



ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Отдел информационно-технического сопровождения

Инструкция пользователя локальной вычислительной сети

Утверждаю

И.о. ректора ФГБОУ ВО СГМУ

(г. Архангельск)

Минздрава России, к.м.н.,

Н. А. Былова



2026 г.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

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.	29.09.2026



ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Отдел информационно-технического сопровождения

Инструкция пользователя локальной вычислительной сети

1. Рассмотрено на заседании Ученого совета, протокол № 1 от «28» 08 2026г.
2. Утверждено и введено в действие приказом и.о. ректора университета № 602 от «30» 09 2026г.
3. Соответствует требованиям вуза.



СОДЕРЖАНИЕ

1. Общие положения	4
2. Порядок получения доступа	4
3. Права пользователя	5
4. Обязанности пользователя	5
5. Пользователю запрещается	6
6. Правило работы с паролями	6
7. Правила использования ресурсов ЛВС	7
8. Порядок действий при сбоях и инцидентах	9
9. Ответственность	9
10. Заключительные положения	10
Приложение 1. Памятка для пользователей по созданию надёжного пароля	11
Приложение 2. Лист ознакомления	12



1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с Положением о локальной вычислительной сети и Политикой парольной защиты федерального государственного бюджетного образовательного учреждения высшего образования «Северный государственный медицинский университет» Министерства здравоохранения Российской Федерации (далее – Университет) и определяет порядок действий, права, обязанности и ответственность пользователей при работе в локальной вычислительной сети (далее – ЛВС) Университета.

1.2. Инструкция является обязательной для исполнения всеми сотрудниками Университета, обучающимися, а также иными лицами, допущенными к ресурсам ЛВС в установленном порядке.

1.3. Под пользователем ЛВС понимается любое физическое лицо, использующее ресурсы ЛВС для выполнения трудовых, учебных или иных правомерных задач.

1.4. Пользователь допускается к работе в ЛВС только после ознакомления под подпись с настоящей Инструкцией, Положением о ЛВС и Политикой парольной защиты.

2. Порядок получения доступа

2.1. Доступ к ресурсам ЛВС предоставляется на основании письменной заявки, подписанной руководителем структурного подразделения (для сотрудников) или представителем деканата (для обучающихся).

2.2. В заявке указываются:

- фамилия, имя, отчество пользователя;
- должность, структурное подразделение, номер кабинета (для сотрудников) или группа и курс (для обучающихся);
- перечень ресурсов ЛВС и информационных систем, необходимых для исполнения должностных обязанностей или выполнения учебных задач.

2.3. На основании заявки администратор ЛВС создает учетную запись пользователя, назначает права доступа в соответствии с должностными обязанностями (принцип минимальной достаточности) и выдает идентификационные данные (логин и пароль).

2.4. Регистрация пользователя в ЛВС производится в срок, не превышающий 3 рабочих дней с момента подачи заявки.



2.5. При первом входе в систему пользователь обязан сменить пароль, выданный администратором, на собственный, соответствующий требованиям Политики парольной защиты.

2.6. Пользователь имеет право работать в ЛВС только под своей учетной записью и только на тех компьютерах, доступ к которым ему разрешен.

3. Права пользователя

3.1. Пользователь ЛВС имеет право:

- использовать сервисы и ресурсы ЛВС, предоставленные ему для выполнения служебных обязанностей или учебных задач;
- получать от администратора ЛВС консультационную поддержку по вопросам работы с сервисами и ресурсами ЛВС;
- обращаться к администратору ЛВС с заявками на подключение нового оборудования, изменение прав доступа к сервисам и ресурсам с обоснованием служебной или учебной необходимости;
- запрашивать у администратора ЛВС информацию о плановых профилактических работах и перерывах в работе сети.

