МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное учреждение науки
ИНСТИТУТ ФИЗИКИ МЕТАЛЛОВ имени М.Н. Михеева
Уральского отделения Российской академии наук

П Р И К А З

«_26_» _ноября_ 2018 г. № _146_

г. Екатеринбург

О работе в сети «Интернет»

В целях обеспечения защиты информационных ресурсов Института, в соответствии с требованиями Федерального закона «Об информации, информатизации и защите информации» от 27 июля 2006 года № 149-ФЗ

ПРИКАЗЫВАЮ:

1. Утвердить Положение об организации работы пользователей телекоммуникационной сети Института с выходом в «Интернет» (далее – Положение) (приложение 1).

2. Главному специалисту по защите информации СМЕРДОВУ А.П. обеспечить систематический контроль за соблюдением требований Положения и других нормативно-правовых документов, регламентирующих деятельность в области защиты информации (приложение 2).

3. Контроль за исполнением приказа возложить на заместителя директора по безопасности и режиму СВИНЦОВА С.А.

Директор института,
академик РАН Н.В. Мушников

Приложение 1 к приказу
от 26.11.2018 № 146

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное учреждение науки
ИНСТИТУТ ФИЗИКИ МЕТАЛЛОВ имени М.Н. Михеева
Уральского отделения Российской академии наук
(ИФМ УрО РАН)

УТВЕРЖДАЮ
Директор института,
академик РАН
_____ Н.В. Мушников
«26» ноября 2018 г.

ПОЛОЖЕНИЕ
об организации работы пользователей телекоммуникационной сети института с выходом в «Интернет»

Екатеринбург
2018 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящее «Положение об организации работы пользователей телекоммуникационной сети Института с выходом в «Интернет»» (далее «Положение») определяет требования к организации работ и порядку подключения серверов и персональных компьютеров к телекоммуникационной сети Института с выходом в «Интернет»» (далее «Сеть») с учетом условий обеспечения безопасности информации и эффективного использования ресурсов и возможностей сети.

1.2. Положение разработано на основании Федерального закона «Об информации информатизации и защите информации» от 27 июля 2006 года №149-ФЗ, «Доктрины информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации 9 сентября 2000 года № Пр-1895, «Специальных требований и рекомендаций по защите конфиденциальной информации» (СТР-К) утвержденных приказом Гостехкомиссии России 30 августа 2002 года № 282, указа Президента «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17 марта 2008 года № 351 и других нормативно-правовых документов в области защиты информации.

1.3. Ответственность за организацию работ по защите информации в институте возлагается на одного из заместителей директора Института, согласно распределению обязанностей в дирекции, и на руководителей структурных подразделений Института.

1.4. Подключение, техническое обслуживание и администрирование работы в Сети осуществляет отдел электронных коммуникаций Института.

1.5. Ответственность за реализацию требований настоящего Положения при проведении работ с использованием Сети возлагается в пределах их компетенции на:

- главного специалиста по защите информации;
- администратора Сети;
- руководителей структурных подразделений Института;
- работников отдела электронных коммуникаций, осуществляющих подключение и техническое обслуживание серверов;
- исполнителей работ на персональных компьютерах.

2. ПОРЯДОК ПОДКЛЮЧЕНИЯ К СЕТИ

2.1 Компьютеры и серверы, подключаемые к сети, должны быть сконфигурированы таким образом, чтобы обеспечить адекватную защиту от несанкционированного доступа к ним через Сеть. Подключение осуществляет отдел электронных коммуникаций Института.

2.2 Запрещается подключение к Сети компьютеров и серверов, обрабатывающих конфиденциальную информацию и сведения, содержащие государственную тайну.

3. ТРЕБОВАНИЯ К ПРОВЕДЕНИЮ РАБОТ В СЕТИ

3.1 Приказом директора Института, по представлению руководителя отдела электронных коммуникаций и согласованию с главным специалистом по защите информации, назначается администратор Сети, отвечающий за вопросы организации работ в Сети Института, в том числе с учетом требований обеспечения безопасности информации.

3.2 Пароли для различных ресурсов сети, почтовых аккаунтов должны быть достаточно сложными для подбора и уникальными для каждого ресурса.

Ответственность за дискретизацию пароля лежит на пользователе.

3.3 Запрещается запоминание (хранение) парольной информации в операционной системе персонального компьютера. Ввод пароля пользователя производится вручную каждый раз при подключении к информационным системам.

