Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ставропольский государственный медицинский университет»
Министерства здравоохранения Российской Федерации

Кафедра информационных и цифровых технологий

УТВЕРЖДАЮ

Заведующий кафедрой информационных и цифровых технологий

_____/А.А.Хрипунова
«21» мая 2025 г.

Фонд оценочных средств по дисциплине

Наименование дисциплины	**Медицинская информатика**
Направление подготовки	31.08.77 Ортодонтия
Направленность (профиль)	Ортодонтия
Форма обучения	Очная
Год начала подготовки	2025

Ставрополь, 2025

1. Перечень компетенций, формируемых дисциплиной (полностью или частично)

Коды и наименование компетенций	Наименование компетенций
ПК 4	Готовность к применению социально-гигиенических методик сбора и медико-статистического анализа информации о стоматологической заболеваемости

1. Виды оценочных материалов и соответствие с формируемыми компетенциями

Наименование компетенций	Виды оценочных материалов	Количество заданий
ПК-4	Задание закрытого типа на установление соответствия	5 с эталоном ответов
	Задание закрытого типа на установление последовательности	5 с эталоном ответов
	Задание открытого типа с развернутым ответом/ задача	5 с эталоном ответов
	Задания открытого типа с кратким ответом	5 с эталоном ответов
	Задание закрытого типа	30 с эталоном ответов
Всего		50 заданий

2. Банк заданий по оценке уровня формирования компетенций

№ п/п	Наименование компетенций	Задание	Эталоны ответов
Задание закрытого типа на установление соответствия			

№ п/п	Наименование компетенций	Задание	Эталоны ответов
Задание закрытого типа на установление соответствия			
1.	ПК-4	Установите соответствие между термином и его определением или областью применения. КОМПОНЕНТ МИС — ФУНКЦИЯ 1. Электронная медицинская карта (ЭМК) — А. Инструмент для анализа данных и поиска закономерностей 2. Система поддержки принятия — Б. Цифровой аналог бумажной истории болезни	1–Б, 2–В, 3–Г, 4–А

		врачебных решений (СППВР) 3. Модуль телемедицинских консультаций 4. BI-аналитика (бизнес-аналитика) В. Автоматические подсказки о лекарственных взаимодействиях Г. Организация удаленных консилиумов врачей	
2.	ПК-4	Установите соответствие уровнем доступа и категориями работников медицинской организации. УРОВЕНЬ ДОСТУПА КАТЕГОРИЯ СОТРУДНИКОВ 1. Полный доступ к ЭМК (чтение, редактирование) А. Администратор баз данных, IT-специалист 2. Ограниченный доступ (чтение, частичное редактирование) Б. Пациент (через личный кабинет) 3. Технический доступ (к структурам БД, логам) В. Лечащий врач, заведующий отделением 4. Просмотр собственных данных Г. Медицинская сестра, фельдшер	1–В, 2–Г, 3–А, 4–Б
3.	ПК-4	Установите соответствие между типом угрозы и его характеристикой. ТИП УГРОЗЫ ПРИМЕР 1. Техническая угроза А. Врач сообщил коллеге пароль от своей учетной записи 2. Человеческий фактор (непреднамеренный) Б. Хакерская атака на сервер больницы (вирус-шифровальщик) 3. Организационная угроза В. Медсестра случайно отправила результаты анализов не тому пациенту 4. Злонамеренные действия Г. Отсутствие регламента работы с персональными данными	1–Б, 2–В, 3–Г, 4–А
4.	ПК-4	Установите соответствие между принципом информационной безопасности и его описанием. ПРИНЦИП ИБ ОПИСАНИЕ 1. Конфиденциальность А. Информация должна быть доступна авторизованным	1–Б, 2–Г, 3–А, 4–В

