



ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Отдел информационно-технического сопровождения

Политика парольной защиты

Утверждаю
И.о. ректора ФГБОУ ВО СГМУ
(г. Архангельск)
Минздрава России, к.м.н.,
Н. А. Былова



2026 г.

ПОЛИТИКА ПАРОЛЬНОЙ ЗАЩИТЫ
ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Версия 1.0

Дата введения: 30.09. 2026 г.

Архангельск
2026

	Должность	Фамилия/подпись	Дата
Разработал	Специалист по защите информации отдела ИТС	Чернышов С. Е.	25.09.2026
Проверил	Начальник управления правового и кадрового обеспечения	Сороченко Н.С.	28.09.2026
Согласовал	И.о проректора по цифровой трансформации	Яценко А. А.	28.09.2026



ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Отдел информационно-технического сопровождения

Политика парольной защиты

1. Рассмотрено на заседании Ученого совета, протокол № 1 от «28» 08 2026г.
2. Утверждено и введено в действие приказом и.о. ректора университета № 603 от «30» 09 2026г.
3. Соответствует требованиям вуза.



СОДЕРЖАНИЕ

1. Общие положения	4
2. Термины, определения, обозначения и сокращения	5
3. Цели и задачи	6
4. Требование к длине и сложности паролей	7
5. Периодичность и правила смены паролей	9
6. Хранение и передача паролей	10
7. Многофакторная аутентификация	12
8. Сервисные и привилегированные учётные записи	13
9. Ответственность	16
10. Заключительные положения	17
Приложение 1. Рекомендации по созданию надёжного пароля для пользователей	19
Приложение 2. Журнал учёта привилегированных учётных записей	20
Приложение 3. Журнал учёта сервисных учётных записей	21
Приложение 4. Лист ознакомления	22



1. Общие положения

1.1. Настоящая Политика парольной защиты (далее – Политика) устанавливает единые требования к созданию, использованию, хранению, передаче и смене паролей для доступа к информационным системам, информационным системам персональных данных (ИСПДн), автоматизированным рабочим местам, ресурсам локальной вычислительной сети и иным защищаемым информационным ресурсам федерального государственного бюджетного образовательного учреждения высшего образования «Северный государственный медицинский университет» Министерства здравоохранения Российской Федерации (далее – Университет).

1.2. Политика является локальным нормативным актом Университета, разработана в соответствии с действующим законодательством Российской Федерации и требованиями Федерального закона от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и экспортному контролю от 18.02.2013г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и экспортному контролю от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», и иных нормативных актов Российской Федерации в области информации, информационных технологий и защиты информации, в том числе локальных нормативных актов Университета.

1.3. Действие настоящей Политики распространяется на:

- всех сотрудников Университета (в том числе совместителей и временных работников);
- обучающихся (студентов, ординаторов, аспирантов, слушателей программ ДПО), имеющих доступ к информационным ресурсам Университета;



- внешних пользователей, допущенных к информационным системам Университета в установленном порядке;

- подрядные организации и их сотрудников, осуществляющих обслуживание информационных систем Университета;

- администраторов информационных систем и администратора безопасности.

1.4. Настоящая Политика является обязательным для исполнения локальным нормативным актом. Требования Политики подлежат безусловному выполнению всеми лицами, указанными в п. 1.3.

1.5. В случае противоречия между настоящей Политикой и иными локальными нормативными актами Университета в области защиты информации, применяются положения настоящей Политики.

2. Термины, определения и сокращения

В настоящей Политике используются следующие термины, определения и сокращения:

Аутентификация – процедура проверки подлинности пользователя или устройства на основе предоставленных идентификационных данных (пароля, токена, биометрического признака и т.п.).

Идентификатор (логин) – уникальная буквенно-числовая или символьная последовательность, позволяющая однозначно идентифицировать пользователя в информационной системе.

ИС – информационная система.

ИСПДн – информационная система персональных данных.

