



ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Отдел информационно-технического сопровождения

Положение о локальной вычислительной сети

Утверждаю

И.о. ректора ФГБОУ ВО СГМУ

(г. Архангельск)

Минздрава России, к.м.н.,

Н. А. Былова



«30» сентября

2026 г.

ПОЛОЖЕНИЕ О ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Версия 3.0

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 И. Г.	28.09.2026
Согласовал	И.о проректора по цифровой трансформации	Яценко А. А.	25.09.2026



ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Отдел информационно-технического сопровождения

Положение о 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. Термины и определения	5
3. Цели и задачи локальной вычислительной сети	6
4. Структура и состав локальной вычислительной сети	7
5. Управление и администрирование локальной вычислительной сетью	8
6. Правила внесения изменений в конфигурацию ЛВС	9
7. Требования к обслуживанию физической структуры ЛВС	9
8. Порядок предоставления доступа к ресурсам локальной вычислительной сети	10
9. Изменение и прекращение доступа к ресурсам локальной вычислительной сети ...	11
10. Права и обязанности пользователей локальной вычислительной сети	12
11. Правила использования ресурсов локальной вычислительной сети	13
12. Обеспечение безопасности информации в локальной вычислительной сети	15
13. Ответственность	17
14. Заключительные положения	18
Приложение 1. Заявка на доступ к ресурсам ЛВС	20
Приложение 2. Журнал учета изменений ИТ-инфраструктуры	21



ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Отдел информационно-технического сопровождения

Положение о локальной вычислительной сети

1. Общие положения

1.1. Настоящее Положение о локальной вычислительной сети (далее – Положение) определяет назначение, структуру, принципы построения, правила эксплуатации и порядок использования локальной вычислительной сети (далее – ЛВС) в федеральном государственном бюджетном образовательном учреждении высшего образования «Северный государственный медицинский университет» Министерства здравоохранения Российской Федерации (далее – Университет).

1.2. Положение является локальным нормативным актом Университета и разработано в соответствии с действующим законодательством Российской Федерации и требованиями Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 31.12.2021 № 2606 «Об утверждении Правил оказания услуг связи по передаче данных», постановления Правительства Российской Федерации от 31.12.2021 № 2607 «Об утверждении Правил оказания телематических услуг связи», приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказа ФСТЭК России 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 и требования настоящего Положения распространяются на всех сотрудников Университета, обучающихся, а также на иных лиц, допущенных к ресурсам ЛВС в установленном порядке и являющихся пользователями ЛВС.



2. Термины и определения.

В настоящем Положении используются следующие термины и определения:

Администратор безопасности информационных ресурсов (ответственный за защиту информации) – должностное лицо, уполномоченное на выполнение административных функций и обеспечивающее безопасность функционирования информационных ресурсов.

Администратор информационного ресурса – работник (или группа работников), уполномоченный на выполнение административных функций и обеспечивающий функционирование информационного ресурса.

Администратор локальной вычислительной сети – сотрудник (или подразделение), ответственный за проектирование, внедрение, сопровождение, обеспечение работоспособности и безопасности ЛВС.

Гостевая беспроводная сеть – сегмент ЛВС, предназначенный для предоставления доступа к сети Интернет посетителям и иным лицам, не являющимся сотрудниками или обучающимися Университета, с обязательной идентификацией и аутентификацией.

Доступ к информации (доступ) – возможность получения информации и её использования.

Идентификатор – уникальная буквенно-числовая последовательность, позволяющая однозначно определить пользователя локальной вычислительной сети.

Информационная безопасность (безопасность информации) – состояние защищённости информации, при котором обеспечиваются её конфиденциальность, целостность и доступность.

Локальная вычислительная сеть (ЛВС) – совокупность программных, аппаратных и кабельных компонентов, объединяющих автоматизированные рабочие места пользователей, серверы и периферийное оборудование в единую вычислительную среду в пределах зданий и помещений Университета.

Несанкционированный доступ (НСД) – доступ к ресурсам ЛВС, осуществленный с нарушением установленных правил разграничения доступа.

Пароль – секретное условное слово, фраза или произвольный набор знаков (состоящий из букв, цифр и других символов), предназначенный для подтверждения личности или полномочий пользователя.