3.4 Установка и настройка программного обеспечения персональных компьютеров для доступа к Сети должна производиться работником отдела электронных коммуникаций по предварительной заявке или лицом ответственным за работу данного компьютера под контролем администратора Сети.

3.5 Структурные подразделения Института за счет своих ресурсов обязаны обеспечить на всех имеющихся в данном подразделении серверах и компьютерах наличие антивирусной защиты.

Средства антивирусной защиты должны быть сертифицированы и обеспечивать защиту данных, обрабатываемых с использованием информационно-коммуникационных технологий в соответствии с требованиями, предъявляемыми к информационной системе.

3.6 Все получаемые из Сети файлы (тексты, программы, архивы и др.) должны обязательно проверяться на отсутствие компьютерных вирусов до открытия и копирования их на другие компьютеры.

4. ОРГАНИЗАЦИЯ КОНТРОЛЯ ЗА РАБОТОЙ В СЕТИ

4.1 Текущий контроль за выполнением требований информационной безопасности при работе в Сети осуществляют руководители соответствующих структурных подразделений и пользователи персональных компьютеров.

4.2 Текущий контроль за выполнением требований информационной безопасности в Сети по Институту в целом осуществляет администратор сети.

4.3 Периодический контроль технической защиты информации при работе в Сети организует главный специалист по защите информации с привлечением специалистов необходимого профиля и квалификации. Результаты контроля оформляются актом, представляемым на утверждение директору Института.

5. ОСНОВНЫЕ ПРАВА И ОБЯЗАННОСТИ АДМИНИСТРАТОРА СЕТИ

5.1 Администратор Сети является штатным сотрудником отдела электронных коммуникаций. Он назначается приказом директора по представлению началь-

ника отдела электронных коммуникаций, согласованным с главным специалистом по защите информации Института, и подчиняется начальнику отдела.

5.2 Администратор Сети должен иметь специальное профильное образование и обладать профессиональными навыками администрирования и настройки современных программных и программно-технических средств.

5.3 Решение вопросов обеспечения информационной безопасности входит в служебные обязанности администратора Сети. Он несет ответственность за реализацию и состояние защиты информации от несанкционированного доступа (далее НСД).

5.4 Администратор Сети (с учетом действующих в Институте норм обеспечения охраны служебной (коммерческой) тайны) обладает правами доступа к любым информационным, программным и аппаратным ресурсам Сети и средствам их защиты, за исключением средств защиты государственной тайны.

5.5 Методическое руководство работой администратора Сети по защите от НСД в установленном порядке осуществляет главный специалист по защите информации.

5.6 Администратор Сети обязан:

5.6.1 Знать требования основных законодательных, нормативных и руководящих документов в области защиты от НСД к информации.

5.6.2 Осуществлять учет и постоянный контроль за составом программного и технического обеспечения серверов и полномочиями пользователей серверов.

5.6.3 Осуществлять установку и настройку средств защиты информации (далее СЗИ) от НСД на серверы и периодически проводить проверку правильности функционирования СЗИ (выборочное тестирование).

5.6.4 Предоставлять пользователям серверов необходимые полномочия и определять им идентификаторы.

5.6.5 Своевременно обновлять антивирусные базы и средства защиты на серверах Института и систематически осуществлять контроль адекватности антивирусной защиты серверов Сети.

5.6.6 Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования серверов и персональных компьютеров пользователей, работающих в Сети, и осуществления НСД к информации. При обнаружении попыток НСД к информации принимать необходимые меры по устранению нарушений и их дальнейшему предотвращению.

5.6.7 Участвовать в расследовании причин совершения нарушений и возникновения кризисных ситуаций в результате НСД в Сеть.

5.6.8 Осуществлять периодический контроль соблюдения норм и инструкций по обеспечению безопасности информации при работе в сети «Интернет».

5.6.9 При необходимости проводить занятия с сотрудниками Института по требованиям основных законодательных, нормативных и руководящих документов, действующих в области защиты от НСД к информации.

5.7 Администратор Сети имеет право:

5.7.1 Требовать от пользователей персональных компьютеров соблюдения утвержденных инструкций по обеспечению безопасности информации при работе в сети «Интернет».

5.7.2 Прекращать работу серверов и персональных компьютеров при несоблюдении настоящего Положения и других утвержденных инструкций по обеспечению безопасности информации при работе в Сети, информируя об этом руководителей соответствующих подразделений и начальника отдела электронных коммуникаций.