Компрометация пароля – событие, при котором пароль становится известен третьим лицам (несанкционированное разглашение, перехват, подбор, использование вредоносного ПО и т.п.).

Многофакторная аутентификация (MFA/2FA) – метод аутентификации, требующий предоставления двух и более независимых факторов подтверждения личности (знание – пароль; владение – токен, смарт-карта, мобильное устройство; встроенный признак – биометрия).



Пароль – секретная последовательность символов (букв, цифр, специальных знаков), используемая для подтверждения прав пользователя на доступ к информационной системе или ресурсу.

Парольная политика – совокупность правил, устанавливающих требования к созданию, использованию, хранению, смене и передаче паролей.

Пользователь – физическое лицо, допущенное к работе с информационной системой и использующее её ресурсы для выполнения служебных, учебных или иных правомерных задач.

Привилегированная учётная запись – учётная запись, предоставляющая пользователю повышенные права доступа (административные, супервизорские, системные) по сравнению с обычными пользователями.

Ротация паролей – процедура периодической смены пароля на новый в соответствии с установленными правилами.

Сервисная учётная запись – техническая учётная запись, используемая приложениями, службами, автоматизированными процессами и системными компонентами для выполнения своих функций без участия пользователя.

УЗ – уровень защищённости (для ИСПДн).

Учётная запись – совокупность данных о пользователе (идентификатор, пароль, права доступа, персональная информация), хранящаяся в информационной системе.

ФСТЭК России – Федеральная служба по техническому и экспортному контролю.

3. Задачи и цели

3.1. Основными целями настоящей Политики являются:

- обеспечение надёжной защиты информационных ресурсов Университета от несанкционированного доступа путём использования устойчивых к подбору паролей;
- минимизация рисков компрометации учётных записей пользователей;
- обеспечение соответствия требованиям законодательства Российской Федерации в области защиты информации и персональных данных;
- снижение вероятности успешных атак, связанных с подбором паролей (брутфорс, словарные атаки, фишинг);
- предотвращение несанкционированного доступа к персональным данным, сведениям, составляющим врачебную тайну, и иной конфиденциальной информации;



- формирование единых стандартов и правил работы с паролями для всех категорий пользователей.

3.2. Основными задачами Политики являются:

- установление минимальных требований к длине и сложности паролей;
- регламентация периодичности и правил смены паролей;
- определение порядка хранения и передачи паролей;
- внедрение многофакторной аутентификации для критичных информационных систем;
- регулирование порядка использования сервисных и привилегированных учётных записей;
- установление мер ответственности за нарушение требований Политики.

4. Требования к длине и сложности паролей

4.1. Минимальная длина пароля устанавливается в зависимости от класса ИС или уровня защищённости ИСПДн и категории пользователя.

Класс ИС / Уровень защищённости	Категория пользователей	Минимальная длина пароля
1-й класс / 1-й УЗ	Привилегированные учётные записи	Не менее 15 символов
1-й класс / 1-й УЗ	Обычные пользователи	Не менее 12 символов
2-й класс / 2-й УЗ	Привилегированные учётные записи	Не менее 12 символов
2-й класс / 2-й УЗ	Обычные пользователи	Не менее 10 символов
3-й, 4-й класс / 3-й, 4-й УЗ	Все категории	Не менее 8 символов
Сервисные учётные записи	-	Не менее 12 символов

4.2. Для всех категорий пользователей при создании пароля следует соблюдать следующие требования к сложности пароля:

- пароль должен содержать буквы в верхнем и нижнем регистре (A–Z, a–z);
- пароль должен содержать цифры (0–9);
- пароль должен содержать специальные символы из следующего набора: ! @ # \$ % ^ & * () _ + - = { } [] : ; < > , . ? / ~ | (использование пробелов не допускается).



