



## 1. Общие положения

1.1. Инструкция предназначена для сотрудников Республиканского Центра СПИД, выполнение должностных обязанностей которых связано с использованием персональных компьютеров (пользователей), и определяет их полномочия, обязанности и ответственность при использовании информационных ресурсов информационно-вычислительных сетей общего пользования (далее – ИВС ОП), в том числе сети Интернет, а также основные требования по обеспечению безопасности информации.

1.2. Руководители структурных подразделений Республиканского Центра СПИД, пользователи и администраторы обязаны знать и выполнять нормативные правовые акты, затрагивающие вопросы информатизации, защиты информации и информационной безопасности в части соблюдения требований и ограничений по использованию информационных ресурсов.

1.3. Администратор информационной безопасности организуют ознакомление пользователей с настоящей Инструкцией.

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

1.5. Основными угрозами безопасности информации при использовании ИВС ОП в Республиканском Центре СПИД являются:

- заражение информационно-вычислительных ресурсов Республиканского Центра СПИД программными вирусами;
- несанкционированный доступ внешних пользователей к информационно-вычислительным ресурсам Республиканского Центра СПИД (в т.ч. сетевые атаки);
- внедрение в автоматизированные информационные системы Республиканского Центра СПИД программных закладок;
- загрузка трафика нежелательной корреспонденцией (спамом);
- несанкционированная передача служебной информации ограниченного доступа сотрудниками Республиканского Центра СПИД в сеть Интернет (внутренний нарушитель);
- блокировка межсетевого взаимодействия с ИВС ОП путем нарушения целостности данных о настройках коммуникационного оборудования, обеспечивающего взаимодействие с ИВС ОП;
- нарушение целостности и достоверности открытых и общедоступных информационных ресурсов Республиканского Центра СПИД, размещаемых в ИВС ОП.

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

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов;
- использование сертифицированных средств защиты информации, в том числе антивирусных и криптографических;



- 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);
- контроль информации, загружаемой или передаваемой в ИВС ОП;
- запрет обращения к нежелательным ресурсам ИВС ОП;
- 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. Доступ к Интернет-ресурсам**

2.1. Республиканский Центр СПИД обеспечивает доступ пользователей сети к ресурсам ИВС ОП;

2.2. Открытие и контроль доступа регулируется администратором информационной безопасности. Подключение сотрудников Республиканского Центра СПИД к ИВС ОП осуществляется только на основании списка лиц, допущенных к ресурсам ИВС ОП.

2.3. Доступ к ресурсам ИВС ОП предоставляется сотрудникам Республиканского Центра СПИД 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:

- загружать, самостоятельно устанавливать прикладное, операционное, сетевое и другие виды программного обеспечения, а также осуществлять обновления, если эта работа не входит в его должностные обязанности;
- запрещается нецелевое использование подключения к ИВС ОП;
- осуществлять работу при отключенных средствах защиты информации, установленных на рабочей станции;
- допускать к работе посторонних лиц;
- передавать по сети ИВС ОП защищаемую информацию без использования средств шифрования;
- совершать любые попытки деструктивных действий по отношению к нормальной работе внутренней сети Республиканского Центра СПИД и ИВС ОП (рассылка вирусов, сетевые-атаки и т.п.);
- применять имена пользователей и пароли, используемые в Республиканском Центре СПИД в информационных системах за пределами Республиканского Центра СПИД;



- использовать электронную служебную почту Республиканского Центра СПИД в личных целях;
- использовать для служебной переписки иную электронную почту отличную от служебной электронной почты Республиканского Центра СПИД;
- посещать игровые, социальные, развлекательные и прочие сайты, не имеющие отношения к деятельности сотрудника Республиканского Центра СПИД;
- посещать сайты сомнительной репутации (сайты, содержащие нелегально распространяемое ПО и другие);
- посещение ресурсов трансляции потокового видео и аудио (вебкамеры, трансляция ТВ и музыкальных программ в Интернете), создающих большую загрузку сети и мешающих нормальной работе остальных пользователей;
- игры на компьютере автономно и в сети;
- производить какие-либо действия с информацией, зараженной вирусом;
- подключаться к ресурсам ИВС ОП, используя рабочую станцию Республиканского Центра СПИД через не служебный канал доступа – сотовый телефон, модем, и др. устройства;
- создание личных веб-страниц и хостинг (размещение web- или ftp-сервера) на компьютере пользователя;
- нарушение закона об авторском праве: копирование и использование материалов и программ, защищенных законом об авторском праве;
- совершать действия, противоречащие законодательству, а также настоящей Инструкции.

