

Министерство здравоохранения Иркутской области
областное государственное бюджетное
профессиональное образовательное учреждение
«Саянский медицинский колледж»
(ОГБПОУ «Саянский медицинский колледж»)

РАССМОТРЕНО и ОДОБРЕНО
на педагогическом совете протокол № 1
от «21» 08 2016 г.

УТВЕРЖДАЮ

Директор ОГБПОУ «Саянский
медицинский колледж»

Е. Н. Третьякова
20 16 г.



ПОЛОЖЕНИЕ

об электронной информационно-образовательной среде
в ОГБПОУ «Саянский медицинский колледж»

СОГЛАСОВАНО

Председатель ЦМК общеобразовательного
цикла

И.В. Пыжьянова

Председатель ЦМК СГ и ОП циклов

Т.С. Лидуева

Председатель ЦМК ПМ по специальности
Лечебное дело Е.В. Буленкова

Председатель ЦМК ПМ по специальности
Сестринское дело Н.Г. Самсонова

Саянск, 2026

ОГБПОУ «Саянский медицинский колледж»	Положение об электронной информационно-образовательной среде в ОГБПОУ «Саянский медицинский колледж»	Стр. 1 из 15
--	---	--------------

Содержание

№ Раздела	Название раздела	Стр.
1	Общие положения	3
2	Термины и определения	4
3	Цели, задачи и принципы функционирования ЭИОС	5
4	Структура ЭИОС и её компоненты	6
5	Формирование и функционирование ЭИОС	7
6	Требования к техническому, технологическому и телекоммуникационному обеспечению ЭИОС	8
7	Требования к защите информации и персональных данных	9
8	Права и обязанности участников образовательных отношений	9
9	Механизм реализации ЭИОС, взаимодействия, связи, ответственность за использование и сохранность информационных ресурсов	11
10	Порядок разрешения инцидентов и технической поддержки	13
11	Финансовое обеспечение функционирования ЭИОС	13
	Лист дополнений и изменений	15

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Введено взамен Положения от 30.01.2023г. «Об электронной информационно-образовательной среде в ОГБПОУ «Саянский медицинский колледж».

1.2. Назначение Положения

Настоящее Положение об электронной информационно-образовательной среде (далее — Положение) определяет назначение, структуру, порядок формирования и функционирования электронной информационно-образовательной среды (далее — ЭИОС) в областном государственном бюджетном профессиональном образовательном учреждении «Саянский медицинский колледж» (далее — Колледж).

1.3. Нормативная база

Положение разработано в соответствии с:

Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (в части требований к ЭИОС, установленных статьёй 16);

Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

Постановлением Правительства РФ от 20.10.2021 № 1802 «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети "Интернет" и обновления информации об образовательной организации, а также о признании утратившими силу некоторых актов и отдельных положений некоторых актов Правительства Российской Федерации»;

Приказом Минобрнауки России от 14.06.2013 № 462 «Об утверждении Порядка проведения самообследования образовательной организацией» (с последующими изменениями);

Приказом Минобрнауки России от 10.12.2013 № 1324 «Об утверждении показателей деятельности образовательной организации, подлежащей самообследованию» (с последующими изменениями);

Приказом Минпросвещения России от 24.08.2022 № 762 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования»;

Приказом Минпросвещения России от 04.07.2022 № 526 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 31.02.01 Лечебное дело» (в действующей редакции);

Приказом Минпросвещения России от 04.07.2022 № 527 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 34.02.01 Сестринское дело» (в действующей редакции);

Приказом 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»;

Уставом Колледжа;

Локальными нормативными актами Колледжа, регламентирующими организацию и обеспечение образовательного процесса.

1.4. Область применения

Настоящее Положение распространяется на всех участников образовательных отношений Колледжа: обучающихся, педагогических работников, административно-управленческий персонал, учебно-вспомогательный персонал, а также иных лиц, использующих ЭИОС в своей деятельности.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем Положении применяются следующие термины и определения:

Электронная информационно-образовательная среда (ЭИОС) — совокупность электронных информационных ресурсов, электронных образовательных ресурсов, информационных технологий, соответствующих технологических средств, обеспечивающих освоение обучающимися образовательных программ среднего профессионального образования (далее — ОП СПО) в полном объеме независимо от их места нахождения.

Электронные информационные ресурсы — совокупность данных, представленных в электронной форме, доступ к которым обеспечивается через информационно-телекоммуникационные сети.