4.3. Для всех категорий пользователей при создании паролей запрещается использование:

- словарных слов (в том числе на русском и английском языках, включая транслитерацию);
- личной информации пользователя (даты рождения, имена собственные, клички животных, номера телефонов, паспортные данные, адреса, названия организаций и т.п.);
- последовательных символов (12345, qwerty, abcde, йцукен и т.п.);
- одинаковых символов (aaaaaa, 111111, zzzzzz и т.п.);
- простых комбинаций, легко поддающихся подбору (admin, password, 123456, qwerty и т.п.);
- паролей, совпадающих с идентификатором пользователя.

4.4. Блокировка учётной записи пользователя производится после 3 последовательных неудачных попыток ввода пароля (для 1-го и 2-го класса ИС / УЗ) и после 5 неудачных попыток (для 3-го и 4-го класса ИС / УЗ).

Блокировка учётной записи пользователя осуществляется на 30 минут. По истечении указанного времени учётная запись автоматически разблокируется. При повторных блокировках администратор ИС (ИСПДн) проводит личную идентификацию пользователя и получает письменное объяснение о причинах, приведших к блокировке учётной записи.

4.5. Для снижения вероятности успешных атак, связанных с подбором паролей учётной записи должны быть выполнены следующие настройки истории паролей:

- запрещается повторное использование последних 5 паролей (для систем 1-го и 2-го класса ИС / УЗ);
- запрещается повторное использование последних 3 паролей (для систем 3-го и 4-го класса ИС / УЗ).

4.6. При наличии технической возможности организовать проверку пароля на уязвимость, т.е. при создании или смене пароля должна осуществляться автоматическая его проверка на наличие в общедоступных базах скомпрометированных паролей. В случае обнаружения пароля в таких базах система проверки должна отклонить его и предложить пользователю выбрать другой пароль.

4.7. В целях недопущения несанкционированного доступа для всех информационных систем устанавливается автоматическая блокировка сессии пользователя при бездействии в течение 15 минут. Возобновление работы возможно только после



повторной аутентификации. Для 1-го и 2-го классов ИС / УЗ время бездействия не должно превышать 10 минут.

5. Периодичность и правила смены паролей

5.1. Периодичность смены паролей зависит от типа учетной записи и класса ИС или уровня защищённости ИСПДн.

Тип учётной записи	Срок действия пароля
Обычные учётные записи пользователей (1-й и 2-й класс ИС / 1-й и 2-й УЗ)	Не более 60 календарных дней
Обычные учётные записи пользователей (3-й и 4-й класс ИС / 3-й и 4-й УЗ)	Не более 90 календарных дней
Привилегированные учётные записи (все классы ИС / все УЗ)	Не более 60 календарных дней
Сервисные учётные записи	В соответствии с п.8.3.3. настоящей Политики

5.2. Минимальный срок действия пароля 1 день после предыдущей смены (за исключением случаев принудительного сброса администратором ИС (ИСПДн) при компрометации пароля). Пользователь не может самостоятельно провести смену пароля ранее чем через 1 день после предыдущей смены

5.3. Обязательная смена пароля производится:

- при первом входе пользователя в систему после получения учётной записи;
- по истечении установленного срока действия пароля;
- при подозрении на компрометацию учётной записи (в том числе по требованию администратора безопасности или администратором ИС (ИСПДн));
- по требованию администратора безопасности или администратора ИС (ИСПДн) в рамках проведения плановых мероприятий.

5.4. Порядок смены пароля:

- смена пароля производится только через штатные средства информационной системы (интерфейс смены пароля, диалог входа в систему с принудительной сменой);
- пользователь должен самостоятельно инициировать смену пароля по истечении срока его действия (информационная система должна напоминать об истечении срока не менее чем за 14 дней до окончания срока действия);



- при смене пароля информационная система должна проверять его на соответствие требованиям длины, сложности и истории.

5.5. Пользователю запрещается:

- передача пароля третьим лицам для смены пароля;
- смена пароля с использованием нештатных средств и/или утилит, не включенных в состав информационной системы;
- установка пароля, полученного от администратора или другого лица, без его немедленной смены.