4. Обязанности пользователя

4.1. Пользователь ЛВС обязан:

- соблюдать требования настоящей Инструкции, Положения о ЛВС и Политики парольной защиты;
- использовать сервисы и ресурсы ЛВС исключительно для служебных или учебных целей;
- содержать в тайне личные аутентификационные данные (логин и пароль);
- немедленно уведомлять администратора ЛВС о фактах компрометации учетной записи или подозрительной активности;
- не реже одного раза в 60 дней (для информационных систем 1-го и 2-го класса/уровня защищённости) производить смену пароля в установленном порядке;
- не реже 90 дней (для информационных систем 3-го и 4-го класса/уровня защищённости) производить смену пароля в установленном порядке;



- своевременно (не позднее дня увольнения или отчисления) уведомлять администратора ЛВС о прекращении трудовых или учебных отношений;
- бережно относиться к оборудованию ЛВС, не производить его самостоятельное перемещение и перекоммутацию;
- сообщать администратору ЛВС обо всех сбоях, некорректной работе сети и её компонентов;
- соблюдать правила антивирусной безопасности, не отключать установленные администратором защитные средства.

5. Пользователю запрещается

5.1. Пользователю ЛВС запрещается:

- предпринимать попытки несанкционированного доступа к ресурсам ЛВС, к которым ему не предоставлены права;
- передавать свои аутентификационные данные третьим лицам или использовать чужие учетные записи;
- устанавливать на рабочую станцию нелегальное, вредоносное или неразрешенное программное обеспечение;
- самостоятельно изменять конфигурацию операционной системы и сетевые настройки рабочей станции;
- использовать сетевое оборудование и информационные ресурсы для совершения действий, противоречащих законодательству Российской Федерации;
- осуществлять запуск сетевых сканеров, анализаторов трафика, программ подбора паролей и иных средств, способных нарушить стабильность работы ЛВС;
- распространять информацию, порочащую честь и деловую репутацию граждан и организаций, а также материалы оскорбительного или экстремистского содержания;
- самостоятельно подключать к ЛВС любое оборудование без согласования с администратором;
- отключать или обходить установленные средства защиты информации (антивирус, межсетевой экран и др.).

6. Правила работы с паролями

6.1. Требования к паролю:



- длина пароля – не менее 12 символов (для привилегированных учетных записей – не менее 15 символов);

- пароль должен содержать буквы в верхнем и нижнем регистре, цифры и специальные символы (! @ # \$ % ^ & * () _ + - = { } [] : ; < > , . ? / ~ |);

- запрещается использовать словарные слова, личную информацию (даты рождения, имена, номера телефонов), последовательные символы (12345, qwerty), одинаковые символы (aaaaaa), пароли, совпадающие с идентификатором.

6.2. Порядок смены пароля пользователем:

- смена пароля производится только через штатные средства информационной системы;

- при смене пароля система автоматически проверяет его на соответствие требованиям длины, сложности и истории (запрещено повторное использование последних 5 паролей);

- запрещается передавать пароль третьим лицам для смены пароля;

- запрещается использовать нештатные средства и утилиты для смены пароля.

6.3. Хранение и передача паролей пользователем:

- запрещается записывать пароли на бумажных носителях, стикерах, в открытых файлах;

- запрещается сообщать пароли по телефону, в электронной почте, мессенджерах, социальных сетях;

- запрещается хранить пароли в открытом виде на рабочей станции, в облачных хранилищах;

- запрещается использовать один и тот же пароль для доступа к различным системам и ресурсам.

6.4. Действия пользователя при компрометации пароля:

- немедленно сменить скомпрометированный пароль;

- уведомить непосредственного руководителя и администратора ЛВС о факте компрометации;

- прекратить обработку данных с использованием скомпрометированной учетной записи.

7. Правила использования ресурсов ЛВС



7.1. Доступ в сеть Интернет предоставляется пользователям исключительно для решения служебных или учебных задач. Потоки данных, не связанные с основной деятельностью Университета (просмотр развлекательных сайтов, загрузка мультимедийного контента неслужебного характера, сетевые игры), могут быть ограничены или запрещены.

7.2. Пользователи могут пользоваться подключением к беспроводным сетям Университета.

Подключение к служебной беспроводной сети производится с использованием протоколов шифрования не ниже WPA2-Enterprise с аутентификацией через каталог пользователей.

Пользователям запрещается создание несанкционированных точек доступа и подключение личных устройств к служебной беспроводной сети. Личные устройства подключаются к служебной беспроводной сети только при наличии отдельного разрешения руководства Университета.

