

Положение
о порядке пользования сети Интернет в Воронежском институте повышения
квалификации сотрудников ГПС МЧС России

1. Основные понятия

1.1. Интернет (сеть Интернет, Internet) - глобальная телекоммуникационная сеть информационных и вычислительных ресурсов с коллективным доступом на основе использования единой стандартной схемы адресации. Интернет состоит из множества взаимосвязанных компьютерных сетей и обеспечивает удаленный доступ к компьютерам, электронной почте, доскам объявлений, базам данных и дискуссионным группам.

1.2. Локальная вычислительная сеть Воронежского института повышения квалификации сотрудников ГПС МЧС России (далее ЛВС) – это система, предназначенная для объединения вычислительной техники в единую сеть передачи данных и организацию коллективного управляемого доступа в сеть Интернет. Подразделяется на беспроводной и проводной сегменты.

1.3. Проводной сегмент ЛВС - структурированная кабельная система, состоящая из активного и пассивного сетевого оборудования и набора коммуникационных элементов. Является основой ЛВС.

1.4. Беспроводной сегмент ЛВС - сеть передачи данных без использования кабельной проводки. Построена на основе проводного сегмента ЛВС с использованием технологии Wi-Fi.

1.5. Сервис сети Интернет - совокупность аппаратных и программных средств, обеспечивающих выполнение функций, направленных на обеспечение информационного взаимодействия пользователей между собой и с информационными ресурсами сети Интернет.

1.6. Служба сети Интернет - специальное (служебное) программное обеспечение, позволяющее организовать доступ пользователей к сети Интернет и определяющее порядок их работы с различными сервисами сети.

1.7. Канал передачи - комплекс технических средств и среды распространения, обеспечивающий передачу сигнала между сетевыми станциями, сетевыми узлами или оконечными устройствами.

1.8. Линия передачи - физическая соединительная линия, объединяющая сетевую станцию и сетевой узел или две сетевые станции между собой для обеспечения процесса приема-передачи информации.

1.9. Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

1.10. Информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

1.11. Сайт в сети Интернет - совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети Интернет.

1.12. Сетевая станция (автоматизированное рабочее место (далее - АРМ) - комплекс технических и программных средств, подключенных к сети, предназначенный для автоматизации профессионального труда специалиста и обеспечивающий решение сетевых задач, анализ, обработку и хранение различного вида информации.

1.13. Пользователь - любое должностное лицо, использующее ЛВС как самостоятельно, так и через посредника, для получения информации или решения различных информационных задач.

1.14. Вредоносная программа - самостоятельная компьютерная программа или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях.

1.15. Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

1.16. Информация - сведения (сообщения, данные) независимо от формы их представления.

1.17. Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

2. Общие положения

2.1. Основой разработки Положения о порядке пользования сети Интернет (далее - Положение) в Воронежском институте повышения квалификации сотрудников ГПС МЧС России (далее - институт) являются:

- Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»;
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;

- Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

- Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии»;

- Постановление Правительства РФ от 24 ноября 2009 г. № 953 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти»;

- Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2.2. Положение определяет общий порядок и единые требования подключения АРМ пользователей к сервисам сети Интернет и предоставления им доступа к информационным ресурсам.

2.3. Доступ пользователей МЧС России к ресурсам и сервисам сети Интернет осуществляется в целях получения необходимой информации для выполнения служебных задач.

2.4. Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. Отделение информационного обеспечения населения и технологий информационной поддержки РС ЧС и пожарной безопасности отдела учебной и научной работы института оставляет за собой право ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и Российским Законодательством.

2.5. При работе с ресурсами сети Интернет запрещается:

- разглашение служебной и иной информации ограниченного доступа, ставшей известной сотруднику по служебной необходимости либо иным путем;

- распространение информации, 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 расовой, национальной и религиозной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.;

- публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения или ограничения функциональности любого компьютерного (телекоммуникационного) оборудования, 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 размещения ссылок на вышеуказанную информацию;

- загрузка и запуск исполняемых либо иных файлов без предварительной проверки на наличие вирусов установленным антивирусным пакетом;

- использование программных и аппаратных средств, позволяющих получить доступ к ресурсу, запрещенному к использованию политикой института

2.6. Подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информацию, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к сети Интернет не допускается.

3. Подключение АРМ пользователей института к сети Интернет

3.1. Работа по подключению АРМ пользователей к сети Интернет выполняется отделом учебной работы института, уполномоченным осуществлять программно-техническое сопровождение и контроль за техническим состоянием программно-технических средств и систем пользователей, на основании письменных заявок на предоставление доступа к ЛВС, информационным ресурсам и сервисам сети Интернет от руководителей структурных подразделений института на имя начальника отдела учебной работы института, согласованных с группой по защите государственной тайны института.

3.2. Подключение АРМ пользователей института осуществляется к проводному или беспроводному сегменту ЛВС по решению начальника отдела учебной работы института.

3.3. К ЛВС могут быть подключены только АРМ, соответствующие минимальным аппаратным и программным требованиям, достаточным для функционирования современных антивирусных программ, приобретенных в установленном порядке института, а также находящиеся на материальном учете института. Подключение иных персональных компьютеров и других устройств запрещено.

