МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное
бюджетное учреждение науки
Федеральный исследовательский центр
«Коми научный центр Уральского отделения
Российской академии наук»
(ФИЦ Коми НЦ УрО РАН)

Институт геологии
имени академика Н.П. Юшкина
Коми научного центра Уральского отделения
Российской академии наук
(ИГ ФИЦ Коми НЦ УрО РАН)

РОССИЯСА НАУКА ДА ВЫЛЫС ВЕЛӧДЧАН МИНИСТЕРСТВО

«Россияса наукаяс академиялӧн
Урал юкӧнса Коми наука шӧринлӧн»
туялан удж нуӧдысь федеральнӧй шӧрин
Федеральнӧй канму
сьӧмкуд наука учреждение
(ТФШ РНА УрЮ Коми НШ)

Россияса наукаяс академиялӧн
Урал юкӧнса Коми наука шӧринлӧн
Академик Н.П. Юшкин нима
геология институт
(ТФШ РНА УрЮ Коми НШ ГИ)

ПРИКАЗ

15.05.2026 № 29

г. Сыктывкар

Об утверждении Политики по управлению паролями ИГ ФИЦ Коми НЦ УрО РАН

На основании докладной записки руководителя группа автоматизации научных исследований Рудницкого С.В.

ПРИКАЗЫВАЮ:

1. Утвердить Политику по управлению паролями ИГ ФИЦ Коми НЦ УрО РАН согласно Приложения к настоящему приказу.
2. Руководителям структурных подразделений ознакомить работников подчиненных подразделений ИГ ФИЦ Коми НЦ УрО РАН с настоящим приказом под подпись. Листы ознакомления направить в отдел кадров ИГ ФИЦ Коми НЦ УрО РАН.
3. Начальнику отдела кадров ИГ ФИЦ Коми НЦ УрО РАН обеспечить ознакомление вновь принимаемых на работу лиц с настоящим приказом под подпись.
4. Контроль за исполнением приказа оставляю за собой.

Врио директора С.К. Кузнецов

Приложение

УТВЕРЖДЕНО
приказом ИГ ФИЦ Коми НЦ УрО РАН
от 15.05.2026 г. № 29

Политика по управлению паролями Института геологии имени академика Н. П. Юшкина Коми научного центра Уральского отделения Российской академии наук Федерального государственного бюджетного учреждения науки Федерального исследовательского центра «Коми научный центр Уральского отделения Российской академии наук»

1. Общие положения

1.1. Настоящая Политика определяет требования к управлению паролями пользователей информационных систем (далее - ИС) и информационно-телекоммуникационной инфраструктуры (далее - ИТКС) ИГ ФИЦ Коми НЦ УрО РАН (далее – Институт).

1.2. Политика разработана в целях:

– обеспечения конфиденциальности, целостности и доступности информации;

– снижения рисков несанкционированного доступа к информационным системам;

– выполнения требований законодательства Российской Федерации в области защиты информации (в том числе персональных данных);

– реализации мер защиты информации, предусмотренных системой защиты информации Института.

1.3. Политика обязательна для исполнения всеми сотрудниками Института, использующими информационные системы, а также сторонними лицами, получившими доступ к информационным системам Института на договорной основе.

1.4. Контроль исполнения настоящей Политики возлагается на руководителя группы автоматизации (лицо, ответственное за обеспечение защиты информации) и руководителей структурных подразделений.

2. Область применения

Политика распространяется на все информационные системы и сервисы Института, использующие аутентификацию по паролю, включая, но не ограничиваясь:

– Доменные службы: Windows Server Domain (Active Directory), Samba Domain;

– Рабочие станции (ОС): Операционные системы рабочих мест сотрудников: Windows, Linux;

– Система электронного документооборота (СЭД): Directum;

– Почтовая инфраструктура: Корпоративная электронная почта *@geo.komisc.ru

– Веб-портал организации: Официальный сайт с личным кабинетом сотрудника geo.komisc.ru;

– Бухгалтерские и учетные системы: 1С: Предприятие (БД, серверы приложений);

– Средства криптографической защиты: Электронная подпись (ЭЦП), средства защиты информации (СКЗИ), используемые для шифрования и аутентификации;

Иные информационные системы: Видеоконференцсвязь, системы дистанционного обучения, виртуальные частные сети (VPN), системы удаленного доступа, специализированное научное ПО с парольной аутентификацией.