Электронные образовательные ресурсы (ЭОР) — образовательные ресурсы, представленные в электронно-цифровой форме и включающие структуру, предметное содержание и метаданные о них.

Электронная библиотечная система (ЭБС) — база данных, содержащая издания учебной, учебно-методической и иной литературы, доступ к которым обеспечивается через информационно-телекоммуникационные сети.

Идентификация — процедура установления соответствия предъявленного идентификатора (логина) конкретному субъекту (пользователю).

Аутентификация — процедура проверки подлинности пользователя путём сравнения введённого пароля с паролем, сохранённым в базе данных пользователей.

Персональные данные (ПДн) — любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

Информационная безопасность — состояние защищённости информации и её носителей от несанкционированного доступа, уничтожения, модификации, блокирования, копирования и иных неправомерных действий.

3. ЦЕЛИ, ЗАДАЧИ И ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ЭИОС

3.1. Цели использования ЭИОС

Целями использования ЭИОС являются:

создание в Колледже единого образовательного пространства на основе современных информационных технологий;

информационное обеспечение образовательного процесса в соответствии с требованиями к реализации ОП СПО, реализуемым в Колледже;

создание на основе современных информационных технологий площадки для коммуникации между преподавателями и обучающимися;

обеспечение возможности формирования обучающимися индивидуальной траектории и темпа освоения ОП СПО;

обеспечение информационной открытости Колледжа в соответствии с требованиями действующего законодательства Российской Федерации в сфере образования.

3.2. Задачи ЭИОС

Основными задачами ЭИОС являются:

организация доступа к учебным планам, рабочим программам учебных дисциплин (модулей), практической подготовки, к изданиям электронных библиотечных систем и электронным образовательным ресурсам, указанным в рабочих учебных программах;

фиксация хода образовательного процесса, результатов промежуточной аттестации и результатов освоения ОП СПО;

взаимодействие между участниками образовательных отношений, в том числе синхронное и (или) асинхронное взаимодействие посредством сети «Интернет»;

обучение и систематическое повышение квалификации педагогических работников, работающих с ЭИОС;

обеспечение обучающихся в течение всего периода обучения доступом к электронной библиотечной системе (далее — ЭБС), содержащей издания

учебной, учебно-методической и иной литературы, используемой в образовательном процессе;

обеспечение доступа обучающихся к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин (модулей);

обеспечение обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов доступом к ЭИОС в адаптированной форме.

3.3. Принципы функционирования ЭИОС

Функционирование ЭИОС строится на следующих принципах:

законность — соответствие всех процедур требованиям законодательства Российской Федерации;

открытость — доступность ЭИОС для всех участников образовательных отношений;

надёжность — бесперебойное функционирование и сохранность данных;

безопасность — защита информации и персональных данных в соответствии с законодательством;

единство — единая точка входа и единые требования к идентификации и аутентификации пользователей.

4. СТРУКТУРА ЭИОС И ЕЁ КОМПОНЕНТЫ

4.1. Составные элементы ЭИОС

Составными элементами ЭИОС Колледжа являются:

- Доступ к сети «Интернет» в Колледже (проводной и беспроводной);
- Электронная библиотечная система «Консультант студента»;
- Электронные образовательные ресурсы и профессиональные базы данных;
- Программная среда «1С: Колледж», предназначенная для оперативной автоматизации процессов решения задач образовательного учреждения;
- Электронное расписание в программе «1С: Автоматизированное составление расписания»;
- Электронный журнал в Единой образовательной сети «Дневник.ру»;
- Виртуальная обучающая среда Moodle (далее — СДО Moodle);
- Личный кабинет в федеральной государственной информационной системе «Моя школа»;
- Официальный сайт Колледжа (режим доступа: <http://med-sayansk.ru/>);

4.2. Социальные сети

Официальные группы Колледжа в социальных сетях (Мих, ВК) не являются частью ЭИОС и используются исключительно в целях информационного освещения деятельности Колледжа и оперативного

взаимодействия с обучающимися и их родителями (законными представителями).

5. ФОРМИРОВАНИЕ И ФУНКЦИОНИРОВАНИЕ ЭИОС

5.1. Общие требования

5.1.1. В целях обеспечения защиты информации, соблюдения конфиденциальности информации ограниченного доступа и реализации права на доступ к информации для надёжного, безотказного и производительного функционирования ЭИОС Колледжа устанавливаются следующие требования:

ЭИОС и отдельные её элементы должны соответствовать действующему законодательству РФ в области образования, защиты авторских прав, защиты информации, защиты персональных данных;

доступ к ЭИОС осуществляется с компьютеров Колледжа и других устройств, имеющих выход в «Интернет», под личными логинами и паролями;

функционирование ЭИОС обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, её использующих и поддерживающих.