Пользователь – сотрудник Университета, обучающийся или иное лицо, допущенное к работе в ЛВС и использующее её ресурсы для выполнения трудовых, учебных или иных правомерных задач.

Рабочая станция – автоматизированное рабочее место пользователя, подключённое к ЛВС и оснащённое интерфейсом для доступа к информационным ресурсам.

Ресурсы ЛВС – серверное и коммуникационное оборудование, рабочие станции, общесистемное и прикладное программное обеспечение, данные, каналы связи и доступ к сети Интернет, предоставляемые в рамках ЛВС.

Типовая роль – установленный для категории пользователей набор функций и полномочий при использовании информационных ресурсов ЛВС.

3. Цели и задачи локальной вычислительной сети

3.1. Основная цель создания и функционирования ЛВС – повышение эффективности деятельности Университета за счёт оперативного обмена информацией, автоматизации учебных, научных и управленческих процессов, коллективного использования вычислительных и информационных ресурсов, а также обеспечения защищённой информационной среды.

3.2. Основные задачи ЛВС:

- обеспечение централизованного хранения, обработки и защиты данных, включая персональные данные и сведения, составляющие врачебную тайну;
- предоставление пользователям совместного доступа к прикладным системам, базам данных, файловым хранилищам, периферийному оборудованию (принтеры, многофункциональные устройства);
- поддержка функционирования электронных образовательных сред, дистанционных образовательных технологий, электронных библиотечных систем и иных учебных ресурсов;
- организация работы систем видеоконференцсвязи;
- организация внутренней электронной почты, средств коллективной работы и обмена сообщениями;
- обеспечение управляемого и безопасного доступа к глобальной сети Интернет, включая фильтрацию нежелательного контента и защиту от вредоносного программного обеспечения;



- организация управляемого гостевого доступа к сети Интернет с идентификацией пользователей через «Единую системы идентификации и аутентификации» (далее – ЕСИА), с полной изоляцией гостевого трафика от корпоративной сети;
- обеспечение идентификации и аутентификации пользователей, разграничения их прав доступа к ресурсам ЛВС в соответствии с установленными типовыми ролями;
- обеспечение управляемого и защищённого доступа к государственным и иным информационным системам, используемым в деятельности Университета (в том числе к государственным информационным системам в сфере образования и здравоохранения);
- регистрация событий безопасности, мониторинг работоспособности сетевой инфраструктуры, своевременное выявление и реагирование на инциденты информационной безопасности;
- резервное копирование критически важных данных и конфигураций сетевого оборудования, обеспечение возможности восстановления работоспособности ЛВС после сбоев и аварий.

4. Структура и состав локальной вычислительной сети

4.1. Физическую структуру ЛВС образуют:

- структурированная кабельная система (СКС), соединительное оборудование;
- активное сетевое оборудование (коммутаторы, маршрутизаторы, точки беспроводного доступа);
- серверное оборудование (серверы, системы хранения данных, источники бесперебойного питания);
- автоматизированные рабочие места пользователей (персональные компьютеры, ноутбуки, терминалы);
- программно-аппаратные средства защиты информации (межсетевые экраны, криптографические шлюзы, средства защиты от несанкционированного доступа).

4.2. Логическая структура ЛВС включает:

- доменную структуру или рабочую группу, сегментирование сети на подсети (изолированные подсети для служебного трафика, служебные и гостевые беспроводные сети), в том числе с учётом требований безопасности;
- каталог пользователей и групп, политики безопасности



- систему сетевых сервисов (DNS, DHCP, файловые службы, веб-сервисы, базы данных, корпоративная почта);

- систему защиты информации (антивирусная защита, система обнаружения и предотвращения вторжений, подсистема сбора и анализа событий безопасности).

4.3. Схема организации ЛВС, её границы, используемое оборудование и программное обеспечение, включая средства защиты информации, определяются проектной и эксплуатационной документацией, утверждаемой ректором Университета или уполномоченным лицом.

5. Управление и администрирование локальной вычислительной сетью

5.1. Планирование дальнейшего развития, контроль и общее руководство работами по развитию и функционированию ЛВС осуществляет проректор по цифровой трансформации.