3. Требования к паролям пользователей

3.1. Основные требования

3.1.1. Каждый пользователь должен иметь уникальную учетную запись для доступа к информационным системам.

3.1.2. Запрещается использование групповых (общих) учетных записей. Исключение допускается только для административных учетных записей, используемых для обслуживания информационных систем и оборудования, при условии, что доступ к таким учетным записям имеют только уполномоченные администраторы.

3.1.3. Пароль должен быть известен только пользователю. Администраторам информационных систем запрещается требовать от пользователя сообщать свой пароль.

3.1.4. При первом входе в систему пользователь обязан изменить временный пароль, выданный администратором, на постоянный, удовлетворяющий требованиям настоящей Политики.

3.2. Требования к сложности пароля

Пароль пользователя должен соответствовать следующим требованиям:

– Минимальная длина не менее 8 символов

– Максимальная длина не более 64 символов (или максимально допустимая системой)

– Символы не менее трех из четырех категорий:

Прописные латинские буквы (A–Z);

Строчные латинские буквы (a–z);

Цифры (0–9);

Специальные символы (! @ # $ % ^ & * ( ) _ + ~ - = [ ] { } | ; : , . ? /)

– Запрещено использование слова «password», имени пользователя, имени организации, последовательных символов (qwerty, 12345) и других легко угадываемых комбинаций

– Непечатаемые символы не допускаются (например, Tab, Enter, Esc);

– Кириллица не допускается (только латиница).

3.3. Срок действия пароля и история

– Срок действия пароля: 90 дней (3 месяца)

– Упреждение о смене пароля: за 7 дней до истечения срока

– Запрет использования предыдущих паролей: не менее 8 предыдущих паролей не должны повторяться

– Минимальный срок действия пароля: 1 день (для предотвращения немедленной смены на тот же пароль через историю).

3.4. Блокировка учетной записи

– Количество неверных попыток входа: не более 5 последовательных неудачных попыток

– Длительность блокировки: не менее 15 минут (или до разблокировки администратором)

– Сброс счетчика неудачных попыток: через 15 минут после последней неудачной попытки.

4. Особенности управления паролями в различных системах

4.1. Доменные службы (Windows Server Domain, Samba Domain)

– Политика паролей реализуется централизованно через групповые политики (GPO) для Windows Domain и через параметры домена Samba.

– Пароли пользователей домена должны соответствовать требованиям раздела 3.

– Административное управление паролями осуществляется через штатные средства домена.

4.2. Система электронного документооборота (СЭД)

– При наличии интеграции с доменом (LDAP / Active Directory) используются доменные пароли.

– При отсутствии интеграции парольная политика СЭД настраивается на параметры, не менее строгие, чем указанные в разделе 3.

4.3. Почтовый сервер

– Пароли пользователей почтового сервера должны соответствовать требованиям раздела 3.

– Для веб-доступа к почте действуют общие требования к паролю и блокировке.

4.4. Сайт организации с личным кабинетом

– Личные кабинеты сотрудников на веб-портале должны использовать парольную политику, соответствующую разделу 3.

4.5. 1С: Предприятие

– Пароли пользователей 1С должны соответствовать требованиям раздела 3.

–Запрещается использование стандартных паролей для учетных записей администратора 1С.

4.6. Электронная подпись (ЭЦП)

– Пароль (PIN-код) от ключевого носителя должен быть не менее 6 символов и отвечать требованиям сложности.

– Запрещается передача ключевого носителя и PIN-кода третьим лицам.

4.7. Рабочие места сотрудников (Windows, Linux)

4.7.1. Общие требования

– Для входа в операционную систему сотрудник должен использовать учетную запись, подчиняющуюся требованиям настоящей Политики.

– При наличии доменной инфраструктуры (Windows Domain, Samba Domain) приоритетным является использование доменных учетных записей. Локальные учетные записи на рабочих станциях допускаются только в исключительных случаях (например, для компьютеров, не входящих в домен, или для локальных администраторов).

4.7.2. Windows (рабочие станции)

– Политика паролей для доменных учетных записей настраивается централизованно через Group Policy Object (GPO) и должна соответствовать требованиям раздела 3.

– Для локальных учетных записей (например, Administrator на компьютерах вне домена) требования к паролю настраиваются с использованием Local Group Policy (secpol.msc).

– Параметры блокировки учетной записи (5 неверных попыток, блокировка на 15 минут) также настраиваются через GPO или локальную политику безопасности.

– Запрещается отключение запроса пароля при выходе из режима сна или блокировки экрана. Автоматическая блокировка экрана должна наступать не позднее чем через 15 минут бездействия.