### 3.2. Пользователь обязан:

- знать и уметь пользоваться антивирусным программным обеспечением. При обнаружении вируса он должен сообщить об этом администратору;
- информировать администратора о любых нарушениях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети;
- знать и соблюдать установленные правила работы в локальной сети (Приложение №1 к настоящей Инструкции);
- знать и соблюдать установленные правила работы с электронной почтой (Приложение №2 к настоящей Инструкции);
- знать и соблюдать установленные правила работы в сети Интернет (Приложение №3 к настоящей Инструкции).

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

3.4. Администратор информационной безопасности обязан:



- производить подключение к сети ИВС ОП только через специализированное устройство (Firewall) для обеспечения защиты информационной сети;

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

- оказывать методическую и консультационную помощь пользователям по вопросам, входящим в его компетенцию;

- ежемесячно вести учет и анализ использования ресурсов сети ИВС ОП по каждому пользователю;

- 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 имеет право:

- при обнаружении доступа к развлекательным сайтам, запретить доступ к сайту;

- 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;

- в целях обеспечения безопасности электронной системы Республиканского Центра СПИД 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 Республиканского Центра СПИД администратор информационной безопасности осуществляет:

- контроль посещения ресурсов сети Интернет сотрудниками Республиканского Центра СПИД, а также получаемых и передаваемых сотрудниками данных, в том числе и по электронной почте;

- контроль за соблюдением настоящей Инструкции;

- организацию и контроль за безопасным использованием ресурсов сети ИВС ОП.

## 5. Действия в нештатных ситуациях

5.1. При утрате (в том числе частично) подключения к сети ИВС ОП лицо, обнаружившее неисправность, сообщает об этом ответственному сотруднику за организацию подключения к сети Интернет;

5.2. При заражении компьютера вирусами его использование немедленно прекращается сотрудником, обнаружившим заражение. О

сложившейся ситуации сообщается администратору информационной безопасности. Компьютер отключается от сети до момента очистки от всех вирусов.

Разработал  
Администратор информационной безопасности \_\_\_\_\_ /Сандаков З.Н.



«\_\_\_» \_\_\_\_\_ 20\_\_ г.



Приложение №1  
к Инструкции о порядке  
работы при подключении к  
сетям общего пользования  
и (или) международного  
обмена в Республиканском  
Центре СПИД

### Правила по работе в локальной сети

1. Пользователи сети обязаны:

- при доступе к внешним ресурсам сети, соблюдать правила, установленные администратором информационной безопасности (далее – администратор ИБ) для используемых ресурсов;
- немедленно сообщать администратору ИБ об обнаруженных проблемах в использовании предоставленных ресурсов. Администратор ИБ, при необходимости, с помощью других специалистов, должны провести расследование указанных фактов и принять соответствующие меры;
- не разглашать известную им конфиденциальную информацию (имена пользователей, пароли), необходимую для безопасной работы в сети;
- обеспечивать беспрепятственный доступ администратора ИБ к сетевому оборудованию и компьютерам пользователей, для организации профилактических и ремонтных работ;
- выполнять предписания администраторов ИБ, направленные на обеспечение безопасности сети;
- в случае обнаружения неисправности (например, сильный посторонний шум или запах, необычное поведение затрудняющее работу) компьютерного оборудования или программного обеспечения, пользователь должен немедленно обратиться к администратору ИБ;
- удалять с сетевых ресурсов устаревшие или не используемые файлы, владельцем или создателем которых он является;

2. Пользователи сети имеют право:

- использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках. Администратор ИБ вправе ограничивать доступ к некоторым сетевым ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на повышение эффективности использования сетевых ресурсов;
- обращаться к администратору ИБ по вопросам, связанным с распределением ресурсов компьютера. Какие-либо действия пользователя, ведущие к изменению объема используемых им ресурсов, или влияющие на загруженность или безопасность системы, должны санкционироваться администратором ИБ;



- обращаться за помощью к администратору ИБ при решении задач использования ресурсов сети;
- вносить предложения по улучшению работы с ресурсом.