5.1.2. Определение ответственных за функционирование ЭИОС:

общее руководство ЭИОС осуществляет заместитель директора по учебной работе;

техническое сопровождение и администрирование ЭИОС осуществляет системный администратор;

методическое сопровождение осуществляют методист, председатели цикловых методических комиссий.

5.2. Требования к подготовке пользователей

5.2.1. Пользователи должны иметь соответствующую подготовку по работе с элементами ЭИОС:

обучающиеся — наличие базовых навыков работы с компьютером;

педагогические работники, участвующие в реализации ОП СПО, — повышение квалификации по программам дополнительного профессионального образования в области информационно-коммуникационных технологий и (или) электронного обучения.

5.2.2. Обучающиеся под подпись получают логины и пароли доступа в СДО Moodle и внешние ЭБС.

5.3. Порядок предоставления доступа

5.3.1. Учётные записи пользователей создаются системным администратором на основании:

приказа о зачислении обучающегося (для обучающихся);

трудового договора (для работников);

заявки руководителя структурного подразделения (при необходимости).

5.3.2. При создании учётной записи пользователь получает логин и первичный пароль. Первичный пароль подлежит обязательной смене при первом входе в систему.

5.3.3. Пользователь несёт ответственность за сохранность своего логина и пароля.

6. ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ, ТЕХНОЛОГИЧЕСКОМУ И ТЕЛЕКОММУНИКАЦИОННОМУ ОБЕСПЕЧЕНИЮ ЭИОС

6.1. Общие требования

ЭИОС обеспечивает надёжное, безотказное и производительное выполнение следующих технических, технологических и телекоммуникационных требований:

всё серверное оборудование имеет средства отказоустойчивого хранения и восстановления данных;

всё серверное оборудование имеет аппаратные и (или) программные средства обеспечения информационной безопасности;

обеспечивается восстановление информации в ретроспективе не менее 2 (двух) недель;

компьютеры объединены в единую локальную сеть;

для всех обучающихся и работников обеспечен доступ к работе в ЭИОС из любой точки, имеющей подключение к сети «Интернет», как с территории Колледжа, так и вне его пределов.

6.2. Требования к резервному копированию

6.2.1. Резервное копирование данных ЭИОС осуществляется:

ежедневно — инкрементное копирование (данные за текущий день);

еженедельно — полное копирование (все данные);

ежемесячно — архивирование полной копии с хранением не менее 6 месяцев.

6.2.2. Резервные копии хранятся на отдельных носителях, обеспечивающих возможность восстановления данных при сбоях.

6.3. Требования к антивирусной защите

6.3.1. Все серверы и рабочие станции, подключённые к ЭИОС, должны быть обеспечены лицензионным антивирусным программным обеспечением.

6.3.2. Обновление антивирусных баз осуществляется не реже одного раза в сутки.

6.3.3. Проведение полной антивирусной проверки серверного оборудования осуществляется не реже одного раза в неделю.

6.4. Требования к защите от несанкционированного доступа

6.4.1. Доступ к серверному оборудованию и административным панелям ЭИОС осуществляется только уполномоченными лицами.

7. ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ И ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Общие требования

7.1.1. Обработка персональных данных в ЭИОС осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

7.1.2. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных определяются в соответствии с Приказом ФСТЭК России от 18.02.2013 № 21.

7.1.3. Обработка персональных данных без использования средств автоматизации осуществляется в соответствии с Постановлением Правительства РФ от 15.09.2008 № 687.

7.2. Меры по защите информации

В ЭИОС применяются следующие меры по защите информации:

назначение ответственного за обеспечение безопасности персональных данных;

ограничение доступа к персональным данным в соответствии с должностными обязанностями;

применение средств защиты информации (антивирусы, межсетевые экраны, системы обнаружения вторжений);

регистрация и учёт носителей информации;

резервное копирование и восстановление данных;

шифрование каналов передачи данных (при необходимости);

ведение журналов безопасности.

