Приложение № 2
к Приказу от «05» февраля 2016 г. № 37

Национальный исследовательский центр
«Курчатовский институт»
Федеральное государственное бюджетное учреждение
«Петербургский институт ядерной физики им. Б.П. Константинова»

ИНСТРУКЦИЯ
пользователя информационных систем
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»

СОГЛАСОВАНО:
Протокол заседания Научно-технического
совета по информационным технологиям
ФГБУ «ПИЯФ» от 23.06.2015 г. № 10

г. Гатчина
2015 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция пользователя информационных систем (далее – «Инструкция») определяет общие правила работы в информационных системах и сетях ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» (далее – «Институт»).

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

1.3. Пользователями являются все работники Института и третьи лица, участвующие в процессах автоматизированной обработки данных и 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, Концепцией и Политикой ИБ Института, другими документами Института, регламентирующими обработку данных в информационных системах, Уставом Института, а также нормативными и законодательными актами Российской Федерации.

1.5. Информация, образованная в процессе трудовой деятельности пользователя, является собственностью Института и не подлежит использованию в личных целях пользователя либо других лиц и организаций.

1.6. Методическое руководство работой пользователя в информационных системах и сетях Института осуществляет его непосредственный руководитель, а также: работники, ответственные за администрирование сегментов информационной телекоммуникационной системы Института; работники, выполняющие функции администраторов локальной вычислительной сети; работники, выполняющие функции администраторов информационных систем; работники, выполняющие функции администраторов по обеспечению безопасности информации (далее – «администраторы»).

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

2.1. Знать и соблюдать законодательные, регулирующие и договорные требования по соблюдению авторских и смежных прав на интеллектуальную собственность в сфере программного обеспечения, а также в отношении научных и иных работ, произведений, трудов и материалов.

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

2.3. Выполнять на рабочем месте с использованием средств вычислительной техники (далее – «рабочая станция») только те процедуры

обработки данных, которые определены должностной инструкцией, служебными либо договорными обязанностями.

2.4. Использовать информационные ресурсы Института и переданные в распоряжение технические средства хранения, обработки и передачи информации только для выполнения порученных работ, а также исполнения должностных либо договорных обязанностей.

2.5. При прекращении работ (трудовых отношений) все материальные носители, содержащие служебную информацию (usb-накопители, магнитные и оптические диски, распечатки, черновики, кино- и фотоматериалы, модели, образцы и прочее) – передать непосредственному руководителю.

3. ПРАВА ПОЛЬЗОВАТЕЛЯ

3.1. Использовать информационные ресурсы и системы Института, сервисы сети Интернет для выполнения служебных обязанностей.

3.2. Направлять своему руководителю обоснованные предложения по приобретению и установке нового программного и аппаратного обеспечения.

3.3. Направлять своему руководителю обоснованные предложения по модернизации (по замене на новые аналоги) используемого программного и аппаратного обеспечения.

3.4. Получать от своего руководителя и администраторов консультации по правилам работы с информационными ресурсами, системами, сетевыми услугами и базами данных Института.

3.5. Обращаться за помощью и консультациями по адресу электронной почты: **help@pnpi.nrcki.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 нелицензионное программное обеспечение.

4.3. Нарушать авторские и смежные права на интеллектуальную собственность в отношении научных, литературных, художественных, кинематографических, музыкальных и иных работ, произведений, трудов и материалов.

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

4.5. Оставлять свое рабочее место, предварительно не заблокировав экран (рабочий сеанс) и не предприняв соответствующих мер по защите внутренней (служебной) информации на физических носителях.

4.6. Без согласования с руководителем и администратором изменять состав и конфигурацию используемых программных и аппаратных средств, устанавливать и модифицировать программное и аппаратное обеспечение.

4.7. Выполнять действия, направленные на получение

несанкционированного доступа к информационным системам, компьютерам, серверам и сетям Института, а также к ресурсам сети Интернет.

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

4.9. Использовать нерегламентированные (не относящиеся к работе, не разрешенные руководителем) программы и ресурсы: создающие избыточную нагрузку на сеть (игры, музыка, фильмы, P2P-клиенты); предназначенные для распространения или получения информации с нарушением авторских и смежных прав; средства удаленного администрирования и т.д.

4.10. Без согласования с руководителем 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.

4.11. В случае возникновения неисправностей в вычислительном или сетевом оборудовании Института – самостоятельно их устранять, не поставив в известность руководителя и администратора.

4.12. Препятствовать должностным лицам и ответственным работникам Института при проведении проверок и служебных расследований, связанных с обеспечением безопасности информации.

4.13. Удалять или искажать программы и файлы со служебными данными и иной важной информацией.

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

4.15. Использовать компьютерные административные учетные записи, за исключением обстоятельств, когда без этого невозможно выполнение должностных обязанностей.

4.16. Использовать административные учетные записи без пароля.

4.17. Устанавливать и использовать программное обеспечение, которое не требуется для выполнения должностных обязанностей.

4.18. Без согласования с руководителем и администратором 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.

