресурсов с помощью этих средств;

3.4.3. Оказывать методическую и консультационную помощь пользователям по вопросам, входящим в его компетенцию;

3.4.4. Ежемесячно вести учет и анализ использования ресурсов сети ИВС ОП по каждому пользователю;

3.4.5. Принимать меры для предотвращения и устранения нарушений требований настоящей инструкции пользователями и других негативных ситуациях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети.

### 3.5. Администратор ИБ имеет право:

3.5.1. При обнаружении доступа к развлекательным сайтам, запретить доступ к сайту;

3.5.2. При обнаружении использования пользователем программных продуктов, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети, запретить доступ к сети ИВС ОП;

3.5.3. В целях обеспечения безопасности электронной системы ГАУ ДПО ИРО производить выборочные и полные проверки всей электронной системы и отдельных файлов без предварительного уведомления работников.

## 4. Контроль использования ресурсов сети Интернет

4.1. В целях обеспечения информационной безопасности и безопасности внутренней сети ГАУ ДПО ИРО администратор ИБ осуществляет:

4.1.1. Контроль посещения ресурсов сети Интернет работниками ГАУ ДПО ИРО, а также получаемых и передаваемых работниками данных, в том числе и по электронной почте;

4.1.2. Контроль за соблюдением требований настоящей Инструкции;

4.1.3. Организацию и контроль за безопасным использованием ресурсов сети ИВС ОП.

## 5. Действия работников ГАУ ДПО ИРО в нештатных ситуациях

5.1. При утрате (в том числе частично) подключения к сети ИВС ОП лицо, обнаружившее неисправность, сообщает об этом работнику центра программно-технического обеспечения.

5.2. При заражении компьютера вирусами его использование немедленно прекращается работником, обнаружившим заражение. О сложившейся ситуации сообщается администратору ИБ. Компьютер отключается от сети до момента очистки от всех вирусов.