Министерство науки и высшего образования
Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ
ИНСТИТУТ СИСТЕМ ЭНЕРГЕТИКИ
им. Л.А. МЕЛЕНТЬЕВА
СИБИРСКОГО ОТДЕЛЕНИЯ
РОССИЙСКОЙ АКАДЕМИИ НАУК
(ИСЭМ СО РАН)

П Р И К А З

от "4" апреля 2024 г. г. Иркутск № 10

Об утверждении политики информационной безопасности и инструкции пользователя информационных систем ИСЭМ СО РАН

В целях принятия дальнейших мер по защите информации в ИСЭМ СО РАН (далее – Институт) в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации приказываю:

1. Утвердить и ввести в действие Политику информационной безопасности ФГБУН «ИСЭМ СО РАН» (Приложение № 1).
2. Утвердить и ввести в действие Инструкцию пользователя информационных систем ФГБУН «ИСЭМ СО РАН» (Приложение № 2).
3. Руководство работами по внедрению и актуализации Политики информационной безопасности возложить на начальника научно-технического отдела информационных технологий и информационной безопасности Пальцева А.С.
4. Обязанности по контролю соблюдения требований Политики информационной безопасности возложить на сотрудников научно-технического отдела информационных технологий и информационной безопасности.
5. Контроль за исполнением настоящего приказа оставляю за собой.

Директор института
академик РАН В.А. Стенников

Приложение №2
к приказу №_10_ от "_4_" _апреля_ 2024 г.

Инструкция пользователя информационных систем ФГБУН «Институт Систем Энергетики им. Л.А. Мелентьева СО РАН»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция пользователя информационных систем (далее - «Инструкция») определяет общие правила работы в информационных системах и сетях ФГБУН «Институт систем энергетики им. Л.А. Мелентьева СО РАН» (далее - «Институт»).

1.2. Настоящая Инструкция разработана в соответствии с требованиями Политики информационной безопасности Института. Сокращения, термины и определения, используемые в настоящей Инструкции, соответствуют Политике информационной безопасности Института.

1.3. Пользователями являются все сотрудники Института и третьи лица, имеющие доступ к информационным ресурсам и информационным системам (вычислительному и сетевому оборудованию, аппаратным средствам, программному обеспечению, данным и средствам их защиты) Института.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, должностной инструкцией, Положением о своем подразделении, Политикой информационной безопасности Института, Уставом Института, а также нормативными и законодательными актами Российской Федерации.

1.5. Методическое руководство работой пользователя в информационных системах и сетях Института осуществляет его непосредственный руководитель, а также руководитель и сотрудники НТО ИТИБ.

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

2.1. Знать и выполнять требования законодательных актов Российской Федерации, настоящей Инструкции, Политики информационной безопасности и других внутренних документов Института, регламентирующих правила работы в информационных системах.

2.2. Выполнять на рабочем месте с использованием средств вычислительной техники только те действия, которые определены должностной инструкцией, служебными либо договорными обязанностями.

2.3. Использовать информационные ресурсы и системы Института только для выполнения порученных работ, а также исполнения должностных либо договорных обязанностей.

2.4. При прекращении трудовых отношений все средства вычислительной техники, а также материальные носители, содержащие служебную информацию (usb-накопители, магнитные и оптические диски и т.д.) - передать непосредственному руководителю в надлежащем состоянии.

3. ПРАВА ПОЛЬЗОВАТЕЛЯ

3.1. Использовать информационные ресурсы и системы Института, сеть Интернет, электронную почту для выполнения должностных обязанностей.

3.2. Направлять своему руководителю и руководителю НТО ИТИБ обоснованные предложения по приобретению и установке, а также модернизации программного и аппаратного обеспечения.

3.3. Получать от своего руководителя и сотрудников НТО ИТИБ инструктаж и консультации по правилам работы с информационными ресурсами, системами, сетью Интернет, электронной почтой и т.д.

3.4. Обращаться за помощью и консультациями в НТО ИТИБ по адресам электронной почты: **admin@isem.irk.ru , paltsev@isem.irk.ru.**

4. ПРАВИЛА И ОГРАНИЧЕНИЯ

Пользователю ЗАПРЕЩАЕТСЯ:

4.1. Нарушать установленные в Институте правила работы в информационных системах и сетях.

4.2. Получать (приносить, скачивать), хранить, устанавливать и использовать программное обеспечение, которое не требуется для выполнения должностных обязанностей.

4.3. Использовать программное и аппаратное обеспечение Института в неслужебных (личных) целях.

4.4. Оставлять свое рабочее место, предварительно не заблокировав рабочий сеанс и не предприняв соответствующих мер по защите информации на физических носителях.

4.5. Без согласования с НТО ИТИБ изменять состав и конфигурацию используемых программных и аппаратных средств, устанавливать и модифицировать программное и аппаратное обеспечение.

4.6. Выполнять действия, направленные на получение несанкционированного доступа к информационным системам, компьютерам, серверам и сетям Института, а также к ресурсам сети Интернет.