7.3. Обязанности работников в части защиты информации

Работники Колледжа, имеющие доступ к ЭИОС, обязаны:

соблюдать требования законодательства о персональных данных;

не разглашать персональные данные обучающихся и работников третьим лицам;

не использовать персональные данные в личных целях;

сообщать ответственному за безопасность ПДн о фактах нарушения защиты информации.

8. ПРАВА И ОБЯЗАННОСТИ УЧАСТНИКОВ ОБРАЗОВАТЕЛЬНЫХ ОТНОШЕНИЙ

8.1. Права обучающихся

Обучающиеся имеют право:

на доступ к ЭИОС в течение всего периода обучения;

на получение логина и пароля для доступа к ЭИОС;

на доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям ЭБС и ЭОР;

на получение учебно-методической, технической и консультационной поддержки при работе с ЭИОС.

8.2. Обязанности обучающихся

Обучающиеся обязаны:

соблюдать правила электронной этики внутри сетевого учебного сообщества;

соблюдать авторские соглашения и указывать ссылки на источники при использовании цитат;

не передавать свои логин и пароль третьим лицам;

не осуществлять несанкционированный доступ к ЭИОС;

не использовать ЭИОС в целях, противоречащих законодательству Российской Федерации;

сообщать системному администратору о невозможности авторизованного входа.

8.3. Права педагогических работников

Педагогические работники имеют право:

на доступ к ЭИОС в течение всего периода работы;

на использование ЭОР и ЭБС в образовательном процессе;

на размещение учебных материалов в ЭИОС;

на получение технической и методической поддержки при работе с ЭИОС.

8.4. Обязанности педагогических работников

Педагогические работники обязаны:

использовать ЭИОС в образовательном процессе в соответствии с требованиями ФГОС СПО;

своевременно наполнять ЭИОС учебными материалами;

фиксировать результаты промежуточной аттестации обучающихся в ЭИОС;

соблюдать требования по защите персональных данных;

соблюдать правила электронной этики.

8.5. Права администрации

Администрация Колледжа имеет право:

на полный доступ к ЭИОС;

на получение отчетов о функционировании ЭИОС;

на принятие управленческих решений на основе данных ЭИОС.

8.6. Обязанности администрации

Администрация Колледжа обязана:

обеспечивать функционирование ЭИОС в соответствии с законодательством;

назначать ответственных за функционирование ЭИОС;

обеспечивать защиту информации и персональных данных;

обеспечивать обучение работников работе с ЭИОС.

8.7. Права и обязанности системного администратора

Системный администратор имеет право:

на доступ к административным панелям ЭИОС;

на блокировку учётных записей пользователей при нарушении правил использования ЭИОС.

Системный администратор обязан:

обеспечивать бесперебойное функционирование ЭИОС;

создавать и удалять учётные записи пользователей;

проводить резервное копирование данных;

обеспечивать антивирусную защиту;

сообщать руководству об инцидентах информационной безопасности.

9. МЕХАНИЗМ РЕАЛИЗАЦИИ ЭИОС, ВЗАИМОДЕЙСТВИЯ, СВЯЗИ, ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ И СОХРАННОСТЬ ИНФОРМАЦИОННЫХ РЕСУРСОВ

9.1. Общие правила использования ЭИОС

9.1.1. Использование материалов, извлечённых из ЭИОС, способом, предполагающим получение к ним доступа неограниченного круга лиц, должно сопровождаться указанием на ЭИОС, из которой эти материалы извлечены.

9.1.2. Право доступа к ЭИОС имеют все участники образовательных отношений в пределах их прав доступа, установленных разделом 8 настоящего Положения.

9.1.3. Каждый обучающийся и работник имеет право на получение учебно-методической, технической, консультационной поддержки при работе с ЭИОС.

9.2. Правила электронной этики

9.2.1. Обучающиеся и работники, получившие учётные данные, обязаны соблюдать правила электронной этики внутри сетевого учебного сообщества в ЭИОС:

компетентно отвечать в форумах, обсуждениях, опросах и других формах сетевого общения;

соблюдать авторские соглашения и всегда указывать ссылки на источники при использовании цитат в сообщениях;

проявлять корректность в общении с другими участниками сетевого сообщества.

9.3. Ответственность пользователей

9.3.1. Обучающийся и работник, получившие учётные данные для авторизованного доступа в ЭИОС, уведомляют системного администратора в случае невозможности авторизованного входа с первичным или изменённым пользователем паролем с целью временного блокирования доступа в систему от своего имени.