Подключение к гостевой беспроводной сети для доступа к сети Интернет возможно посетителям (гостям) Университета. Доступ к гостевой беспроводной сети предоставляется исключительно после идентификации и аутентификации через ЕСИА. Срок сессии гостевого доступа не может превышать 24 часа. В случае недоступности ЕСИА доступ к гостевой сети не предоставляется.

7.3. Удаленный доступ пользователей к ресурсам ЛВС предоставляется только при использовании сертифицированных СКЗИ и многофакторной аутентификации. Удаленный доступ предоставляется на основании отдельной заявки сроком не более 3 месяцев.

7.4. Служебная электронная почта:

- используется только для служебной переписки;
- запрещается использовать служебную почту для регистрации на сторонних ресурсах, рассылки спама, передачи вредоносных файлов и конфиденциальной информации (персональных данных, врачебной тайны).

7.5. Программное обеспечение:

- использование ПО, не входящего в утвержденный перечень разрешенного ПО, запрещается;
- установка дополнительного ПО производится только по согласованию с проректором по цифровой трансформации.



8. Порядок действий при сбоях и инцидентах

8.1. При обнаружении сбоев, некорректной работы сети или её компонентов пользователь обязан:

- немедленно прекратить работу, способную усугубить ситуацию;
- сообщить о проблеме администратору ЛВС с указанием времени, характера сбоя и своих действий.

8.2. При обнаружении инцидента информационной безопасности (подозрение на несанкционированный доступ, вирусная активность, компрометация учетной записи) пользователь обязан действовать в соответствии с утверждённым в Университете «Порядком реагирования на инциденты информационной безопасности:

- незамедлительно сообщить о случившемся ответственному за защиту информации и администратору ЛВС;
- прекратить любые действия до получения инструкций;
- не предпринимать самостоятельных действий по устранению инцидента (не перезагружать компьютер, не удалять файлы).

8.3. При обнаружении на территории Университета утерянного или оставленного без присмотра мобильного устройства, ноутбука, нетбука, пользователь обязан немедленно уведомить охрану на ближайшем к месту обнаружения посту охраны.

9. Ответственность

9.1. За нарушение требований настоящей Инструкции, Положения о ЛВС и Политики парольной защиты пользователи несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

9.2. Пользователь несет персональную ответственность за сохранность своих аутентификационных данных и за все действия, совершённые с использованием его учётной записи, включая случаи передачи пароля третьим лицам.

9.3. За разглашение паролей, передачу их третьим лицам или использование чужих учётных записей пользователь может быть привлечён к дисциплинарной ответственности вплоть до увольнения (для сотрудников) или отчисления (для обучающихся).

9.4. Нарушение требований Инструкции, повлёкшее утрату или компрометацию персональных данных, сведений, составляющих врачебную тайну, или иной защищаемой



ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Отдел информационно-технического сопровождения

Инструкция пользователя локальной вычислительной сети

информации, является основанием для применения мер ответственности в соответствии с законодательством Российской Федерации.

10. Заключительные положения

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

10.2. Все сотрудники Университета, обучающиеся и иные лица, имеющие доступ к ресурсам ЛВС, должны быть ознакомлены с настоящей Инструкцией под подпись (Приложение 2). Ознакомление проводится при приёме на работу (зачислении) или при предоставлении доступа к ЛВС.

10.3. Изменения и дополнения в Инструкцию вносятся по мере необходимости и утверждаются ректором Университета по представлению проректора по цифровой трансформации.

10.4. Подлинный экземпляр Инструкции хранится в Службе делопроизводства и контроля документооборота Университета. Электронная версия размещается на официальном сайте Университета.

	ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России
	Отдел информационно-технического сопровождения
	Инструкция пользователя локальной вычислительной сети

Приложение 1

Памятка для пользователей по созданию надёжного пароля

№ 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@lSGMU#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

Инструкция пользователя локальной вычислительной сети

Приложение 2

Лист ознакомления

Настоящим подтверждаю, что ознакомлен(а) с Инструкцией пользователя ЛВС ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России и обязуюсь соблюдать её требования.

№ п/п	Фамилия, имя, отчество	Должность/статус	Подпись	Дата
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				