МЧС РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ «НОГИНСКИЙ СПАСАТЕЛЬНЫЙ ЦЕНТР МИНИСТЕРСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ»

ПРИКАЗ

19.03.2020 г. Ногинск № 151

Об утверждении Инструкции о порядке организации и функционирования сегмента сети Интернет в ФГКУ «Ногинский СЦ МЧС России»

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», приказом МЧС России от 01.07.2008 № 359 «Об утверждении Инструкции о порядке организации и функционирования сегмента сети Интернет МЧС России» и приказом Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» п р и к а з ы в а ю:

1. Утвердить инструкцию о порядке организации и функционирования сегмента сети Интернет в ФГКУ «Ногинский СЦ МЧС России» (далее – Инструкция) (приложение № 1).

2. Начальникам структурных подразделений ФГКУ «Ногинский СЦ МЧС России» (далее - центр) организовать работу в соответствии с Инструкцией.

3. Приказ довести до личного состава центра в части, его касающейся.

4. Контроль исполнения настоящего приказа возложить на начальника штаба – заместителя начальника центра.

Начальник центра
полковник Е.В. Гаврилюк

Приложение №1
к приказу начальника Ногинского СЦ
от «19» 03 2020 г. № 151

ИНСТРУКЦИЯ
О ПОРЯДКЕ ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЯ СЕГМЕНТА СЕТИ ИНТЕРНЕТ В ФГКУ «НОГИНСКИЙ СЦ МЧС РОССИИ»

1. ОСНОВНЫЕ ТЕРМИНЫ

1.1. Сегмент сети Интернет организаций МЧС России – часть сегмента сети Интернет МЧС России, построенный по административному и территориальному признакам и объединяющий совокупность каналов передачи и программно-технических средств и систем, предназначенных для работы в сети Интернет, организаций МЧС России.

1.2. Сервис сети Интернет – программное средство обеспечения информационного взаимодействия пользователей между собой и с информационными ресурсами сети Интернет.

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

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

1.5. Главный узел сегмента сети Интернет МЧС России – комплекс программно-технических средств, предназначенный для организации и обеспечения доступа пользователей к информационным ресурсам и сервисам сети Интернет. Главный узел выполняет функции координирующего органа в функционировании сегмента сети Интернет МЧС России.

1.6. Узел сегмента сети Интернет МЧС России – комплекс программно-технических средств, предназначенный для организации доступа к информационным ресурсам и сервисам сети Интернет, представляющий совокупность сетевых станций и каналов передачи.

1.7. Уязвимость – некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

1.8. Автоматизированное рабочее место (далее – АРМ) – рабочее место, оснащенное персональным компьютером, программным обеспечением и совокупностью информационных ресурсов индивидуального или коллективного пользования, которые позволяют вести обработку данных с целью получения информации при выполнении профессиональных функций.

1.9. Операционная система (далее – ОС) – комплекс программ, обеспечивающих взаимодействие всех аппаратных и программных частей компьютера между собой и взаимодействие пользователя и компьютера.

1.10. Средства защиты информации (далее – СЗИ) – совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

1.11. Персональные данные (далее – ПД) – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

1.12. Несанкционированный доступ (далее – НСД) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

1.13. IP-адрес – уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP.

1.14. Сеть Интернет (далее – сеть) – глобальная сеть построенная на основе стека протоколов TCP/IP

1.15. Программное обеспечение (далее – ПО) – совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

1.16. Бесплатное программное обеспечение – программное обеспечение, лицензионное соглашение которого не требует каких-либо выплат правообладателю

1.17. Коммерческое программное обеспечение – программное обеспечение, созданное с целью получения, прибыли от его использования другими, например, путём продажи экземпляров.

1.18. Свободное программное обеспечение – программное обеспечение, пользователи которого имеют права на его неограниченную установку, запуск, свободное использование, изучение, распространение и изменение (совершенствование), а также распространение копий и результатов изменения.

1.19. Вредоносное программное обеспечение – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

1.20. Пользователь – должностное лицо, использующее ресурсы Интернет для выполнения своих должностных обязанностей.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Инструкция об использовании сегмента сети Интернет в Ногинском спасательном центре (далее – Инструкция) устанавливает порядок подключения и использования сети должностными лицами Ногинского спасательного центра (далее – Центра).

2.2. Действие Инструкции распространяется на всех должностных лиц Центра.

2.3. Доступ к сети предоставляется ограниченному кругу должностных лиц Центра в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.

2.4. Для доступа должностных лиц к сети допускается применение только лицензионного, бесплатного или свободного ПО.

2.5. Операции по предоставлению доступа должностных лиц к сети и контролю его использования выполняются непосредственно (при участии) администратором безопасности.

2.6. АРМ, используемые для обработки информации ограниченного распространения , не могут быть подключены к сети.

2.7. АРМ, работающие в ведомственной цифровой сети передачи данных, не могут быть одновременно подключены к сети.

2.8. Центр оставляет за собой право блокировать или ограничивать доступ пользователей к Интернет-ресурсам.

2.9. При подозрении должностного лица в нецелевом использовании сети инициализируется служебная проверка, проводимая комиссией, в состав которой входит представитель отдела связи и ответственный за информационную безопасность в подразделении.