5.2. Администрирование ЛВС осуществляется сотрудниками отдела развития ИТ-инфраструктуры, на которых возлагаются функции администратора ЛВС. В обязанности сотрудников отдела развития ИТ-инфраструктуры входит:

- поддержание работоспособности активного и пассивного сетевого оборудования;
- установка, настройка и обновление системного и прикладного программного обеспечения на серверных платформах;
- установка, настройка и обновление программного обеспечения на активном сетевом оборудовании;
- управление учётными записями пользователей, правами доступа к ресурсам;
- мониторинг и протоколирование работы сети, анализ инцидентов и сбоев;
- ведение актуальной документации по конфигурации сети, включая схемы ЛВС, перечни активного сетевого оборудования с указанием IP-адресов, журналы учёта изменений конфигурации, а также регламенты выполнения плановых и аварийных работ;
- взаимодействие с провайдерами услуг связи и поставщиками оборудования;

Совместно с ответственным за защиту информации разрабатываются и реализуются меры по обеспечению информационной безопасности в ЛВС (антивирусная защита, межсетевое экранирование, резервное копирование).

5.3. Администратор ЛВС имеет право:



- ограничивать или прекращать доступ любого пользователя к ресурсам ЛВС в случае нарушения настоящего Положения, обнаружения угрозы безопасности или по служебной необходимости;

- проводить плановые и внеплановые профилактические работы, при этом уведомляя пользователей о возможных перерывах в работе (кроме экстренных ситуаций);

- контролировать использование ресурсов ЛВС в объеме, минимально необходимом для выполнения сотрудниками их должностных обязанностей, а обучающимися – учебных задач, с соблюдением требований законодательства Российской Федерации о персональных данных.

5.4. Все изменения в конфигурации ЛВС, перемещение оборудования, ввод новых и исключение имеющихся сервисов, установка и изъятие оборудования, производятся только после согласования и утверждения данных работ проректором по цифровой трансформации с обязательным отражением в существующей схеме организации ЛВС и эксплуатационной документации.

6. Правила внесения изменений в конфигурацию ЛВС

6.1. Любые изменения логической структуры ЛВС, правил маршрутизации, политик безопасности, а также конфигурации активного сетевого и серверного оборудования осуществляются исключительно с обязательной фиксацией в едином электронном «Журнале учета изменений ИТ-инфраструктуры» (Приложение 2).

6.2. Запись в «Журнале учета изменений ИТ-инфраструктуры» должна содержать:

- дату и время проведения работ;
- ФИО сотрудника проводившего работы;
- краткое описание внесенных изменений;
- наименование модифицируемого узла (оборудования/сервиса);
- причину внесения изменений (номер заявки или служебная необходимость).

6.3. Внесению изменений в критически важные узлы (маршрутизаторы, коммутаторы ядра, гипервизоры, контроллеры домена) предшествует обязательное создание резервной копии текущей конфигурации (backup).

7. Требования к обслуживанию физической структуры ЛВС.



7.1. Все физические подключения и перекоммутации в серверных помещениях и коммутационных шкафах ЛВС Университета должны выполняться с соблюдением правил обязательной маркировки.

7.2. Каждый коммутационный шнур (патч-корд) должен иметь физическую маркировку с обеих сторон. Маркировка должна однозначно идентифицировать назначение подключения (например: номер порта на патч-панели – номер порта на коммутаторе, либо номер кабинета – номер порта).

7.3. Категорически запрещается оставление в коммутационных шкафах неподключенных (висящих) патч-кордов, а также создание временных немаркированных соединений на срок более 24 часов.

7.4. При выявлении в коммутационном шкафу немаркированных кабельных соединений, администратор ЛВС имеет право произвести их демонтаж в ходе проведения плановых профилактических работ без предварительного уведомления.

7.5. В целях обеспечения бесперебойной работы сетевой инфраструктуры и предотвращения аппаратных сбоев, сотрудники отдела развития ИТ-инфраструктуры обязаны проводить плановый технический осмотр серверных помещений и коммутационных шкафов не реже 1 (одного) раза в 2 (два) месяца.

7.6. Плановый технический осмотр в обязательном порядке должен включать в себя:

- визуальную проверку индикации портов и системных панелей активного оборудования на наличие ошибок и неисправностей;
- проверку состояния систем охлаждения и обесточивание/очистку оборудования от скоплений пыли;
- контроль температурного режима внутри коммутационных шкафов. Отметка о проведенном осмотре и выявленных недостатках заносится в «Журнал учета изменений ИТ-инфраструктуры».

