ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ НАУЧНОЕ УЧРЕЖДЕНИЕ
«ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
«КРАСНОЯРСКИЙ НАУЧНЫЙ ЦЕНТР
СИБИРСКОГО ОТДЕЛЕНИЯ РОССИЙСКОЙ АКАДЕМИИ НАУК»
(КНЦ СО РАН, ФИЦ КНЦ СО РАН)

ПРИКАЗ

10.04.2026 N58 а/х

г. Красноярск

О мерах по повышению защищенности информационной инфраструктуры

В целях актуализации нормативных документов ФИЦ КНЦ СО РАН в части обеспечения информационной безопасности,

ПРИКАЗЫВАЮ:

1. Утвердить Регламент эксплуатации автоматизированных рабочих мест работников ФИЦ КНЦ СО РАН в новой редакции согласно Приложению №1 к настоящему приказу.
2. Ответственным за информационную безопасность в обособленных подразделениях и филиалах ФИЦ КНЦ СО РАН назначенных в соответствии с приказом от 15.09.2025г. № 119 а/х, а также руководителям структурных подразделений ФИЦ КНЦ СО РАН организовать внеплановую смену пользовательских паролей на АРМ под роспись в листе ознакомления (Приложению №2 к настоящему приказу). Скан копии листов ознакомления в срок не позднее 29.05.2026г. направить на электронный адрес infosec@ksc.krasn.ru.
3. Отделу кадров ФИЦ КНЦ СО РАН, включая кадровые службы обособленных подразделений и филиалов, при оформлении трудовых договоров включить актуальную версию Регламента эксплуатации автоматизированных рабочих мест в раздел ознакомления с локальными нормативными актами.
4. Возложить персональную ответственность за соблюдения требований Регламента, а также требований законодательства в области защиты информации на директоров обособленных подразделений и филиалов ФИЦ КНЦ СО РАН.
5. Инженеру отдела НТИ Ковальковой М.Б. довести настоящий приказ до руководителей филиалов, обособленных и структурных подразделений ФИЦ КНЦ СО РАН.
6. Заместителю начальника ИТЦ Вяткину В.П. обеспечить размещение приказа на официальном сайте ФИЦ КНЦ СО РАН.
7. Признать утратившим силу приложение №1 «Регламент эксплуатации автоматизированных рабочих мест работников ФИЦ КНЦ СО РАН» к приказу от 21.02.2024 №32а/х «О внесении изменений в Приказ от 14.07.2022 №90 а/х «Об утверждении нормативной документации ИТЦ ФИЦ КНЦ СО РАН»»

8. Контроль исполнения настоящего приказа возложить на заместителя директора по научной работе Варнакова С.Н.

Директор А.А. Шпедт

Лыткин Андрей Игоревич (Информационно-телекоммуникационный центр, Начальник отдела)
itc@ksc.krasn.ru
+7(391) 290-56-50

Приложение N 1

к приказу ФИЦ КНЦ СО РАН

от 10.04.2026 N 58 а/х

Регламент

эксплуатации автоматизированных рабочих мест работников ФИЦ КНЦ СО РАН

1. Общие положения

1.1. Настоящий Регламент эксплуатации автоматизированных рабочих мест работников ФИЦ КНЦ СО РАН (далее – Регламент) разработан с целью обеспечения единого подхода к организации использования в ФИЦ КНЦ СО РАН, в том числе в филиалах и обособленных подразделениях (далее - Центр), средств вычислительной техники, входящих в состав автоматизированных рабочих мест, и устанавливает правила организации автоматизированных рабочих мест и информационно-телекоммуникационной сети Центра и их использования работниками Центра.

1.2. Требования Регламента распространяются на работников всех подразделений Центра, использующих в работе средства вычислительной техники.

1.3. Термины и сокращения, используемые в настоящем Регламенте:

ПО – программное обеспечение.

Реестр ПО – электронный ресурс, содержащий перечень ПО, разрешенного для установки и использования на АРМ работников Центра, поддерживаемый ИТЦ в актуальном состоянии на основании информации о полученных Центром лицензиях и о свободно распространяемом ПО. Реестр ПО размещается в системе 1С «Документооборот».

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

ИС – информационная система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

Сеть Интернет – глобальная информационно-телекоммуникационная система, обеспечивающая удаленный доступ к ресурсам различного содержания и направленности.

IP-адрес – уникальный идентификатор устройства, подключенного к ИТС Центра.

Пользователь – в рамках документа – работник Центра, использующий средства вычислительной техники и сеть Интернет для выполнения своих должностных обязанностей;

Доступ к сети Интернет – физические, организационные, программные, правовые меры обеспечения доступа к ресурсам сети Интернет с использованием ИТС Центра.

ИТ, информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

АРМ, автоматизированное рабочее место – программно-аппаратный комплекс, предназначенный для выполнения работником операций в рабочих процессах на своем рабочем месте.

СВТ, средства вычислительной техники – совокупность программного, аппаратного, методического, технического обеспечений.

ИТЦ, Информационно-телекоммуникационный центр – структурное подразделение, обеспечивающее функционирование ИТ в Центре.