4.7. Изменять параметры средств защиты информации (в том числе настройки брандмауэра и средств антивирусной защиты), а также прекращать их работу.

4.8. Использовать нерегламентированные (не относящиеся к работе, не разрешенные) программы и ресурсы: создающие избыточную нагрузку на сеть (игры, музыка, фильмы, P2P-клиенты), средства удаленного администрирования и т.д.

4.9. Без согласования с НТО ИТИБ создавать сетевые ресурсы совместного использования (папки и файлы общего доступа). Изменять содержимое сетевых ресурсов или права доступа к ним без разрешения их владельцев. Предоставлять права к любым ресурсам вида: «полный доступ для всех». Разрешать неавторизованный (анонимный, гостевой) доступ к сетевым ресурсам с правом на запись (изменение) содержимого.

4.10. В случае возникновения неисправностей в вычислительном или сетевом оборудовании Института - самостоятельно их устранять, не поставив в известность

непосредственного руководителя, а также руководителя или сотрудников НТО ИТИБ.

4.11. Препятствовать должностным лицам и ответственным сотрудникам Института при проведении проверок и служебных расследований, связанных с обеспечением информационной безопасности.

4.12. Удалять или изменять программы и файлы со служебными данными и иной важной информацией.

4.13. Использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты информации, которые могут привести к возникновению внештатной ситуации или к компьютерному инциденту.

4.14. Без согласования с руководителем НТО ИТИБ подключать к сетям Института личные средства вычислительной техники, мобильные и сетевые устройства, а также изменять IP-адреса, MAC-адреса и иные сетевые настройки любого оборудования.

4.15. Несанкционированно распространять конфиденциальную информацию, содержащую персональные данные, служебную или коммерческую тайну.

4.16. Распространять и получать материалы, противоречащие законодательству Российской Федерации и внутренним правилам Института.

5. ПАРОЛИ

5.1. Общие требования к паролям

5.1.1. Минимальная длина пароля (для компьютера, электронной почты и т.п.): восемь символов.

5.1.2. Минимальное требование к составу пароля: как минимум одна буква латинского алфавита в верхнем и нижнем регистре, одна цифра и один специальный символ типа ! @ # $ % ^ & * _ = и т.п.

5.1.3. Нельзя использовать повторно ранее использованные пароли.

5.1.4. Пароль не должен совпадать с именем учетной записи (логином) и содержать легко угадываемые слова и числа (имена, даты рождения и т.п.), общепринятые сокращения, номера документов и иную информацию о пользователе, доступную третьим лицам.

5.1.5. Нельзя использовать в качестве пароля один повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

5.1.6. Нельзя использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (123456, qwerty и т.п.).

5.2. Правила использования паролей

5.2.1. Пользователю **ЗАПРЕЩАЕТСЯ:**

- сообщать свой пароль третьим лицам;
- предоставлять третьим лицам доступ к своей рабочей станции, информационным системам, электронной почте и т.п. под своей учетной записью и паролем;
- записывать и хранить пароли в легкодоступных местах: в ящике стола, на мониторе, на листах бумаги, на клавиатуре и т.д.

5.2.2. Пользователь **ОБЯЗАН:**

- при вводе пароля - исключить возможность его считывания посторонними лицами или техническими средствами;
- немедленно сообщать руководителю и в НТО ИТИБ об утере, утечке, несанкционированном изменении пароля.

5.2.3. Внеплановая замена или удаление пароля пользователя производится в следующих случаях:

- при подозрении на компрометацию пароля;
- при прекращении полномочий (увольнение, смена обязанностей);
- по указанию руководителя или сотрудников НТО ИТИБ.

5.2.4. При увольнении или смене обязанностей пользователя, имеющего, кроме своей учетной записи, доступ к другим ресурсам (сетевое оборудование, серверы, административные учетные записи и т.п.) - производится также внеплановая смена паролей к этим ресурсам.

6. АНТИВИРУСНАЯ ЗАЩИТА

6.1. Пользователь **ОБЯЗАН** производить антивирусную проверку всех файлов, полученных им любым способом и из любого места.

6.2. При подозрении на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажение и пропадание данных, частые сообщения об ошибках и т.п.), пользователь должен поставить в известность сотрудника НТО ИТИБ и провести полную антивирусную проверку своей рабочей станции.

6.3. В случае обнаружения вируса, пользователь должен:

- прекратить работу (если завершение работы штатными средствами невозможно - отключить рабочую станцию от электрической сети);
- немедленно поставить в известность сотрудника НТО ИТИБ;
- совместно с сотрудником НТО ИТИБ провести лечение или уничтожение зараженных файлов.

7. РЕЗЕРВНОЕ КОПИРОВАНИЕ

7.1. Пользователю рекомендуется регулярно самостоятельно выполнять резервное копирование своих файлов на внешний носитель (usb-накопитель, жесткий или оптический диск и т.п.), либо на сетевой ресурс (облачное хранилище Института и т.п.).

7.2. Перед резервным копированием файлов необходимо завершить работу всех программ и закрыть все редактируемые документы.