8. Порядок предоставления доступа к ресурсам локальной вычислительной сети

8.1. Доступ к ресурсам ЛВС предоставляется на основании поданной пользователем письменной «Заявки на предоставление доступа к ресурсам ЛВС» (Приложение 1), подписанное руководителем его структурного подразделения или лица его замещающего.



Заявку для доступа представителей сторонней организации подписывает и подает руководитель структурного подразделения в интересах которого выполняются работы по договору.

Для доступа ресурсам ЛВС обучающихся, заявку подписывает и подает представитель деканата.

Заявка подается на имя проректора по цифровой трансформации.

8.2. В заявке указываются:

- фамилия, имя, отчество пользователя;
- должность, структурное подразделение, номер кабинета (компания и номер договора для сторонних организаций, группа и курс для обучающихся);
- перечень ресурсов ЛВС и информационных систем, необходимых для исполнения должностных обязанностей или выполнения договорных обязательств (научной, учебной или иной деятельности для обучающихся).

8.3. На основании заявки администратор ЛВС создает учетную запись пользователя и назначает права доступа к ресурсам ЛВС и информационным системам в соответствии с должностными обязанностями, выполняемыми работами, научной или учебной деятельностью пользователя. После чего выдает пользователю идентификационные данные (логин и пароль) с записью в «Журнале учета пользователей локальной вычислительной сети».

8.4. Права доступа предоставляются по принципу минимальной достаточности – пользователю предоставляется только тот объем прав, который необходим для выполнения его должностных обязанностей, выполнения работ, научной или учебной деятельности.

8.5. Пользователь допускается к работе с ресурсами ЛВС только после ознакомления под подпись с настоящим Положением, Политикой парольной защиты, Инструкцией пользователя ЛВС и требованиями по защите информации.

8.6. Регистрация пользователя в ЛВС производится администратором ЛВС на основании заявки в срок не превышающий 3 рабочих дней.

9. Изменение и прекращение доступа к ресурсам локальной вычислительной сети

9.1. Изменение прав доступа пользователя к ресурсам ЛВС осуществляется:

- по инициативе пользователя;



- по инициативе непосредственного руководителя;
- по решению администратора ЛВС при выявлении нарушений требований информационной безопасности.

9.2. Изменение прав доступа оформляется аналогично предоставлению доступа (п. 8.1–8.5 настоящего Положения).

9.3. Права доступа пользователя прекращаются в следующих случаях:

- увольнение (отчисление) пользователя;
- перевод пользователя на другую должность, не требующую доступа к ресурсам ЛВС или окончание срока обучения;
- истечение срока действия договора (для работников сторонних организаций);
- выявление фактов грубого нарушения требований информационной безопасности.

9.4. При прекращении прав доступа (увольнение, отчисление), администратор ЛВС обязан заблокировать учетную запись пользователя в день, следующий за днём прекращения соответствующих отношений, а если это невозможно – не позднее следующего рабочего дня. В иных случаях, предусмотренных п. 9.3, блокировка производится в течение 1 рабочего дня с момента получения администратором соответствующего уведомления.

9.5. Администратор ЛВС не реже одного раза в год проводит сверку действующих учётных записей со списками, предоставленными отделом кадров и учебным управлением. Учётные записи пользователей, отсутствующие в предоставленных списках, подлежат блокировке

10. Права и обязанности пользователей локальной вычислительной сети

10.1. Пользователь ЛВС имеет право:

- использовать сервисы и ресурсы ЛВС, предоставленные ему для выполнения служебных обязанностей или учебных задач;
- получать от администратора консультационную поддержку по работе с сервисами и ресурсами ЛВС в пределах установленного Положения;
- обращаться к администратору с заявками на подключение нового оборудования, изменение прав доступа к сервисам и ресурсам с обоснованием служебной или учебной необходимости, изменения учётных данных в учетной записи.

10.2. Пользователь обязан:



- соблюдать требования настоящего Положения и иных инструкций по работе с ЛВС;
- использовать сервисы и ресурсы ЛВС исключительно для служебных или учебных целей, определённых трудовым договором, должностной инструкцией или учебным планом;
- содержать в тайне личные пароли и аутентификационные данные, не передавать их третьим лицам, немедленно уведомлять администратора о фактах компрометации учётной записи;
- не допускать установки нелицензионного, вредоносного, неразрешённого программного обеспечения, а также самостоятельного изменения конфигурации операционной системы и сетевых настроек рабочей станции;
- соблюдать правила антивирусной безопасности, не отключать установленные администратором защитные средства;
- бережно относиться к оборудованию ЛВС, не производить его самостоятельное перемещение и перекоммутацию;
- сообщать обо всех сбоях, некорректной работе сети и её компонентов администратору.