4.19. Несанкционированно распространять конфиденциальную информацию, содержащую персональные данные, служебную или коммерческую тайну, а также сведения о сущности изобретения, исследования, разработки, модели или промышленного образца до официальной публикации информации о них.

4.20. 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: пользовательского – шесть символов, административного – восемь символов.

5.1.2. Минимальное требование к составу пароля: латинские буквы и цифры. Дополнительные требования к административным паролям: буквы в верхнем и нижнем регистрах, спецсимволы типа: (! @ # $ % ^ & * - _ < >).

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.).

5.1.7. Период замены пользовательского пароля: один раз в год. Рекомендованный интервал – шесть месяцев.

5.1.8. Период замены административного пароля: один раз в полгода. Рекомендованный интервал – три месяца.

5.2. Правила использования паролей

5.2.1. Пользователю **ЗАПРЕЩАЕТСЯ:**

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

5.2.2. Пользователь **ОБЯЗАН:**

- изменять свой пароль по требованию операционной системы, информационной системы либо администратора;
- при вводе пароля – исключить возможность его считывания посторонними лицами или техническими средствами;
- немедленно сообщать руководителю и администратору об утере, утечке, несанкционированном изменении пароля или срока его действия.

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

- при подозрении на компрометацию (раскрытие, утечку) пароля;
- при окончании срока действия пароля;
- при прекращении полномочий (увольнение, смена обязанностей);
- по указанию администратора.

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 от любого абонента.

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 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 администратора;
- совместно с владельцем зараженных файлов выяснить необходимость их дальнейшего использования;
- совместно с администратором провести лечение или уничтожение зараженных файлов.

7. РЕЗЕРВНОЕ КОПИРОВАНИЕ

7.1. Рекомендуется регулярно (не реже одного раза в неделю) самостоятельно выполнять резервное копирование своих файлов на внешний носитель (usb-накопитель, жесткий или оптический диск и т.п.) либо на сетевой ресурс (сетевая папка на сервере, облачное хранилище и т.п.).

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

7.3. Резервные копии данных на локальных дисках и в пользовательских сетевых папках на серверах Института должны храниться в сжатом виде (в формате zip, 7z и т.п.). Для сжатия данных рекомендуется бесплатная свободно распространяемая программа 7zip.

7.4. Доступ к содержимому резервных копий должен быть защищен паролем. Требования к уровню сложности паролей:

- архивы на локальных дисках – «пользовательский»;
- архивы на сетевых папках и на внешних сетевых ресурсах (облачные хранилища и пр.) – «административный».

7.5. Категорически **ЗАПРЕЩАЕТСЯ** хранить резервные копии вместе с исходными данными на одном физическом носителе (usb-накопителе, диске, дисковом массиве и т.д.).

7.6. 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 только в том случае, если это не противоречит требованиям по информационной безопасности, указанным в данной Инструкции и иных нормативных документах Института.

8.1.2. Техническая возможность получить доступ к информационным ресурсам или сервисам не гарантирует того, что запрошенный ресурс или сервис разрешен пользователю политиками и правилами Института.

8.1.3. Основанием для подключения рабочей станции пользователя к информационным системам, электронной почте, сети Интернет является заявка ответственному лицу от руководителя пользователя с указанием требуемого ресурса и полномочий доступа к нему.

8.1.4. После получения заявки администратор организует подключение рабочей станции пользователя к указанным информационным ресурсам.

8.1.5. Администраторы осуществляют контроль над использованием в Институте информационных систем, электронной почты и сети Интернет.

8.1.6. Рабочая станция пользователя может быть отключена от информационных ресурсов Института и сети Интернет на основании:

- нарушения пользователем данной Инструкции и иных нормативных актов Института в области информационной безопасности;
- нарушения пользователем действующего законодательства в сфере информационных технологий, а также авторских и смежных прав;
- увольнения пользователя либо смены его обязанностей;
- обнаружения и расследования попыток несанкционированного доступа, вирусных и иных атак;
- проведения технических работ.

8.2. Правила работы в сети Интернет

8.2.1. Использование сервисов сети Интернет в Институте осуществляется 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 ресурсов 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, WiFi-устройства и прочее).

8.3. Правила работы с электронной почтой

8.3.1. Электронная почта Института предназначена для выполнения должностных обязанностей.

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

- рассылать почтовые сообщения одновременно на множество

адресов, за исключением служебных объявлений;

- использовать не свой обратный адрес при отправке почты;
- отправлять сообщения неэтичного или незаконного содержания;
- отправлять незатребованную или непроверенную информацию;
- 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 любые вложенные файлы без предварительной проверки антивирусными средствами;
- открывать вложенные файлы и ссылки, присланные от неизвестных отправителей либо без предварительного запроса.

8.3.3. При работе с электронной почтой **РЕКОМЕНДУЕТСЯ:**

- отвечать на рабочие письма в течение 24 часов с момента их получения (за исключением выходных и праздничных дней);
- на время длительного отсутствия создать уведомление, в котором указать срок отсутствия и контактные данные замещающего работника.

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 либо нарушение авторских и смежных прав в соответствии с нормативными актами Института и законодательством Российской Федерации.