7.3. Резервные копии данных в облачном хранилище Института должны храниться в архивированном виде (с целью экономии места).

7.4. Категорически **ЗАПРЕЩАЕТСЯ** хранить резервные копии вместе с исходными данными на одном физическом носителе (usb-накопителе, жёстком диске).

7.5. Пользователь несет персональную ответственность за целостность и сохранность рабочих файлов и документов на своей рабочей станции.

8. РАБОТА В ИНФОРМАЦИОННЫХ СИСТЕМАХ, В СЕТИ ИНТЕРНЕТ, С ЭЛЕКТРОННОЙ ПОЧТОЙ

8.1. Общие положения

8.1.1. Доступ к информационным системам, электронной почте Института и сети Интернет предоставляется пользователю Института в случае, если это не противоречит требованиям по информационной безопасности, указанным в политике информационной безопасности, данной Инструкции и иных нормативных документах Института.

8.1.2. Основанием для подключения рабочей станции пользователя к информационным системам, электронной почте, сети Интернет является заявка руководителю НТО ИТИБ от пользователя с указанием нужных сервисов для подключения.

8.1.3. После получения заявки сотрудник НТО ИТИБ организует подключение рабочей станции пользователя к указанным информационным ресурсам.

8.1.4. Сотрудники НТО ИТИБ осуществляют контроль над использованием в Институте информационных систем, электронной почты и сети Интернет.

8.1.5. Рабочая станция пользователя может быть отключена от информационных ресурсов Института, электронной почты и сети Интернет на основании:

- нарушения пользователем данной Инструкции и иных нормативных актов Института в области информационной безопасности;
- увольнения пользователя либо смены его обязанностей;
- обнаружения попыток несанкционированного доступа, компьютерных атак, а также расследования компьютерного инцидента;
- проведения технических работ.

8.2. Правила работы в сети Интернет

8.2.1. Использование сети Интернет в Институте осуществляется исключительно для выполнения должностных обязанностей.

8.2.2. Информация о ресурсах сети Интернет, посещаемых пользователями, протоколируется и может быть предоставлена руководству для анализа и принятия мер.

8.2.3. При использовании сети Интернет **ЗАПРЕЩАЕТСЯ:**

- предоставлять третьим лицам доступ в сеть Интернет со своей рабочей станции, в том числе программно-техническими способами;
- получать на рабочих станциях доступ к сети Интернет любым способом, кроме предоставленного Институтом (несанкционированно установленные GPRS-модемы, Wi-Fi-устройства и прочее), если это не согласовано с НТО ИТИБ. Основанием для использования данных устройств является заявление пользователя на имя руководителя НТО ИТИБ с указанием целей использования устройств и срока, в течение которого данные устройства будут использоваться. Заявление должно быть одобрено руководителем НТО ИТИБ. То же самое относится и к получению доступа к сети Интернет посредством технологии виртуальных частных сетей (VPN).

• открывать подозрительные ресурсы, переходить по подозрительным ссылкам, при открытии ресурса нужно убедиться в том, что он использует защищённое соединение (https://...)

8.3. Правила работы с электронной почтой

8.3.1. Корпоративная электронная почта Института предназначена исключительно для выполнения должностных обязанностей.

8.3.2. При работе с электронной почтой Института **ЗАПРЕЩАЕТСЯ:**

• рассылать почтовые сообщения одновременно на большое количество адресов, за исключением служебных объявлений;

• отправлять сообщения неэтичного или незаконного содержания;

• использовать рабочий адрес электронной почты для подписки на неслужебные почтовые рассылки (коммерческие, развлекательные и т.п.), а также для регистрации на сторонних сайтах (форумы, клубы и т.п.);

• отправлять и открывать при получении исполняемые или системные файлы (в частности, с расширениями bas, bat, bin, cab, cat, cmd, com, cpl, csh, dat, dll, dpl, drv, exe, inf, ins, inx, ipa, isu, jar, job, js, jse, ksh, lib, lnk, mdz, msc, msi, msp, mst, msu, nls, olb, osx, out, paf, pif, prg, pwz, reg, rgs, rom, run, scr, sct, sh, shb, shs, sys, tlb, vb, vbe, vbs, vbscript, vxd, workflow, ws, wsf, wsh), в том числе в составе архивных файлов;

• открывать вложенные файлы и ссылки, присланные в письмах от неизвестных отправителей, либо без предварительного запроса. При малейшем подозрении на то, что письмо может быть вирусным или мошенническим, необходимо писать или звонить в НТО ИТИБ.

9. ОТВЕТСТВЕННОСТЬ

Пользователь несет персональную (должностную, материальную, административную, уголовную) ответственность за свои действия или бездействие, которые повлекут за собой разглашение или утрату конфиденциальных (служебных, коммерческих, персональных и иных) данных, а также нарушение функционирования информационных систем, информационно-телекоммуникационной сети Института или ее отдельных компонентов, несанкционированный доступ к информации, нарушение требований настоящей Инструкции и других внутренних документов Института, регламентирующих правила работы в информационных системах, в соответствии с нормативными актами Института и законодательством Российской Федерации.