10.3. Пользователю запрещается:

- предпринимать попытки несанкционированного доступа к сервисам и ресурсам ЛВС, к которым ему не предоставлены права;
- использовать сетевое оборудование и информационные ресурсы для совершения любых 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, экстремистского содержания.

11. Правила использования ресурсов локальной вычислительной сети

11.1. Доступ в сеть Интернет предоставляется пользователям исключительно для решения служебных или учебных задач. Потоки данных (сетевой трафик), не связанные с основной деятельностью Университета (просмотр развлекательных сайтов, загрузка



объёмного мультимедийного контента неслужебного характера, сетевые игры), могут быть ограничены или запрещены.

11.2. Доступ в сеть Интернет и к ресурсам локальной вычислительной сети посредством внутренних беспроводных сетей осуществляется только авторизованными пользователями ЛВС. Подключение к университетской служебной беспроводной сети производится с использованием протоколов шифрования не ниже WPA2-Enterprise с аутентификацией через каталог пользователей (Active Directory или аналогичный) позволяющий однозначно идентифицировать пользователя ЛВС. Запрещается создание несанкционированных точек доступа, а также подключение к университетской беспроводной сети личных устройств, за исключением случаев, когда подключение личных устройств разрешено отдельным распоряжением руководства Университета, при условии соблюдения требований информационной безопасности.

11.3. Для доступа к сети Интернет посетителям и иным лицам организуется гостевая беспроводная сеть. Доступ предоставляется исключительно после идентификации и аутентификации с использованием ЕСИА. Организация гостевого доступа должна обеспечивать полную изоляцию гостевого трафика от служебного. Срок сессии гостевого доступа не может превышать 24 часа, по истечении которых требуется повторная авторизация. В случае недоступности ЕСИА доступ к гостевой сети не предоставляется до восстановления работоспособности системы. Иные способы идентификации для гостевого доступа не допускаются.

11.4. Удалённый доступ к ресурсам локальной вычислительной сети может быть предоставлен только при использовании сертифицированных средств криптографической защиты информации и многофакторной аутентификации пользователя.

Удаленный доступ предоставляется на основании отдельной заявки, сроком не более 3 месяцев, с обязательным протоколированием всех сеансов.

11.5. Служебная электронная почта должна использоваться только для служебной переписки. Пользователю запрещается использовать служебную электронную почту для:

- регистрации на интернет ресурсах, если они не связаны со служебной деятельностью;
- рассылки несанкционированных массовых сообщений (спама);
- передачи файлов, содержащих вредоносное программное обеспечение;



ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Отдел информационно-технического сопровождения

Положение о локальной вычислительной сети

- направления информации конфиденциального характера, в том числе персональных данных и сведений, составляющих врачебную тайну.

11.6. Программное обеспечение, необходимое пользователям для выполнения служебных обязанностей или организации учебного процесса, должно входить в утверждённый перечень разрешенного программного обеспечения. Установка любого дополнительного программного обеспечения на автоматизированное рабочее место пользователя должна быть обоснована служебной или учебной необходимостью и согласована с проректором по цифровой трансформации и внесена в перечень разрешенного программного обеспечения.

11.7. Служебная информация, созданная или обрабатываемая сотрудниками в рамках выполнения трудовых обязанностей, может содержать конфиденциальную информацию о деятельности Университета. Сотрудникам запрещено копировать, выносить или передавать данную информацию третьим лицам или во внешние системы без особого разрешения. Исключения возможны только при наличии письменного разрешения проректора по цифровой трансформации и при неукоснительном соблюдении действующих мер и правил защиты информации.

11.8. Доступ к конфиденциальной информации, находящейся в ЛВС, в том числе к персональным данным и сведениям, составляющим врачебную тайну, разрешён исключительно пользователям, допущенным к ним в соответствии с приказом ректора Университета (или уполномоченного им лица) и ознакомленным с требованиями по обеспечению безопасности информации.