6. Хранение и передача паролей

6.1. В используемых информационных системах при организации хранения паролей должны выполняться следующие требования:

- пароли хранятся в зашифрованном виде с использованием криптографических алгоритмов, обеспечивающих невозможность восстановления исходного пароля (хэширование с «солью»);
- в качестве алгоритмов хэширования используются SHA-256, SHA-3 или более стойкие алгоритмы.

Запрещается передача паролей по открытым каналам связи без использования средств криптографической защиты (SSL/TLS, IPsec и т.п.).

6.2. Во избежание компрометации пароля и создания предпосылок для несанкционированного доступа к информационным системам пользователям запрещается:

- записывать пароли на бумажных носителях, стикерах, в открытых файлах без защиты;
- сообщать пароли по телефону, в сообщениях электронной почты, мессенджерах, социальных сетях;
- хранить пароли в открытом виде на рабочей станции, в электронной почте, мессенджерах, облачных хранилищах;
- использовать менеджеры паролей, не прошедшие сертификацию или не включённые в реестр отечественного ПО;
- хранить пароли в браузере без использования мастер-пароля.
- передавать свои пароли третьим лицам (включая коллег, руководителей, администраторов, техническую поддержку);



- передавать пароли через открытые каналы связи;
- использовать один и тот же пароль для доступа к различным системам и ресурсам.

6.3. В случае компрометации пароля учетной записи информационной системы выполняются следующие процедуры:

Пользователь	- сменить скомпрометированный пароль - уведомить непосредственного руководителя о факте компрометации пароля - прекратить обработку данных с использованием скомпрометированной учетной записью
Руководитель структурного подразделения	- уведомить ответственного за защиту информации и администратора ИС/ИСПДн
Ответственный за защиту информации совместно с администратором ИС/ИСПДн	- заблокировать скомпрометированную учётную запись до выяснения обстоятельств - инициировать проверку журналов аудита для сбора первичной информации об инциденте и выявления несанкционированных действий - составить справку об инциденте
Ответственный за защиту информации	- уведомить руководителя структурного подразделения ответственного за организацию защиты информации
Ответственный за защиту информации по согласованию с руководителем структурного подразделения	- принять решение о блокировке доступа к персональным данным при наличии фактов несанкционированного доступа
Руководитель структурного подразделения ответственного за организацию защиты информации	- эскалация инцидента (при высоком уровне критичности)
Руководитель структурного подразделения ответственного за организацию защиты информации	- уведомить ректора Университета
Ректор, комиссия по расследованию инцидентов информационной безопасности	- подготовить уведомления в Роскомнадзор и ГосСОПКА
Ответственный за защиту информации	- подать уведомления в Роскомнадзор и ГосСОПКА

6.4. При взаимодействии с пользователями администратору информационных систем и администратору безопасности запрещается запрашивать пароли пользователей. В случае необходимости смены пароля учетной записи пользователя (при утере, блокировке, подозрении на компрометацию) администратор инициирует процедуру сброса пароля через штатные средства системы с установленным параметром смены пароля пользователем при первом входе.

После сброса пароля пользователь обязан сменить пароль при первом входе.



7. Многофакторная аутентификация

7.1. Использование многофакторной аутентификации (MFA) является дополнительной защитой учетной записи и при наличии технической возможности должна применяться для следующих категорий учётных записей и информационных систем:

- все привилегированные учётные записи (независимо от уровня защищённости системы);
- системы 1-го и 2-го класса ИС / уровня защищённости (для всех пользователей);
- информационные системы, содержащие персональные данные, сведения, составляющие врачебную тайну, и иную конфиденциальную информацию;
- удалённый доступ к информационным ресурсам Университета (VPN, веб-порталы, системы дистанционного обучения с доступом к персональным данным);
- доступ к системам служебной электронной почты и служебным коммуникационным сервисам.

7.2. Применяемые факторы аутентификации разделяются на три категории и используются в следующем порядке:

1. Первый фактор:

- пароль;
- PIN-код;
- ответ на секретный вопрос.