5.7.3 Обращаться к главному специалисту по защите информации Института с просьбами об оказании необходимой помощи в своей работе.

5.8 Администратор Сети несет персональную ответственность за качество выполняемых им работ, в том числе, по обеспечению защиты Сети от НСД в соответствии с функциональными обязанностями.

6. ОСНОВНЫЕ ПРАВА И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ СЕТИ

6.1 Пользователь Сети обязан:

6.1.1 Строго выполнять требования настоящего Положения, технических и иных норм и инструкций по работе в Сети, в том числе норм и инструкций по защите информации.

6.1.2 Соблюдать действующее законодательство, в том числе в области охраны интеллектуальной собственности.

6.1.3 Ежедневно в автоматическом режиме производить антивирусный контроль персонального компьютера и следить за регулярным обновлением баз антивирусных средств, согласно Инструкции по организации антивирусной защиты (Приложение 1 к настоящему Положению).

6.1.4 Своевременно информировать администратора Сети о замеченных нарушениях режима парольной защиты, попытках НСД к информации и ресурсам Сети, о случаях нарушения целостности программного обеспечения.

6.2 Пользователю Сети запрещается:

6.2.1 Использовать любые программные и аппаратные средства, которые могут привести к перегрузке Сети или иным способом негативно повлиять на ее работу.

6.2.2 Несанкционированный вход на чужие компьютеры (и/или) серверы Сети, подбор паролей для несанкционированного доступа и сканирование Сети и отдельных компьютеров.

6.2.3 Использовать любые программные или аппаратные средства для несанкционированного доступа к компьютерам, маршрутизаторам и другим ресурсам Сети.

6.2.4 Вносить изменения в файлы, не принадлежащие самому пользователю.

6.2.5 Разрабатывать и/или распространять любые виды компьютерных вирусов.

6.2.6 Использовать доступ к Сети в целях, не имеющих отношения к выполнению его служебных обязанностей, в том числе для нужд частного бизнеса и коммерческой рекламы.

6.2.7 Использовать компьютеры Института для любых видов противозаконной деятельности.

6.2.8 Обрабатывать и хранить в Сети сведения, содержащие государственную тайну и конфиденциальную информацию.

6.2.9 Несанкционированно устанавливать на компьютер аппаратные и программные средства удаленного доступа. При необходимости установки средств уда-

ленного доступа в рабочих целях требуется согласование с заместителем директора института по информационным и коммуникационным технологиям.

7. ОПУБЛИКОВАНИЕ МАТЕРИАЛОВ В СЕТИ

7.1 Под опубликованием материалов в Сети понимается перенос информации с персонального компьютера на другой, не входящий в Сеть Института, компьютер с использованием сетевых средств передачи информации, в том числе:

- отправка факсимильных сообщений и электронной почты;
- участие в телеконференциях;
- размещение материалов на серверах и сайтах (веб-страницах) провайдера, своих или других (сторонних) пользователей Сети;
- создание собственных и участие в наполнении сторонних сетевых баз данных;
- размещение информации в сети иными способами, при которых она становится доступной неопределенному кругу лиц.

7.2 Публикуемые материалы должны удовлетворять предъявляемым для открытой печати требованиям действующего законодательства в отношении охраны информации, государственной, служебной (коммерческой) тайны, прав интеллектуальной собственности и других ограничений, устанавливаемых, в частности, настоящим Положением и иными нормативными актами Института.

7.2.1 Перед опубликованием в сети:

- материалов, помещаемых на серверах и сайтах (веб-страницах) независимо от принадлежности последних,
- монографий,
- статей,
- докладов,
- тезисов,
- препринтов,
- баз данных,

содержащих неопубликованные сведения о научных и научно - технических результатах, полученных в Институте, должно быть оформлено Заключение о возможности открытого опубликования в соответствии с действующим в Институте «Положением о порядке подготовки материалов, предназначенных для открытого опубликования и вывоза за границу». При отправке документов и материалов за границу дополнительно в установленном порядке оформляется разрешение-ходатайство на вывоз за границу.

7.4 Персональную ответственность за соблюдение установленного порядка публикации материалов и их содержание несут руководители структурных подразделений и сотрудники Института, осуществляющие публикацию.