12. Обеспечение безопасности информации в локальной вычислительной сети

12.1. Защита информации в ЛВС обеспечивается комплексом организационных, правовых и программно-технических мер, включающих:

- разграничение доступа к информационным ресурсам на основе учётных записей и парольной политики;
- антивирусную защиту на серверах и рабочих станциях;
- межсетевое экранирование для защиты от несанкционированного доступа из внешних сетей;
- систему обнаружения и предотвращения вторжений;



- криптографическую защиту информации конфиденциального характера при её передаче по открытым каналам связи с использованием сертифицированных средств;
- резервное копирование критически важных данных по утверждённому расписанию;
- ведение системных журналов и протоколов для фиксации событий безопасности;
- ведение журналов идентификации пользователей гостевой беспроводной сети с фиксацией фамилии, имени, отчества, даты и времени сессии, MAC-адреса устройства, с сроком хранения не менее 1 года;
- регулярное обновление системного и прикладного программного обеспечения в целях устранения известных уязвимостей;
- контроль целостности системного и прикладного программного обеспечения;
- мониторинг сетевой активности и контроль соблюдения пользователями требований настоящего Положения.

12.2. Парольная политика устанавливает минимальные требования к длине, сложности, периодичности смены паролей, а также блокировку учётной записи при нескольких неудачных попытках входа. Конкретные параметры политики определяются отдельным локальным нормативным актом Университета.

12.3. Администратор локальной вычислительной сети имеет право осуществлять мониторинг сетевой активности в целях выявления неисправностей, угроз безопасности и контроля соблюдения пользователями настоящего Положения. При обнаружении угрозы безопасности администратор ЛВС обязан незамедлительно принять доступные меры по её блокировке (вплоть до временного ограничения доступа) и уведомить об этом ответственного за защиту информации.

12.4. В случае обнаружения инцидента информационной безопасности пользователь обязан незамедлительно сообщить о нём ответственному за защиту информации и прекратить любые действия, способные усугубить ситуацию, до получения инструкций.

12.5. Ответственный за защиту информации совместно с администратором локальной вычислительной сети при получении сообщения об инциденте информационной безопасности обязаны действовать в соответствии с принятым в Университете «Порядком реагирования на инциденты информационной безопасности»:

- принять меры по локализации и ликвидации последствий инцидента;
- провести анализ причин и обстоятельств;



- обеспечить восстановление работоспособности ЛВС и сохранность данных;
- задокументировать факт инцидента и выполненные действия;
- проинформировать руководство Университета в установленном порядке.

12.6. Серверное и активное сетевое оборудование ЛВС размещается в запираемых помещениях (серверных комнатах, коммутационных шкафах), доступ к которым предоставляется только уполномоченным лицам в соответствии со списком, утверждённым проректором по цифровой трансформации.

12.7. В целях выявления уязвимостей и оценки эффективности принятых мер защиты не реже одного раза в год проводится анализ защищённости ЛВС (включая сканирование сетевых портов, проверку настроек оборудования и ПО, тестирование на проникновение). Результаты анализа оформляются актом и учитываются при планировании мероприятий по повышению безопасности информации.

13. Ответственность

13.1. Нарушение требований настоящего Положения может повлечь за собой дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

13.2. Пользователи (сотрудники, обучающиеся и иные лица, допущенные к информационным ресурсам), виновные в нарушении правил эксплуатации ЛВС, повлекшем за собой выход оборудования из строя, утрату или искажение информации, несут ответственность в порядке, установленном законодательством Российской Федерации.

13.3. Администратор локальной вычислительной сети и ответственный за защиту информации несут ответственность за качество и своевременность выполнения функций, предусмотренных настоящим Положением, в пределах своих полномочий.

13.4. Ответственность за сохранность конфиденциальной информации, в том числе персональных данных и медицинских данных, обрабатываемой на автоматизированном рабочем месте, возлагается на пользователя, которому эта информация доверена для выполнения трудовых, учебных или иных задач.

13.5. За разглашение личных аутентификационных данных (идентификатора, пароля) и иных фактов компрометации учётной записи пользователь несёт ответственность



ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Отдел информационно-технического сопровождения

Положение о локальной вычислительной сети

в соответствии с законодательством Российской Федерации, а также с локальными нормативными актами Университета.