2.10. Перечни должностных лиц, имеющих право доступа к ресурсам сети интернет, определяются руководителем структурного подразделения и согласовываются с начальником связи Центра.

3. ПОРЯДОК ДОСТУПА

3.1. Доступ должностных лиц к сети может быть инициирован начальником структурного подразделения в случаях:

3.1.1. Организации АРМ для нового должностного лица.

3.1.2. Выполнения должностным лицом обязанностей, для которых требуется доступ к внешним ресурсам.

3.2. Процесс предоставления доступа должностного лица к сети состоит из следующих этапов:

3.2.1. Подготовка АРМ для работы в сети администратором безопасности структурного подразделения.

3.2.2. Подача Заявки на подключение автоматизированного рабочего места к сегменту сети Интернет Центра (далее – Заявка) осуществляется через отдел связи и автоматизированных систем управления штаба Центра согласно установленной формы (приложение №2).

3.2.3. Подключение АРМ к сети.

4. ЗАДАЧИ, РЕШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ РЕСУРСОВ СЕТИ

Глобальная информационная сеть используется для:

4.1. Повышения квалификации должностных лиц, необходимой для выполнения своих должностных обязанностей.

4.2. Удаленного обучения должностных лиц.

4.3. Проведения видеоконференций с органами ФОИВ, ОИВ и подрядными организациями.

4.4. Доступа к правовым и законодательным базам данных.

4.5. Контактов с должностными лицами других государственных структур.

4.6. Обмена электронной почтой с должностными и частными лицами по не конфиденциальным вопросам.

4.7. Поиска и сбора информации по вопросам напрямую связанным с выполнением должностным лицом его должностных обязанностей.

4.8. Доступа к картографическим и поисковым базам данных.

4.9. Доступа к информационным системам персональных данных.

4.10. Доступа к государственным информационным системам.

4.11. Доступа к официальным ресурсам МЧС России и государственных структур Российской Федерации.

5. ОГРАНИЧЕНИЕ ДОСТУПА К РЕСУРСАМ СЕТИ

5.1. Отдел связи и автоматизированных систем управления штаба Центра оставляет за собой право блокировать или ограничивать доступ должностных лиц к Интернет-ресурсам в следующих случаях:

5.1.1. Содержание ресурсов не имеет отношения к исполнению служебных обязанностей.

5.1.2. Ресурсы, содержание и направленность которых запрещены Российским законодательством.

5.1.3. Должностное лицо не выполняет должностные обязанности связанные с использованием сети.

5.2. Должностным лицам Центра при использовании сети запрещается:

5.2.1. Использовать предоставленный доступ в сеть Интернет в личных целях.

5.2.2. Использовать специализированные аппаратные и программные средства, позволяющие должностным лицам получить несанкционированный доступ к сети Интернет.

5.2.3. Совершать любые действия, направленные на нарушение нормального функционирования сети.

5.2.4. Фальсифицировать свой IP-адрес, а также прочую служебную информацию.

5.2.5. Публиковать, загружать и распространять материалы, содержащие конфиденциальную информацию за исключением случаев, когда это входит в

служебные обязанности и способ передачи является безопасным, согласованным с администратором безопасности структурного подразделения заранее.

5.2.6. Публиковать, загружать и распространять материалы, содержащие информацию, полностью или частично, защищенную авторскими или другим правами, без разрешения владельца.

5.2.7. Публиковать, загружать и распространять материалы, содержащие вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также серийные номера к коммерческому ПО и ПО для их генерации, пароли и прочие средства для получения несанкционированного доступа к платным Интернет-ресурсам, а также ссылки на вышеуказанную информацию.

5.2.8. Публиковать, загружать и распространять материалы содержащие 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 и т.д.

6. ОБЯЗАННОСТИ ДОЛЖНОСТНЫХ ЛИЦ ПРИ РАБОТЕ В СЕТИ

Должностное лицо при работе в сети обязано:

6.1. Соблюдать требования настоящей Инструкции.

6.2. Использовать сеть исключительно для выполнения своих служебных обязанностей.

6.3. Ставить в известность администратора безопасности структурного подразделения о любых фактах нарушения требований настоящей Инструкции.

6.4. Расценивать файлы, загружаемые из сети, как небезопасные и подвергать данные файлы обязательной проверке на отсутствие вредоносного ПО.

Начальник связи – начальник отдела связи и
автоматизированных систем управления штаба

полковник С.Н. Собаков

Приложение №2
к приказу начальника Ногинского СЦ
от «19» 03 20 22 г. № 151

ФОРМА ЗАЯВКИ НА ПОДКЛЮЧЕНИЕ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА К СЕГМЕНТУ СЕТИ ИНТЕРНЕТ

Начальнику связи Ногинского СЦ

Заявка
на подключение автоматизированного рабочего места к сегменту сети Интернет

Прошу Вас организовать работу по подключению к сегменту сети Интернет и предоставлению доступа к информационным ресурсам и сервисам сети Интернет автоматизированного рабочего места

_____

_____,

(должность, звание, ФИО сотрудника)

Расположенного в помещении:

_____

_____ в кабинете № ____

в связи _____

(обоснование согласно должностным обязанностям)

Указанное помещение предназначено (не предназначено) для ведения
(ненужное зачеркнуть)
переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну.

«__» _____ 20__ г. Начальник структурного подразделения