Приложение 1 к
ПОЛОЖЕНИЮ

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ

Настоящая Инструкция определяет требования к организации защиты локальной вычислительной сети, серверов и персональных компьютеров с установленной операционной системой Windows от разрушающего воздействия компьютерных вирусов и устанавливает ответственность за их выполнение руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих ресурсы информационно-телекоммуникационной сети ИФМ УрО РАН (далее – ИТС).

К использованию в ИТС допускаются только сертифицированные антивирусные средства, закупленные у разработчиков (поставщиков) указанных средств.

ПРИМЕНЕНИЕ СРЕДСТВ АНТИВИРУСНОГО КОНТРОЛЯ

Ежедневно в начале работы при загрузке компьютера (для серверов локальной вычислительной сети - при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.

Базы антивирусных средств подлежат регулярному обновлению в автоматическом режиме.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая в ИТС, а также информация на съемных носителях.

Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, потеря и(или) кодирование файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно должен провести внеочередной антивирусный контроль своего персонального компьютера или, при необходимости, привлечь специалистов отдела электронных коммуникаций для определения ими факта наличия или отсутствия компьютерного вируса.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов сотрудников отдела электронных коммуникаций, владельца зараженных файлов, если эти файлы принесены на съемном носителе;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов отдела электронных коммуникаций);
- по факту обнаружения зараженных вирусом файлов составить служебную записку на имя заместителя директора института, отвечающего за защиту информации, в которой необходимо указать предположительный источник (отправителя,

владельца и т.д.) зараженного файла, тип зараженного файла и выполненные антивирусные мероприятия.

ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИТС ОТ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Данные требования минимизируют вероятность возникновения негативных последствий для вашего персонального компьютера и ИТС в целом, причина возникновения которых связана с распространением вредоносного программного обеспечения.

1. **Запрещено** открывать вложения к сообщениям электронной почты, полученные из неизвестных, подозрительных или недоверенных источников. Такие вложения должны незамедлительно удаляться.

2. Сообщения электронной почты, содержащей спам, цепочки сообщений и другую нежелательную почту должны удаляться без пересылки.

3. **Запрещено** скачивать информацию из неизвестных или подозрительных источников.

4. Необходимо избегать предоставления общего доступа к дискам с правами чтения/записи в случае если это не требуется в рамках выполнения основной деятельности.

5. Прежде чем использовать переносные носители информации необходимо просканировать их на отсутствие вирусов.

6. Необходимо регулярно резервировать важные данные и настройки системы. Резервные копии хранить в безопасном месте.

7. В случае необходимости запуска приложения, конфликтующего с установленным антивирусным программным обеспечением, необходимо выполнить полную проверку компьютера на наличие вирусов, отключить антивирусное программное обеспечение и запустить необходимое приложение. Должно быть доподлинно известно, что запускаемое приложение не приведет к негативным последствиям.

После выполнения задач, связанных с использованием приложения, возобновите работу антивирусного программного обеспечения. При отключенном антивирусном программном обеспечении запрещается запускать любые приложения (электронная почта или открытие общего доступа к файловым ресурсам), в результате действия которых ваш персональный компьютер может быть подвержен инфицированию вредоносным ПО.

Ответственность за организацию антивирусного контроля в структурном подразделении возлагается на руководителя структурного подразделения.

Ответственность за организацию антивирусного контроля и соблюдение требований по защите ИТС от угроз информационной безопасности возлагается на пользователей персональных компьютеров.

Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками подразделений организации осуществляется работниками отдела электронных коммуникаций совместно с главным специалистом по защите информации института.

Список рекомендованных средств антивирусной защиты:

- Kaspersky Lab Internet Security (имеет сертификат ФСТЭК России)
- ESET NOD32 Internet Security (имеет сертификат ФСТЭК России)
- Bitdefender Antivirus Free Edition
- Norton Security
- Avira Antivirus Pro
- Avast Internet Security
- Avast Free Antivirus

Приложение 2
К приказу

**Перечень нормативно-правовых документов,
регламентирующих деятельность в области защиты информации**

1. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Руководящий документ: «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», утверждена решением Гостехкомиссии при Президенте Российской Федерации от 30 марта 1992 г.
3. Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 28.06.2014) «Об электронной подписи».
4. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
5. Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
6. Постановление Правительства РФ от 18 ноября 2013 г. № 1035 «О федеральной информационной системе государственной научной аттестации».
7. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
8. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
9. ФСБ России № 416, ФСТЭК России № 489 Приказ от 31 августа 2010 года «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».