14. Заключительные положения

14.1. Настоящее Положение вступает в силу с момента его утверждения ректором Университета.

14.2. Все сотрудники Университета, обучающиеся и иные лица, имеющие доступ к ресурсам ЛВС Университета, должны быть ознакомлены с настоящим Положением под роспись. Ознакомление сотрудников проводится при приёме на работу, обучающихся – при зачислении, иных лиц – при предоставлении им доступа к ЛВС в установленном порядке.

14.3. При прекращении трудовых отношений с сотрудником или отчислении обучающегося доступ к ресурсам ЛВС прекращается, а учётная запись блокируется администратором ЛВС в день, следующий за днём прекращения соответствующих отношений, а если это невозможно – не позднее следующего рабочего дня. Пользователь обязан сдать все носители информации, содержащие служебные данные (в том числе электронные ключи доступа, смарт-карты). Факт сдачи оборудования и носителей оформляется отметкой в обходном листе.

14.4. Изменения и дополнения в Положение вносятся по мере необходимости, в том числе в случае изменения законодательства Российской Федерации, регламентирующего соответствующие отношения. Внесение изменений и дополнений оформляется приказом ректора Университета по представлению проректора по цифровой трансформации.

14.5. С момента утверждения новой редакции Положения (или изменений к нему) предыдущая редакция утрачивает силу.

14.6. Настоящее Положение является обязательным для исполнения всеми пользователями ЛВС Университета. Локальные нормативные акты Университета, регулирующие вопросы эксплуатации ЛВС и защиты информации, применяются в части, не противоречащей настоящему Положению.

14.7. Вопросы, не урегулированные настоящим Положением, решаются в соответствии с действующим законодательством Российской Федерации и иными локальными нормативными актами Университета.

14.8. Подлинный экземпляр настоящего Положения хранится в Службе делопроизводства и контроля документооборота Университета. Электронная версия



ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Отдел информационно-технического сопровождения

Положение о локальной вычислительной сети

Положения размещается на официальном сайте Университета в информационно-телекоммуникационной сети Интернет.

Приложение 1

Заявка на предоставление доступа к ресурсам ЛВС

Имя: Иван Александрович

Фамилия: Иванов

Пол: Мужской

Дата рождения: 15.05.1990

Место рождения: г. Москва

Паспорт: 78 05/0012345

СНИЛС: 50-01-00123456789

ИНН: 50-01-0012345

Адрес: г. Москва, ул. Ленина, д. 10, кв. 10

Телефон: 8 (495) 123-4567

Электронная почта: ivanov.alex@yandex.ru

Имя: Иван Александрович

Фамилия: Иванов

Пол: Мужской

Дата рождения: 15.05.1990

Место рождения: г. Москва

Паспорт: 78 05/0012345

СНИЛС: 50-01-00123456789

ИНН: 50-01-0012345

Адрес: г. Москва, ул. Ленина, д. 10, кв. 10

Телефон: 8 (495) 123-4567

Электронная почта: ivanov.alex@yandex.ru

Имя: Иван Александрович

Фамилия: Иванов

Пол: Мужской

Дата рождения: 15.05.1990

Место рождения: г. Москва

Паспорт: 78 05/0012345

СНИЛС: 50-01-00123456789

ИНН: 50-01-0012345

Адрес: г. Москва, ул. Ленина, д. 10, кв. 10

Телефон: 8 (495) 123-4567

Электронная почта: ivanov.alex@yandex.ru

Имя: Иван Александрович

Фамилия: Иванов

Пол: Мужской

Дата рождения: 15.05.1990

Место рождения: г. Москва

Паспорт: 78 05/0012345

СНИЛС: 50-01-00123456789

ИНН: 50-01-0012345

Адрес: г. Москва, ул. Ленина, д. 10, кв. 10

Телефон: 8 (495) 123-4567

Электронная почта: ivanov.alex@yandex.ru



ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России

Отдел информационно-технического сопровождения

Положение о локальной вычислительной сети

Приложение 2

Журнал учета изменений ИТ-инфраструктуры

№ п/п	Дата и время проведения работ	ФИО проводившего работы	Внесенные изменения
1	2	3	4

Наименование модифицируемого узла (оборудования/сервиса)	Причина внесения изменений (номер заявки или служебная необходимость)	Примечание
5	6	7