Подразделение ИТ – структурное подразделение или специалисты в области ИТ, выполняющие работы по обеспечению работоспособности средств вычислительной техники в соответствующем подразделении Центра.

2. Порядок эксплуатации АРМ

2.1. Порядок ввода в эксплуатацию и/или внесения изменений в состав и конфигурацию АРМ:

2.1.1. В состав АРМ может входить вычислительная техника, набор системного и прикладного ПО, и, при необходимости, вспомогательное периферийное оборудование (принтеры, сканеры, МФУ и прочее), инструкции по эксплуатации, методическая и техническая документация.

2.2. Решение о необходимости установки на рабочем месте работника АРМ и объеме предоставляемых пользовательских прав принимается руководителем структурного подразделения работника. При необходимости руководитель подразделения может запросить консультационную поддержку в Подразделении ИТ об имеющихся в наличии СВТ и их характеристиках.

2.2.1. Заявка об установке на рабочем месте работника АРМ направляется руководителем подразделения в Подразделение ИТ в виде служебной записки.

2.2.2. Специалист Подразделения ИТ устанавливает на рабочем месте работника АРМ, при необходимости вносит изменения в заявленную конфигурацию СВТ.

2.2.3. Перед установкой ПО специалист Подразделения ИТ должен убедится, что указанное в заявке ПО есть в Реестре ПО, и лицензионное соглашение (лицензия) допускает его использование в составе данного АРМ.

2.2.4. Специалист Подразделения ИТ до начала эксплуатации АРМ обязан установить антивирусное ПО и иное ПО, контролирующее безопасную эксплуатацию АРМ, а также ПО, позволяющее осуществлять удаленную диагностику.

2.2.5. Специалист Подразделения ИТ создает работнику учетные записи пользователя, под которыми он должен работать в ИТС Центра и в сети Интернет.

2.2.6. Специалист Подразделения ИТ передает СВТ под роспись работника и руководителя подразделения в служебной записке.

2.2.7. Руководитель подразделения знакомит Работника с правами и обязанностями и правилами пользования сетью Интернет, установленными настоящим Регламентом.

2.3. При переводе работника в другое подразделение или на другую должность, ином изменении трудовой функции руководитель структурного подразделения работника должен сообщить в Подразделение ИТ о необходимости внесении изменений в АРМ и учетные записи такого работника. Руководитель структурного подразделения работника по новому месту работы или при поручении работнику новой трудовой функции формирует соответствующее АРМ в порядке, установленном пунктом 2.2 настоящего Регламента.

2.4. При прекращении трудового договора работник должен сдать руководителю структурного подразделения все СВТ, предоставленные работнику в пользование для выполнения им трудовой функции. Подразделение ИТ прекращает доступ к СВТ, ИТС Центра, сети Интернет в конце последнего рабочего дня работника.

3. Участники процесса эксплуатации АРМ, их права и обязанности

3.1. Участниками процесса эксплуатации АРМ являются работник, непосредственный руководитель работника и специалисты Подразделений ИТ.

3.2. Права и обязанности работника:

3.2.1. Работник имеет право использовать установленное ему АРМ только для выполнения должностных обязанностей в соответствии с трудовым договором.

3.2.2. Работник обязан осуществлять работу в АРМ, передачу данных в ИТС Центра, сети Интернет и ИС только с использованием предоставленных ему Подразделением ИТ индивидуальных пользовательских идентификаторов и паролей (IP-адреса и учетных записей). Инструкция по парольной защите - прил. 1 к настоящему документу.

3.2.3. Работник не вправе самостоятельно устанавливать и/или удалять программные и/или аппаратные компоненты в составе закрепленного за ним АРМ и/или вносить изменения в его конфигурацию без согласования с Подразделением ИТ.

3.3. Руководитель подразделения вправе:

- формировать требования к перечню и конфигурации АРМ подчиненного работника;
- формировать заявку на закупку необходимых для работы компонентов АРМ (лицензии на ПО или аппаратного обеспечения) в установленном Центром порядке.

3.4. Устанавливать СВТ, вносить изменения в конфигурацию в процессе эксплуатации имеют право только специалисты Подразделений ИТ.

3.5. ИТЦ имеет право на постоянной основе с применением технических средств осуществлять удаленный контроль состояния АРМ в режиме реального времени. В случае сомнений в достоверности работы средств удаленного контроля специалист ИТЦ вправе осуществить очный аудит АРМ работника.

4. Правила пользования работниками сетью Интернет

4.1. Доступ к сети Интернет предоставляется работнику только для выполнения должностных обязанностей и служебных поручений непосредственного руководителя по трудовому договору. Доступ к сети Интернет в личных целях не разрешается.

4.2. При использовании сети Интернет работник обязан соблюдать следующие правила:

4.2.1. Передавать информацию посредством использования информационно-телекоммуникационных сетей с соблюдением требований и запретов, установленных Федеральным законодательством, организационно распорядительными документами и локальными нормативными актами ФИЦ КНЦ СО РАН.