### 3. Пользователям сети запрещено:

- разрешать посторонним лицам пользоваться вверенным им компьютером;
- использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей, без согласования с администратором ИБ;
- самостоятельно устанавливать или удалять установленные администратором сетевые программы на компьютерах, подключенных к сети, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов;
- повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю;
- вскрывать компьютеры, сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование без согласования с администратором ИБ, изменять настройки BIOS, а также производить загрузку рабочих станций с дискет;
- самовольно подключать компьютер к сети, а также изменять IP-адрес компьютера, выданный администратором. Передача данных в сеть с использованием других IP адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других компьютерах;
- работать с каналоемкими ресурсами (видео, аудио, радио, чаты, файлообменные сети, torrent и др.) без согласования с администратором. При сильной перегрузке канала вследствие использования каналоемких ресурсов доступ пользователя вызвавшего перегрузку, может быть прекращен;
- получать и передавать в сеть информацию, противоречащую действующему законодательству РФ и нормам морали общества, представляющую коммерческую или государственную тайну;
- обхождение учетной системы безопасности, системы статистики, ее повреждение или дезинформация;
- использовать иные формы доступа к сети, за исключением разрешенных администратором ИБ;
- осуществлять попытки несанкционированного доступа к ресурсам сети, проводить или участвовать в сетевых атаках и сетевом взломе;
- использовать сеть для массового распространения рекламы (спам), коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз и т.п.



Приложение №2  
к Инструкции о порядке  
работы при подключении к  
сетям общего пользования  
и (или) международного  
обмена в Республиканском  
Центре СПИД

### Правила работы с электронной почтой

1. Электронная почта предоставляется сотрудникам Республиканского Центра СПИД только для выполнения своих служебных обязанностей. Использование ее для пересылки файлов в личных целях запрещено. Создание или изменение параметров почтового ящика проводится администратором информационной безопасности на основании служебной записки.
2. На рабочем месте допускается использовать только ящики электронной почты, предоставленные Республиканским Центром СПИД. Прямой доступ к другим почтовым системам может быть заблокирован. Для получения писем с других систем допускается использовать переадресацию, которая может быть настроена с помощью администратора.
3. Все электронные письма, создаваемые и хранимые на компьютерах Республиканского Центра СПИД, являются собственностью Республиканского Центра СПИД и не считаются персональными.
4. Республиканский Центр СПИД оставляет за собой право получить доступ к электронной почте сотрудников, если на то будут веские причины.
5. Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.
6. Пользователи не должны позволять кому-либо посылать письма от чужого имени.
7. В качестве клиентов электронной почты могут использоваться только утвержденные почтовые программы.
8. Нельзя осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).
9. Размер вложений у отправляемых писем не должен превышать 20Мб;
10. При работе с электронной почтой сотрудникам Республиканского Центра СПИД запрещается:
  - использовать адрес электронной почты для оформления подписок;
  - публиковать свой электронный адрес либо адреса других сотрудников Республиканского Центра СПИД на общедоступных Интернет-ресурсах

(форумы, конференции и т.п.) за исключением случаев служебной необходимости;

- рассылать через электронную почту материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также ссылки на вышеуказанную информацию;
- распространять защищаемые авторскими правами материалы, затрагивающие какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;
- распространять информацию, содержание и направленность которой запрещены международным и российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.;
- распространять информацию ограниченного доступа, предназначенную для служебного использования;
- предоставлять кому бы то ни было пароль доступа к своему почтовому ящику.



Приложение №3  
к Инструкции о порядке  
работы при подключении к  
сетям общего пользования  
и (или) международного  
обмена в Республиканском  
Центре СПИД

### **Правила по работе в сети Интернет**

1. Пользователи используют программы для поиска информации в сети Интернет только в случае, если это необходимо для выполнения своих должностных обязанностей.
2. По использованию ресурсов Интернет необходимо ведение статистики.
3. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, протоколируются и могут использоваться для принятия решения о применении к нему санкций.
4. Сотрудникам Республиканского Центра СПИД, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим или нарушает действующее законодательство РФ.
5. Все программы, используемые для доступа к сети Интернет, должны быть утверждены администратором информационной безопасности и на них должны быть настроены необходимые уровни безопасности.
6. Запрещено получать и передавать через сеть информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую тайну, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения.
7. Запрещено обращаться к ресурсам сети Интернет несвязанных непосредственно с выполнением своих должностных обязанностей в рабочее время, а также к ресурсам с сомнительным содержанием.
8. Запрещается скачивать и запускать с любых ресурсов любые неизвестные исполняемые файлы без согласования с администратором информационной безопасности.
9. Запрещено использовать иные формы доступа к сети Интернет, за исключением разрешенных администратором ИБ.
10. Ответственность за все действия в сети Интернет, произведенные с рабочей станции, под именем и с паролем пользователя, им самим или другими физическими, или юридическими лицами и организациями, полностью лежит на самом пользователе.