			пользователям в любое время	
		2. Целостность	Б. Доступ к информации имеют только те, кто имеет на это право	
		3. Доступность	В. Невозможность отказа от авторства или подтверждение подлинности	
		4. Неотказуемость (апеллируемость)	Г. Информация не была изменена или уничтожена несанкционированно	
5.	ПК-4	Установите соответствие между нормативным документом и его содержанием.		1–В, 2–А, 3–Б, 4–Г
		ДОКУМЕНТ	ОСНОВНОЕ СОДЕРЖАНИЕ	
		1. 152-ФЗ «О персональных данных»	А. Порядок оказания телемедицинской помощи	
		2. 323-ФЗ «Об основах охраны здоровья» (глава о телемедицине)	Б. Правила работы с врачебной тайной и информированным согласием	
		3. Приказы Минздрава о ведении ЭМК	В. Требования к сбору, хранению и защите персональных данных	
		4. Уголовный кодекс РФ (ст. 137)	Г. Ответственность за нарушение неприкосновенности частной жизни	
	Задания закрытого типа на установление последовательности			
6.	ПК-4	Расположите шаги при первичной регистрации пациента в медицинской информационной системе: А. Получение информированного согласия на обработку персональных данных Б. Идентификация личности (паспорт, полис) В. Присвоение уникального идентификатора (ID) в системе Г. Внесение демографических данных в электронную карту Д. Прикрепление сканов документов		Б, А, Г, В, Д
7.	ПК-4	Расположите правильную последовательность действий сотрудника при утере пароля от учетной записи в МИС: А. Сообщить заведующему отделением о факте утери Б. Подать заявку в IT-отдел на сброс и генерацию нового пароля		В, А, Б, Г, Д

		В. Попытаться вспомнить пароль самостоятельно (не более 3 попыток) Г. Подтвердить личность перед IT-специалистом Д. Сменить временный пароль при первом входе	
8.	ПК-4	Расположите этапы проведения телемедицинской консультации "врач-врач": А. Проведение видеоконференции и обсуждение клинического случая Б. Получение информированного согласия пациента на передачу данных В. Формирование запроса консультирующим врачом в системе Г. Загрузка медицинских документов (снимки, анализы) в защищенный раздел Д. Внесение заключения консультанта в ЭМК	Б, В, Г, А, Д
9.	ПК-4	Расположите шаги при работе с обезличенными данными из МИС для исследования: А. Формулировка гипотезы и запроса к данным Б. Экспорт данных в статистический пакет (Excel, SPSS, R) В. Получение разрешения этического комитета и локального акта Г. Обработка и визуализация результатов Д. Деидентификация (обезличивание) персональных данных	А, В, Д, Б, Г
10.	ПК-4	Расположите правильную последовательность действий сотрудника при получении подозрительного письма на рабочую почту: А. Не открывать вложения и не переходить по ссылкам Б. Сообщить в IT-отдел или отдел информационной безопасности В. Удалить письмо Г. Проверить адрес отправителя (домен) Д. Заблокировать отправителя	Г, А, Б, В, Д
Задания открытого типа с развернутым ответом			
11.	ПК-4	Вы — заведующий отделением. Медицинская сестра случайно отправила результаты анализов пациента с ВИЧ-статусом по электронной почте на неверный адрес (опечатка в одной букве). Получатель — частное лицо, не имеющее отношения к пациенту. Вопрос: Оцените ситуацию с точки зрения информационной безопасности и законодательства. Какие ваши действия как руководителя? Какие организационные меры необходимо предпринять, чтобы предотвратить подобное в будущем?	1. Оценка ситуации: Произошла утечка конфиденциальной информации (врачебная тайна, персональные данные). Нарушены требования 152-ФЗ и 323-ФЗ. Это инцидент информационной безопасности. 2. Неотложные действия:

			Зафиксировать факт отправки (скриншот, лог почтового сервера). Сообщить ответственному за ИБ и руководству. Связаться с ошибочным получателем (если возможно) с просьбой удалить письмо и не распространять информацию. Оценить масштаб ущерба. 3. Дисциплинарные меры: Провести служебное расследование. К медсестре могут быть применены дисциплинарные взыскания (вплоть до увольнения). 4. Профилактика: Провести внеочередной инструктаж по работе с конфиденциальной информацией. Внедрить технические решения: запрет на отправку персональных данных через личную почту, использование только корпоративной почты с функцией проверки получателя, автоматическое предупреждение при отправке на внешний адрес, DLP-системы.