4.7.3. Linux (рабочие станции)

– При использовании Samba Domain или LDAP/SSSD парольная политика для доменных учетных записей настраивается централизованно на контроллере домена.

– Для локальных учетных записей требования к паролю задаются с использованием модуля PAM (Pluggable Authentication Modules).

– Параметры блокировки учетной записи настраиваются через PAM (pam_faillock). Рекомендуемые значения: 5 неудачных попыток, блокировка на 15 минут.

– Запрещается отключение блокировки экрана. Администратор обязан настроить автоматическую блокировку экрана при бездействии с порогом не более 15 минут.

5. Обязанности пользователей

Пользователь информационных систем Института обязан:

5.1. Использовать пароли, соответствующие требованиям настоящей Политики.

5.2. Незамедлительно сменить пароль при наличии подозрений, что пароль мог стать известен третьим лицам.

5.3. Не записывать пароль на бумажных носителях в открытом виде, не хранить пароли на рабочих столах, мониторах, в незащищенных файлах на компьютере.

5.4. Использовать индивидуальный пароль для личных учетных записей; запрещается сообщать пароль кому-либо, включая руководителей и администраторов.

5.5. Незамедлительно сообщать администратору информационной системы о фактах компрометации пароля или подозрительной активности с учетной записью.

5.6. По окончании работы блокировать рабочую станцию (клавиши Win + L) или выходить из всех информационных систем, если рабочее место остается без контроля пользователя.

6. Обязанности администраторов

Администраторы информационных систем обязаны:

6.1. Обеспечить техническую реализацию требований настоящей Политики в пределах компетенции (настройка групповых политик, параметров аутентификации систем, блокировки учетных записей).

6.2. Не использовать известные пароли пользователей для входа в системы под их учетными записями.

6.3. При необходимости смены пароля пользователя (по заявке или при утере пароля) установить временный пароль, удовлетворяющий требованиям сложности, и обеспечить его смену пользователем при первом входе.

6.4. Вести учет служебных (административных) учетных записей, использовать для них пароли повышенной сложности (не менее 15 символов).

6.5. Регулярно (не реже 1 раза в полугодие) проводить проверку учетных записей на наличие неиспользуемых (уволенных сотрудников, длительно неактивных) и своевременно их блокировать или удалять.

6.6. Обеспечить безопасное хранение паролей от административных учетных записей (с использованием менеджеров паролей с разграничением доступа или защищенных носителей).

7. Порядок действий при утере или компрометации пароля

Ситуация	Действия пользователя	Действия администратора
Забыли пароль	Обратиться к администратору системы с письменным заявлением (на бумажном носителе или через СЭД)	Сбросить пароль, установить временный пароль, обязать пользователя сменить его при первом входе
Подозрение на компрометацию	Немедленно сменить пароль самостоятельно. Если доступ утрачен – сообщить администратору	Заблокировать учетную запись до выяснения обстоятельств, помочь восстановить доступ
Увольнение сотрудника	Не применимо	Не позднее дня увольнения заблокировать (удалить) учетные записи во всех информационных системах

8. Использование двухфакторной аутентификации

8.1. Двухфакторная аутентификация (2FA)

Для систем, поддерживающих двухфакторную аутентификацию (почтовый сервер, VPN, личный кабинет на сайте, удаленный доступ), рекомендуется её использование.

При наличии технической возможности двухфакторная аутентификация является обязательной для:

– административных учетных записей;

– удаленного доступа к информационным системам организации (VPN, RDP через Интернет);

– доступа к информационным системам, содержащим персональные данные и иную охраняемую информацию.

9. Ответственность

9.1. Нарушение требований настоящей Политики влечет дисциплинарную, административную или иную ответственность в соответствии с законодательством Российской Федерации и локальными нормативными актами Института.

9.2. В случае инцидента (несанкционированного доступа, утечки информации), произошедшего по причине несоблюдения требований к парольной защите, виновные лица привлекаются к ответственности в установленном порядке.

10. Заключительные положения

10.1. Настоящая Политика вступает в силу с момента её утверждения приказом директора Института.

10.2. Изменения и дополнения в настоящую Политику вносятся на основании решения директора Института по представлению службы защиты информации.

10.3. Ознакомление сотрудников с Политикой производится под подпись (в том числе с использованием личных кабинетов или СЭД). Ответственность за ознакомление сотрудников возлагается на руководителей структурных подразделений.