3.4. Подключение АРМ к ЛВС осуществляется согласно форме заявки на подключение к ЛВС (приложение №1).

3.5. Все виды работ по изменению конфигурации ЛВС выполняются сотрудниками отдела учебной работы с использованием оборудования и материалов, находящихся на материальном учете института. В случае выполнения работ подрядной организацией, сотрудники отдела учебной работы осуществляют контроль производимых действий.

4. Пользование ресурсами и сервисами сети Интернет должностными лицами института

4.1. Возможность получить доступ к ресурсу не является гарантией того, что запрошенный ресурс является разрешенным политикой института.

5. Ограничения по использованию ресурсов и сервисов сети Интернет и ответственность должностных лиц за неправомерные действия

5.1. Каждое АРМ, подключенное к ресурсам и сервисам сети Интернет, закрепляется за ответственным должностным лицом института. Работа иных должностных лиц на АРМ, подключенном к ресурсам и сервисам сети Интернет, а также проведение регламентных работ может осуществляться только с разрешения ответственного должностного лица, за которым закреплено АРМ.

5.2. За разглашение (передачу) посторонним лицам сведений о режимах контроля и настройках системы обеспечения безопасности информации ответственность несет должностное лицо, непосредственно отвечающее за использование и эксплуатацию данного АРМ.

5.3. Использование служебного времени, выделенного пользователю для работы в сети Интернет, не по назначению, а также загрузка трафика сети решением задач, не связанных с выполнением своих должностных и функциональных обязанностей, является нарушением требований настоящей Инструкции.

5.4. Запрещается использовать ресурсы и сервисы сети Интернет:

- с нарушениями законодательства Российской Федерации;
- в интересах, не связанных со служебной деятельностью;
- для несанкционированного доступа к АРМ, информационно-вычислительным и сетевым ресурсам, принадлежащим другим пользователям или сетям.

5.5. Использование программ для удаленного доступа к АРМ без согласования с отделом учебной работы строго запрещено. Ответственное должностное лицо, за которым закреплено АРМ, несет персональную ответственность.

6. Основные положения и требования по обеспечению безопасности информации при работе пользователей с ресурсами и сервисами сети Интернет

6.1. Обеспечение безопасности информации при работе пользователей сети Интернет с ресурсами и сервисами сети Интернет обеспечивается комплексом организационных, технических и программных мероприятий.

6.2. Достаточность комплекса организационных и программно-технических мероприятий определяется по текущим результатам эксплуатации сети Интернет и периодическим контролем выполнения требований по защите информации.

6.3. Непосредственное выполнение требований по обеспечению безопасности информации возлагается на пользователей сети Интернет.

6.4. Пользователи сети Интернет обязаны соблюдать требования и общий порядок использования ресурсов и сервисов сети Интернет и выполнять требования по обеспечению безопасности информации, установленные настоящей Инструкцией.

6.5. Возможными и наиболее вероятными путями нарушения целостности программной среды, угрозами ее разрушения и модификации и средствами осуществления несанкционированного доступа к информации, циркулирующей в сети Интернет, являются компьютерные вирусы, программные закладки,

разглашение пользователем сети Интернет конфигурации и параметров настройки сетевых АРМ, несанкционированное использование различных программ интерактивного обмена информацией.

6.6. Доступ пользователей сети Интернет к устройствам считывания информации со съемных носителей информации может быть ограничен организационными или программно-техническими мерами по требованиям обеспечения безопасности информации сети Интернет на основании решения начальника института.

6.7. Перед началом сеанса работы в сети Интернет рекомендуется проводить проверку носителей информации и элементов памяти компьютера на наличие вирусов.

6.8. При обнаружении нештатных (неизвестных) режимов функционирования программных средств, возникновения ошибочных команд, а также команд, вызванных несанкционированными действиями обслуживающего персонала или иных лиц, либо появлением ложной информации, должностное лицо, ответственное за использование АРМ, должно немедленно отключиться от ресурсов и сервисов сети Интернет. О выявленных фактах нарушения функционирования сегмента сети ответственное должностное лицо обязано незамедлительно сообщить в отдел учебной работы.

6.9. Оставлять без контроля АРМ пользователей сети Интернет запрещается. По окончании рабочего дня АРМ в обязательном порядке обесточивается ответственным должностным лицом, за которым оно закреплено.

Начальник отдела учебной работы
полковник внутренней службы



Д.Л. Турбин

Форма заявки на предоставление доступа к ЛВС, информационным
ресурсам и сервисам сети Интернет

Начальнику отдела учебной работы
специальное звание
ФИО

Рапорт

Прошу Вас дать рассмотреть техническую возможность подключения к ЛВС,
информационным ресурсам и сервисам сети Интернет:

Тип АРМа (ПК, ноутбук, планшет, смартфон)	Инвентарный номер	Номер кабинета	Должность, ФИО ответственного за АРМ сотрудника

Начальник структурного подразделения
специальное звание

ФИО

СОГЛАСОВАНО:
Начальник группы
по защите государственной тайны
специальное звание

ФИО