			Пересмотреть регламенты отправки результатов.
12.	ПК-4	Вы участвуете в проекте по внедрению системы поддержки принятия врачебных решений (СППВР) в вашем отделении. Система начала выдавать сигналы о лекарственных взаимодействиях, которые, по мнению опытных врачей, являются клинически незначимыми и только замедляют работу. Вопрос: Какова ваша стратегия как врача-лидера мнений? Нужно ли отключить систему? Как взаимодействовать с IT-отделом и разработчиками для настройки системы?	Просто отключать систему нельзя, это шаг назад в безопасности. Стратегия: 1. Сбор данных: Задокументировать конкретные примеры "ложных срабатываний", которые мешают работе. 2. Анализ: Совместно с клиническим фармакологом определить, какие аллерг-сигналы действительно избыточны, а какие критически важны. 3. Взаимодействие с IT/разработчиками: Создать формализованную заявку на настройку (кастомизацию) правил СППВР. Объяснить клиническую логику изменений. 4. Обучение: Провести с коллегами разбор: объяснить, зачем нужны оставшиеся сигналы, как на них правильно реагировать. 5. Пилотный режим: Запустить обновленные настройки на ограниченный срок, собрать обратную связь.

13.	ПК-4	Ординатор решил для своей научной работы использовать данные из электронных карт пациентов (истории болезни, результаты анализов) за последние 5 лет. Он планирует опубликовать статью в журнале. Вопрос: Какие нормативные и этические требования он должен соблюсти? Опишите пошаговый алгоритм получения данных и работы с ними с момента идеи до публикации.	1. Этическая экспертиза: Получить одобрение локального этического комитета (ЛЭК) на проведение исследования. 2. Информированное согласие: Если возможно, получить согласие пациентов. Для ретроспективных исследований часто достаточно решения ЛЭК об использовании данных без согласия при условии обезличивания. 3. Запрос данных: Оформить официальный запрос на имя главного врача. 4. Обезличивание: Получить от IT-отдела выгрузку данных строго в обезличенном виде (удалены ФИО, адреса, точные даты рождения заменены на возраст, присвоен ID). Это требование 152-ФЗ. 5. Хранение: Хранить данные на защищенном ресурсе (рабочий компьютер с паролем, сервер больницы), не передавать третьим лицам.

			6. Публикация: В статье указывать, что данные обезличены, получено одобрение этического комитета, конфликт интересов отсутствует.
14.	ПК-4	В вашей больнице внедряют новую медицинскую информационную систему. Врачи старшего поколения активно сопротивляются, жалуются на сложность интерфейса и рост времени на заполнение документов. Молодые врачи (ординаторы) освоили систему быстро. Вопрос: Предложите программу мероприятий по эффективному внедрению, используя потенциал ординаторов и современные подходы к управлению изменениями (change management).	Программа мероприятий: 1. Выделение супер-пользователей: Назначить ординаторов, успешно освоивших систему, супер-пользователями (тренерами на рабочих местах). 2. Наставничество (парное программирование): Организовать работу в парах "опытный врач (старшее поколение) + ординатор (супер-пользователь)" в первые недели. 3. Сбор обратной связи: Ординаторы могут собирать "боли" старших коллег и систематизировать их для передачи разработчикам. 4. Микрообучение: Разработать короткие (3-5 мин) видеоинструкции по самым частым операциям, которые можно смотреть в любое время.

			5. Мотивация: Учитывать активность в системе при распределении стимулирующих выплат (KPI).
15.	ПК-4	При проверке логов доступа к электронным медицинским картам обнаружено, что медицинская сестра из гинекологического отделения просматривала карты пациенток из терапевтического отделения, не имея к этому служебной необходимости. На вопрос главного врача сестра ответила, что "просто было интересно". Вопрос: Квалифицируйте данное действие. Какие последствия могут наступить для медицинской сестры и для медицинской организации? Какие технические и организационные меры позволяют выявлять такие нарушения?	1. Квалификация: Нарушение врачебной тайны и конфиденциальности персональных данных. Несанкционированный доступ к информации, не связанный с исполнением должностных обязанностей. 2. Последствия: Для медсестры: дисциплинарное взыскание (замечание, выговор, увольнение); возможно привлечение к административной (штраф по КоАП) или уголовной ответственности (ст. 137 УК РФ) по иску пациентки. Для организации: предписание Роскомнадзора, крупный штраф, репутационные потери. 3. Меры выявления и профилактики: Технические: Системы логирования и аудита доступа (кто, когда, к какой карте обращался); SIEM-