9.3.2. Обучающийся и работник используют ресурсы ЭИОС с соблюдением авторских прав, не воспроизводят полностью или частично информацию под своим либо иным логином и паролем, не распространяют, не изменяют либо иным способом модифицируют информацию.

9.3.3. Обучающийся и работник несут ответственность:

за несанкционированное использование регистрационной информации других обучающихся и (или) работников, в частности — использование другого логина и пароля для входа в ЭИОС и осуществление различных операций от имени другого обучающегося и (или) работника;

за умышленное использование программных средств (вирусов и (или) самовоспроизводящегося кода), позволяющих осуществлять несанкционированное проникновение в ЭИОС с целью модификации информации, кражи паролей, угадывания паролей и других несанкционированных действий.

9.4. Порядок блокировки и удаления учётных записей

9.4.1. В случае увольнения работников, отчисления обучающихся, имеющих доступ к ЭИОС:

отдел кадров (по работникам) и учебная часть (по обучающимся) обязаны сообщить системному администратору об этом факте в день увольнения (отчисления);

системный администратор обязан в течение одного рабочего дня заблокировать учётную запись, а по истечении 30 календарных дней — удалить её.

9.4.2. Доступ обучающегося и работника к ЭИОС может быть заблокирован в связи с невыполнением условий использования ЭИОС. Решение о блокировке принимает заместитель директора по учебной работе на основании служебной записки.

9.5. Электронный документооборот и электронная подпись

9.5.1. В ЭИОС Колледжа может применяться электронный документооборот в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и локальными нормативными актами Колледжа.

9.5.2. Электронные документы, подписанные усиленной квалифицированной электронной подписью, признаются равнозначными документам на бумажном носителе.

9.5.3. Порядок применения электронной подписи определяется отдельным локальным нормативным актом Колледжа.

9.6. Размещение информации на официальном сайте

9.6.1. Размещение информации на официальном сайте Колледжа осуществляется в соответствии с Постановлением Правительства РФ от 20.10.2021 № 1802.

9.6.2. Информация на сайте обновляется в течение 10 рабочих дней со дня её создания, получения или внесения изменений.

10. ПОРЯДОК РАЗРЕШЕНИЯ ИНЦИДЕНТОВ И ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

10.1. Техническая поддержка

10.1.1. Техническая поддержка пользователей ЭИОС осуществляется системным администратором.

10.1.2. Заявки на техническую поддержку принимаются:

по электронной почте;

по телефону;

лично (в кабинете системного администратора).

10.1.3. Сроки реакции на заявки:

критические инциденты (невозможность входа в ЭИОС, потеря данных, сбой сервера) — не более 2 часов;

стандартные заявки (проблемы с доступом к отдельным элементам ЭИОС, консультации) — не более 1 рабочего дня;

плановые работы (обновление, настройка) — по согласованию.

10.2. Разрешение инцидентов информационной безопасности

10.2.1. При выявлении инцидента информационной безопасности (несанкционированный доступ, утечка данных, вирусная атака) системный администратор обязан:

принять меры по локализации инцидента;

зафиксировать инцидент в журнале;

провести анализ причин;

принять меры по предотвращению повторения.

10.2.2. О серьезных инцидентах директор Колледжа уведомляет учредителя и, при необходимости, уполномоченные органы.

10.3. Ответственность за функционирование ЭИОС

10.3.1. Ответственность за общее руководство ЭИОС несёт заместитель директора по учебной работе.

10.3.2. Ответственность за техническое функционирование ЭИОС несёт системный администратор.

10.3.3. Ответственность за наполнение и актуализацию учебных материалов в ЭИОС несут педагогические работники.

10.3.4. Ответственность за соблюдение правил использования ЭИОС несут все пользователи.

11. ФИНАНСОВОЕ ОБЕСПЕЧЕНИЕ ФУНКЦИОНИРОВАНИЯ ЭИОС

11.1. Финансовое обеспечение функционирования ЭИОС осуществляется за счёт:

бюджетных ассигнований областного бюджета;

средств от приносящей доход деятельности Колледжа;

иных источников, не запрещённых законодательством Российской Федерации.

11.2. Финансовое обеспечение включает:

- приобретение и обновление программного обеспечения;
- приобретение и обслуживание серверного и компьютерного оборудования;
- оплату услуг связи и доступа к сети «Интернет»;
- оплату лицензий на использование ЭБС и ЭОР;
- повышение квалификации работников в области ИКТ.

ЛИСТ ДОПОЛНЕНИЙ И ИЗМЕНЕНИЙ