2. Второй фактор:

- код TOTP (Time-based One-Time Password) – одноразовый код, генерируемый мобильным приложением;
- аппаратный токен или смарт-карта;
- SMS-сообщение с одноразовым кодом.

3. Биометрия (встроенный признак):

- отпечаток пальца;
- сканер лица;
- радужная оболочка глаза.

При многофакторной аутентификации предпочтительным методом второго фактора является TOTP (одноразовый код, генерируемый мобильным приложением). Использование SMS-сообщений допускается только при отсутствии технической возможности применения более надёжных методов.



Использование биометрических данных для аутентификации может быть разрешено только при условии, что это прямо допускается локальными нормативными актами Университета и не противоречит требованиям законодательства Российской Федерации в области обработки биометрических персональных данных.

7.3. При использовании многофакторной аутентификации должны выполняться следующие требования:

- использование второго фактора обязательно при каждом входе в систему (для систем 1-го класса ИС / УЗ) или при входе с нового устройства/из новой сети (для систем 2-го класса ИС / УЗ);
- допустимое время действия одноразового кода – не более 60 секунд;
- запрещается использование одного и того же одноразового кода более одного раза;
- при утере или смене устройства, используемого для генерации одноразовых кодов, пользователь обязан немедленно уведомить администратора для перенастройки многофакторной аутентификации.

7.4. Подключение многофакторной аутентификации пользователям производится администратором информационной системы или администратором безопасности.

Перед использованием многофакторной аутентификации пользователи должны пройти инструктаж и понять порядок действий.

В качестве резервного метода аутентификации для восстановления доступа, если основной способ подтверждения (TOTP или SMS) временно недоступен, допускается использование одноразовых резервных кодов (backup codes), которые пользователь обязан хранить в безопасном месте.

7.5. В случае допуска к информационной системе Университета для выполнения работ в рамках договора (государственного контракта) внешних пользователей или сотрудников подрядных организаций использование многофакторной аутентификации является обязательным.

Ответственность за обеспечение многофакторной аутентификации для внешних пользователей или сотрудников подрядных организаций возлагается на администратора соответствующей информационной системы.

8. Сервисные и привилегированные учётные записи



8.1. Привилегированными являются учётные записи, предоставляющие пользователю права, превышающие права обычных пользователей (администраторы, супервизоры, системные администраторы, администраторы баз данных, администраторы безопасности и т.п.).

Привилегированные учётные записи должны соответствовать следующим требованиям:

- срок действия пароля не более 60 календарных дней;
- минимальная длина пароля – не менее 12 символов (для систем 1-го и 2-го класса ИС / УЗ – не менее 15 символов);
- использование многофакторной аутентификации (при наличии технической возможности);
- запрет на использование привилегированных учётных записей для выполнения повседневных задач (вход должен осуществляться только при необходимости выполнения административных действий);
- обязательное ведение журнала аудита действий, выполненных с использованием привилегированных учётных записей.
- ведение отдельного реестра (журнала) привилегированных учётных записей.

В реестре (журнале) привилегированных учётных записей должны указываться следующие данные:

- идентификатор учётной записи;
- полное имя пользователя;
- должность/роль;
- перечень систем, к которым предоставлены права;
- дата создания и дата последней смены пароля;
- срок действия пароля;
- отметка о блокировке, изменении прав доступа;

8.2. Сервисные учётные записи используются приложениями, службами и автоматизированными процессами для взаимодействия между системами и компонентами.

Сервисные учётные записи должны соответствовать следующим требованиям:

- пароли должны быть уникальными для каждой сервисной учётной записи;
- минимальная длина пароля – не менее 12 символов;
- пароли должны соответствовать требованиям сложности (п. 4.2);



- пароли должны храниться в зашифрованном виде с использованием средств криптографической защиты;
- рекомендуется автоматическая ротация паролей сервисных учётных записей с периодичностью не более 60 календарных дней (при технической возможности);
- доступ к сервисным учётным записям ограничивается минимально необходимым кругом лиц (не более 2–3 сотрудников для каждой учётной записи);
- ведение отдельного реестра сервисных учётных записей.