			системы, выявляющие аномалии (например, доступ в нерабочее время или к картам из других отделений). Организационные: Регулярные проверки логов службой безопасности; подписание обязательств о неразглашении; обучение персонала.
Задания открытого типа с кратким ответом			
16.	ПК-4	Как называется интернет-мошенничество, целью которого является получение доступа к логинам и паролям путем рассылки писем от имени известных компаний или коллег?	Фишинг
17.	ПК-4	Какой термин используется для обозначения процесса удаления из данных прямой идентифицирующей информации (ФИО, адрес) для использования в исследованиях?	Обезличивание / Деидентификация
18.	ПК-4	Как называется система, которая анализирует входящие и исходящие электронные письма на предмет утечки конфиденциальной информации?	DLP-система (Data Loss Prevention)
19.	ПК-4	Введите аббревиатуру, обозначающую вид электронной подписи, которая формируется простыми кодами и паролями (например, через СМС) и используется для доступа к личному кабинету пациента.	ПЭП (простая электронная подпись)
20.	ПК-4	Как называется технология, позволяющая проводить врачебные консилиумы, консультации и дистанционный мониторинг пациентов с использованием информационно-коммуникационных сетей?	Телемедицина
Задания закрытого типа			
21.	ПК-4	Что относится к персональным данным согласно 152-ФЗ? А. Только паспортные данные Б. Любая информация, относящаяся к прямо или косвенно определенному физическому лицу В. Только данные о состоянии здоровья Г. Только фамилия и имя	Б
22.	ПК-4	Какое действие нарушает правила информационной безопасности? А. Использование двухфакторной аутентификации	Б

		Б. Хранение списка паролей в записной книжке под клавиатурой В. Регулярная смена пароля Г. Блокировка экрана при уходе с рабочего места	
23.	ПК-4	Что такое электронная медицинская карта (ЭМК)? А. Текстовый файл на компьютере врача Б. Совокупность электронных данных о пациенте, структурированных в МИС В. Распечатка истории болезни Г. Фотография пациента в базе данных	Б
24.	ПК-4	Как часто рекомендуется менять пароли для доступа к МИС согласно политике безопасности? А. Никогда, если пароль сложный Б. Каждую неделю В. Каждые 3-6 месяцев Г. Только после увольнения сотрудника	В
25.	ПК-4	Какой федеральный закон регулирует отношения в сфере телемедицины в РФ? А. 152-ФЗ Б. 323-ФЗ В. 273-ФЗ Г. 44-ФЗ	Б
26.	ПК-4	Что такое "логи" в информационных системах? А. Пароли пользователей Б. Файлы, содержащие записи о событиях (входах, изменениях, ошибках) В. Программы для взлома Г. Антивирусные базы	Б
27.	ПК-4	Какой пароль считается наиболее надежным? А. Дата рождения Б. Имя ребенка В. Случайный набор букв разного регистра, цифр и символов Г. 123456	В
28.	ПК-4	Что такое двухфакторная аутентификация? А. Вход по двум разным паролям Б. Подтверждение входа с помощью второго устройства (например, СМС-код + пароль) В. Вход двумя пользователями одновременно Г. Двойной щелчок мыши	Б
29.	ПК-4	Кто несет персональную ответственность за разглашение врачебной тайны? А. Только главный врач Б. Только IT-отдел В. Непосредственно сотрудник, допустивший разглашение Г. Никто не несет	В
30.	ПК-4	Для чего предназначена система поддержки принятия врачебных решений (СППВР)? А. Для автоматической записи пациентов Б. Для помощи врачу в диагностике и выборе лечения В. Для расчета зарплаты Г. Для видеонаблюдения в палатах	Б