4.2.2. не распространять в сети Интернет нежелательную информацию (спам, реклама и т.п.);

4.2.3. Не передавать другим лицам предоставленные ему индивидуальные IP-адреса и учетные записи и не использовать IP-адреса и учетные записи иных лиц для передачи данных в ИТС Центра и в сети Интернет;

4.2.4. При обнаружении попыток несанкционированного доступа или при подозрении на наличие вируса немедленно сообщать в Подразделение ИТ.

4.3. При работе с ресурсами сети Интернет работникам запрещается:

4.3.1. Использовать программные и аппаратные средства, запрещенные к использованию законодательством Российской Федерации;

4.3.2. Публиковать, загружать и распространять материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности компьютерного или телекоммуникационного оборудования;

4.4. Доступ к сети Интернет может быть ограничен без предварительного уведомления пользователей при возникновении нештатных ситуаций либо в целях соблюдения законодательства Российской Федерации.

5. Контроль за соблюдением Регламента

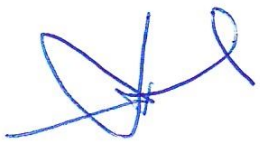
5.1. Контроль за соблюдением настоящего Регламента осуществляют Подразделения ИТ.

5.2.Нарушение требований, установленных настоящим Регламентом, работниками влечет за собой дисциплинарную ответственность, если мотивация, тяжесть и последствия нарушения не предусматривают согласно законодательству иной, более строгой ответственности.

5.3. Персональную ответственность за соблюдения требований Регламента несут директоры обособленных подразделений и филиалов ФИЦ КНЦ СО РАН.

5.4. Подразделение ИТ вправе ограничить работнику доступ к АРМ, сети Интернет в случае выявления нарушения работником настоящего Регламента до устранения нарушения.

РАЗРАБОТАНО:

Начальник ИТЦ  Д.В. Волков

Начальник отдела по технической поддержке ИТС ИТЦ  А.И. Лыткин

Главный специалист по сетевым и информационно-вычислительным сервисам ИТЦ  С.В. Исаев

Приложение 1

к регламенту эксплуатации
АРМ работников ФИЦ КНЦ СО РАН

Инструкция по парольной защите

Пароль – произвольный набор знаков, состоящий из букв, цифр и других символов, предназначенный для подтверждения личности пользователя для доступа к ИТС Центра, сети Интернет и ИС, обеспечивающий идентификацию и аутентификацию на основе сведений, известных только пользователю.

Предоставление паролей должно контролироваться посредством официальной процедуры, отвечающей следующим требованиям:

- при наличии возможности, необходимо настроить ИС таким образом, чтобы при первом входе пользователя с назначенным ему временным паролем система сразу же требовала его сменить;
- временные пароли должны назначаться пользователю только после его идентификации;
- необходимо избегать передачи паролей с использованием третьих лиц или по незащищенным каналам связи;
- временные пароли не должны быть угадываемыми и повторяющимися от пользователя к пользователю;
- пользователь должен подтвердить получение пароля;
- пароли должны храниться в электронном виде только в защищенной форме;
- назначенные производителем ПО пароли должны быть изменены сразу после завершения инсталляции;
- не реже одного раза в год пароль должен быть изменен.

В случае необходимости возможно использование других технологий идентификации и аутентификации пользователей, в частности, биометрических технологий, проверки подписи и аппаратных средств (смарт-карты, e-Token/ruToken, чипы и т.п.).

Личные пароли устанавливаются работниками самостоятельно, либо с привлечением специалистов Подразделения ИТ с учетом следующих требований:

- длина пароля должна быть не менее 15 символов;
- пароль должен содержать буквы верхнего и нижнего регистра, цифры и спецсимволы;
- пароль не должен содержать легко вычисляемые сочетания символов, таких как: имя, фамилия, номер телефона, дата рождения пользователя;
- последовательно расположенные на клавиатуре символы («12345678», «QWERTY», и т.д.);
- пароль не должен содержать общепринятые сокращения («USER», «TEST» и т.п.);

- для ИС находящимся под управлением разных организаций, необходимо устанавливать различные пароли, чтобы компрометация пароля в одной системе не влекла последствий для другой.

Запрещается вести запись паролей (например, на бумаге, в программном файле или в карманном устройстве), за исключением случаев, когда запись может храниться безопасно, а метод хранения был утверждён. Документы и носители с конфиденциальной информацией должны убираться в запираемые места (сейфы, шкафы и т.п.), особенно при уходе с рабочего места.

Вход пользователя в систему не должен выполняться автоматически, без ввода пароля. Оставляя рабочее место без присмотра, пользователь обязан заблокировать компьютер (используя комбинации Win + «L») или выйти из системы.

При использовании мобильных средств (например, ноутбуков, планшетов и мобильных телефонов) необходимо соблюдать дополнительные меры предосторожности, чтобы не допустить компрометацию информации, принадлежащей Центру.

Приложение N 2

к приказу ФИЦ КНЦ СО РАН

от 10.04.2026 N 58 а/х

Лист ознакомления

Подразделение:_____

№ п/п	ФИО работника	Должность	Дата ознакомления	Подпись работника	Дата смены пароля	Подпись работника