В реестре (журнале) сервисных учётных записей должны указываться следующие данные:

- идентификатор учётной записи;
- назначение (для каких приложений/служб используется);
- ответственное лицо (владельца);
- дата создания и дата последней смены пароля;
- срок действия пароля;
- перечень лиц, имеющих доступ к учётной записи.

8.3. При работе с привилегированными и сервисными учётными записями запрещается:

- использование одной учётной записи несколькими пользователями (исключение – привилегированные учётные записи, используемые в рамках одной административной группы, с обязательным ведением индивидуальных сессий и аудита);
- использование сервисных учётных записей для интерактивного входа пользователей;
- использование одной сервисной учётной записи для нескольких приложений или служб (каждое приложение должно иметь собственную учётную запись);
- хранение паролей сервисных учётных записей в открытом виде в скриптах, конфигурационных файлах, репозиториях кода, документации;
- использование сервисных учётных записей с истекшим сроком действия пароля;
- передача паролей сервисных учётных записей третьим лицам без оформления соответствующего разрешения.

8.4. Привилегированные и сервисные учётные записи подлежат регулярной проверке на предмет необходимости их существования (не реже одного раза в квартал). Неиспользуемые учётные записи подлежат блокировке и последующему удалению.



8.5. Периодичность смены паролей сервисных учётных записей:

- при наличии технической возможности – автоматическая ротация не реже 1 раза в 60 дней;
- при отсутствии технической возможности – ручная смена не реже 1 раза в 60 дней с обязательной фиксацией в реестре сервисных учётных записей.

8.6. Ответственность за создание, учёт и контроль использования сервисных и привилегированных учётных записей возлагается на администратора соответствующей информационной системы и администратора безопасности.

9. Ответственность за нарушение

9.1. За нарушение требований настоящей Политики пользователи несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации и локальными нормативными актами Университета.

9.2. Ответственность пользователей:

- пользователи несут персональную ответственность за сохранность своих аутентификационных данных (идентификатора и пароля);
- пользователи несут ответственность за все действия, совершённые с использованием их учётной записи, включая случаи передачи пароля третьим лицам;
- пользователи обязаны немедленно уведомлять администратора безопасности о фактах компрометации учётной записи;
- за разглашение паролей, передачу их третьим лицам, использование чужих учётных записей, в зависимости от тяжести наступивших последствий и нанесённого ущерба, пользователь может быть привлечён к дисциплинарной ответственности вплоть до увольнения (для сотрудников) или отчисления (для обучающихся).

9.3. Администратор информационных систем и администратор безопасности несут ответственность за выполнение следующих требований:

- своевременное доведение требований Политики до пользователей;
- техническая реализация парольной политики в информационных системах;
- контроль соблюдения требований Политики;
- своевременное реагирование на инциденты, связанные с компрометацией учётных записей;



- ведение реестров (журналов) привилегированных и сервисных учётных записей;
- обеспечение многофакторной аутентификации для соответствующих категорий систем и пользователей (при наличии технической возможности).

9.4. Руководители структурных подразделений несут ответственность:

- за организацию ознакомления подчинённых сотрудников с требованиями настоящей Политики и контроль их соблюдения;
- за принятие мер дисциплинарного воздействия к сотрудникам, допустившим нарушения требований Политики.

9.5. Сотрудники подрядных организаций, допущенные к информационным системам Университета, несут ответственность за нарушение требований настоящей Политики в соответствии с заключёнными договорами (государственными контрактами) и законодательством Российской Федерации.

9.6. Нарушение требований Политики, повлёкшее утрату или компрометацию персональных данных, сведений, составляющих врачебную тайну, или иной защищаемой информации, является основанием для применения мер ответственности в соответствии с законодательством Российской Федерации.

10. Заключительные положения

10.1. Настоящая Политика вступает в силу с момента её утверждения ректором Университета.