31.	ПК-4	Какое действие необходимо выполнить при уходе с рабочего места? А. Оставить компьютер включенным с открытой ЭМК Б. Заблокировать компьютер (Win+L) В. Выключить монитор, но оставить сеанс Г. Ничего не делать, если ушел на 5 минут	Б
32.	ПК-4	Что такое "бэкап" (backup)? А. Антивирусная программа Б. Резервное копирование данных В. Удаление вирусов Г. Настройка сети	Б
33.	ПК-4	Какие данные должны быть обязательно обезличены перед передачей исследователю? А. Диагноз Б. Назначенные лекарства В. ФИО и адрес пациента Г. Результаты анализов	В
34.	ПК-4	Что означает аббревиатура "МИС"? А. Международная информационная система Б. Медицинская информационная система В. Метод искусственного синтеза Г. Модуль идентификации сотрудника	Б
35.	ПК-4	Какое наказание предусмотрено за разглашение врачебной тайны по ст. 137 УК РФ? А. Только штраф Б. Только общественное порицание В. Вплоть до лишения свободы Г. Лишение медицинского сертификата	В
36.	ПК-4	Что такое "интеграция" медицинских систем? А. Установка нового компьютера Б. Обмен данными между различными системами (например, лабораторной и МИС) В. Отключение старой системы Г. Обучение персонала	Б
37.	ПК-4	Какой способ обмена информацией о пациенте является наиболее безопасным? А. Отправка на личную электронную почту Б. Передача через WhatsApp В. Использование защищенных каналов корпоративной МИС Г. Распечатка и передача через курьера без конверта	В
38.	ПК-4	Кто имеет право вносить изменения в электронную медицинскую карту? А. Любой сотрудник больницы Б. Только лечащий врач и уполномоченный медперсонал В. Пациент самостоятельно Г. IT-специалист	Б
39.	ПК-4	Что такое "телемониторинг"? А. Видеонаблюдение за пациентами Б. Дистанционное наблюдение за состоянием здоровья пациента с передачей данных В. Контроль за работой врачей через веб-камеру	Б

		Г. Запись на прием через интернет	
40.	ПК-4	Какой вирус наиболее опасен для медицинской организации? А. Рекламное ПО Б. Троян-шифровальщик, блокирующий доступ к данным В. Шпионское ПО Г. Браузерный червь	Б
41.	ПК-4	Что необходимо сделать при получении подозрительного письма с вложением от неизвестного отправителя? А. Открыть, чтобы проверить содержимое Б. Переслать коллегам для консультации В. Не открывать, сообщить в IT-отдел Г. Сохранить на рабочий стол	В
42.	ПК-4	Какую информацию пациент может получить через личный кабинет? А. Только результаты анализов за последний месяц Б. Полный доступ к редактированию своей карты В. Доступ к электронным медицинским документам, запись к врачу, сведения о полисе Г. Только запись к врачу	В
43.	ПК-4	Что такое "искусственный интеллект" в медицине? А. Робот, заменяющий врача Б. Система, анализирующая медицинские данные и помогающая в диагностике В. Программа для видеосвязи Г. Электронная очередь	Б
44.	ПК-4	Какие данные НЕ относятся к врачебной тайне? А. Факт обращения за медицинской помощью Б. Диагноз В. Паспортные данные пациента, переданные в страховую компанию для оплаты Г. Сведения о состоянии здоровья	В
45.	ПК-4	Как называется документ, который подтверждает согласие пациента на обработку его персональных данных в МИС? А. Договор о платных услугах Б. Информированное добровольное согласие В. Страховой полис Г. Рецепт	Б
46.	ПК-4	Что означает требование "целостности информации"? А. Информация доступна только авторизованным Б. Информация не была изменена или уничтожена без разрешения В. Информация доступна всегда Г. Информация подписана электронной подписью	Б
47.	ПК-4	Как часто должны проводиться инструктажи по информационной безопасности для сотрудников? А. Один раз при приеме на работу Б. Ежедневно В. Периодически (например, раз в год) и внепланово при инцидентах	В

		Г. Никогда, это личное дело каждого	
48.	ПК-4	Какой вид электронной подписи используется для подписания внутренних медицинских документов врачом? А. Простая Б. Усиленная неквалифицированная (УНЭП) В. Усиленная квалифицированная (УКЭП) для большинства юридически значимых действий Г. Факсимиле	В
49.	ПК-4	Что такое "облачные технологии" в здравоохранении? А. Хранение данных на компьютере в локальной сети Б. Удаленное использование серверов, программного обеспечения и баз данных через интернет В. Специальные программы для шифровки данных Г. Технологии хранения информации на внешних носителях	Б
50.	ПК-4	Кто должен утверждать политику информационной безопасности медицинской организации? А. Заведующий IT-отделом Б. Руководитель организации (главный врач) В. Министерство здравоохранения Г. Страховая компания	Б