10.2. Все сотрудники Университета, обучающиеся и иные лица, имеющие доступ к информационным системам и ресурсам локальной вычислительной сети Университета, должны быть ознакомлены с настоящей Политикой под роспись. Ознакомление проводится:

- при приёме на работу (зачислении) – для сотрудников и обучающихся;
- при предоставлении доступа к информационным системам – для внешних пользователей;
- при каждом пересмотре документа и внесении изменений – для всех категорий пользователей.

10.3. Пересмотр настоящей Политики осуществляется:

- по мере необходимости, но не реже одного раза в год;



- при изменении законодательства Российской Федерации в области защиты информации;
- при изменении внутренних нормативных актов Университета в области защиты информации;
- по результатам проверок контролирующих органов;
- по результатам анализа инцидентов информационной безопасности, связанных с компрометацией учётных записей.

10.4. Изменения и дополнения в Политику вносятся по представлению:

- проректора по цифровой трансформации;
- администратора безопасности информационных систем;
- администратора информационных систем;
- ответственного за защиту информации.

Изменения и дополнения утверждаются ректором Университета.

10.5. Подлинный экземпляр настоящей Политики хранится в структурном подразделении, ответственном за организацию защиты информации. Электронная версия Политики размещается на официальном сайте Университета в информационно-телекоммуникационной сети Интернет и в системе электронного документооборота Университета.

10.6. Вопросы, не урегулированные настоящей Политикой, решаются в соответствии с действующим законодательством Российской Федерации и иными локальными нормативными актами Университета.



ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Отдел информационно-технического сопровождения

Политика парольной защиты

Приложение № 1

Рекомендации по созданию надёжного пароля для пользователей

№ п/п	Рекомендация	Пример
1	Используйте длину не менее 12 символов	SGMU5678_NoDanger!
2	Включайте буквы верхнего и нижнего регистра	YaLubluSGMU#26!
3	Добавляйте цифры и специальные символы	Med!c@ISGMU#2026
4	Используйте фразу из нескольких слов	Zdorovie@SGMU_21%
5	Избегайте личной информации	Не использовать даты рождения, имена, номера телефонов
6	Используйте разные пароли для разных систем.	Для каждой системы – свой уникальный пароль
7	Используйте менеджер паролей (при наличии разрешения)	Храните все пароли в защищённом хранилище



ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Отдел информационно-технического сопровождения

Политика парольной защиты

Приложение № 2

Журнал учёта привилегированных учётных записей

№ п/п	Идентификатор учётной записи	ФИО пользователя	Должность/Роль	Системы (доступ)
1	2	3	4	5
1	admin_sidorov	Сидоров И.И.	Администратор ИС	Ариадна, Брегис

Дата создания	Дата последней смены пароля	Срок действия (до)	Примечание
6	7	8	9
01.01.2026	01.01.2026	01.03.2026	MFA включена



ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Отдел информационно-технического сопровождения

Политика парольной защиты

Приложение № 3

Журнал учёта сервисных учётных записей

№ п/п	Идентификатор учётной записи	Назначение	Ответственный (владелец)	Дата создания
1	2	3	4	5
1	svc_backup	Резервное копирование БД	Петров П.П.	01.01.2026

Дата последней смены пароля	Срок действия (до)	Лица, имеющие доступ	Примечание
6	7	8	9
01.01.2026	01.04.2026	Иванов И.И., Сидоров С.С.	Автоматическая ротация



ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Отдел информационно-технического сопровождения

Политика парольной защиты

Приложение 4

Лист ознакомления

Настоящим подтверждаю, что ознакомлен(а) с Политикой парольной защиты ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России и обязуюсь соблюдать её требования.

№ п/п	Фамилия, имя, отчество	Должность/ статус	Подпись	Дата
1	Иванова И. И.	Доцент кафедры гуманитарных наук	Иванова	01.01.2026
2	Сидоров С. С.	Заведующий службой	Сидоров	02.02.2026
3	Петров П. П.	Обучающийся лечебного факультета	Петров	01.09.2026