федеральное государственное бюджетное образовательное учреждение высшего образования
«Кемеровский государственный медицинский университет»
Министерства здравоохранения Российской Федерации
(ФГБОУ ВО КемГМУ Минздрава России)

УТВЕРЖДАЮ:
Проректор по учебной работе
канд. биол. наук, доцент В.В. Большаков
«28» 03 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

Специальность	31.08.72 Стоматология общей практики
Квалификация выпускника	врач-стоматолог
Форма обучения	очная
Факультет	Управление последипломной подготовки специалистов
Кафедра-разработчик рабочей программы	Кафедра информационных технологий

Семестр	**Трудоемкость**		**Лекций, ч.**	**Лаб. практикум, ч.**	**Практ. занятий, ч.**	**Клинических практ. занятий, ч.**	**Семинаров, ч.**	**СРС, ч.**	**КР**	**Экзамен, ч**	**Форма промежуточного контроля (экзамен/ зачет с оценкой / зачет)**
	зач. ед.	ч.									
3	1	36	6		12			18			зачет
Итого	**1**	**36**	**6**		**12**			**18**			**зачет**

Кемерово 2025

Рабочая программа дисциплины «Информационные технологии и информационная безопасность в медицинской организации» разработана в соответствии с ФГОС ВО – подготовка кадров высшей квалификации по программам ординатуры по специальности 31.08.72 «Стоматология общей практики», утвержденным приказом Министерства образования и науки Российской Федерации № 19 от «09» января 2023 г. (рег. в Министерстве юстиции РФ № 72349 от 13.02.2023 г.).

Рабочую программу разработали:
доцент кафедры информационных технологий, к.филос.н., О.Г. Басалаева
доцент кафедры информационных технологий, к. ф.-м. н., доцент О.М. Колесников

Рабочая программа согласована с научной библиотекой _____Н.А. Окорокова
21 03 2025г.

Рабочая программа согласована с учебно-методической комиссией
Председатель: канд. мед. наук, доцент А.Н. Даниленко_____
протокол № 3 от «26» 03 2025 г.

Рабочая программа согласована с начальником УППС _____ к.м.н., доц. Л.К. Исаков
«27» 03 2025 г.

Рабочая программа зарегистрирована в учебно-методическом отделе
Регистрационный номер 3241
Руководитель УМО д.ф.н., профессор _____ Н.Э. Коломиец

«28» 03 2025 г.

ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ

1.1. Цели и задачи освоения дисциплины

1.1.1. Цель освоения дисциплины «Информационные технологии и информационная безопасность в медицинской организации» - закрепление теоретических знаний, развитие практических умений и навыков по использованию информационных технологий, с соблюдением правил информационной безопасности, необходимых для решения профессиональных задач врача-специалиста.

1.1.2. Задачи дисциплины: формирование знаний нормативных документов в области информационной безопасности и основ информационной безопасности, совершенствование умений по работе с информацией и медицинскими информационными системами, развитие навыков информационного поиска и участия в онлайн-мероприятиях для решения образовательных задач.

1.2. Место дисциплины в структуре ОПОП ВО

1.2.1. Дисциплина «Информационные технологии и информационная безопасность в медицинской организации» относится к факультативной дисциплине.

1.2.2. Для изучения дисциплины необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: Медицинская информатика, Общественное здоровье и здравоохранение.

1.2.3. Изучение дисциплины необходимо для получения знаний, умений и навыков, формируемых последующими дисциплинами/практиками: Общественное здоровье и здравоохранение.

1.2.4. В основе преподавания данной дисциплины лежат следующие типы профессиональной деятельности:

1. организацинно-управленческая

1.2.5. В основе освоения данной дисциплины лежат следующие виды профессиональной деятельности:

1. здравоохранение (в сфере стоматологии общей практики).
2. Административно-управленческая и офисная деятельность (в сфере здравоохранения).

1.3. Компетенции, формируемые в результате освоения дисциплины
1.3.2. Общепрофессиональные компетенции

№ п/п	Наименование категории общепрофессиональных компетенций	Код компетенции	Содержание компетенции	Индикаторы универсальных компетенции	Технология формирования
1	Информационная грамотность	ОПК-1	Способен использовать информационно-коммуникационные технологии в профессиональной деятельности и соблюдать правила информационной безопасности	ОПК-1.1. Знает и понимает основные нормативные документы в области информационной безопасности ОПК-1.2. Знает и понимает основы информационной безопасности ОПК-1.3. Умеет работать с информацией и информационно-коммуникационными системами ОПК-1.4. Умеет осуществлять информационный поиск и обучение с использованием информационно-коммуникационных технологий	Лекции Практические занятия Самостоятельная работа Работа в МИС и онлайн-сервисах, программах телемедицины и видеоконференций.

1.3. Объем учебной дисциплины и виды учебной работы

Вид учебной работы		Трудоемкость, всего		Семестры	
		в зачетных единицах (ЗЕ)	в академи-ческих часах (ч)	**2**	**3**
				Трудоемкость по семестрам (ч)	
Аудиторная работа, в том числе:			18		18
Лекции (Л)		0,17	6		6
Лабораторные практикумы (ЛП)					
Практические занятия (ПЗ)		0,33	12		12
Клинические практические занятия (КПЗ)					
Семинары (С)					
Самостоятельная работа студента (СРС), в том числе НИРС		0,5	18		18
Промежуточная аттестация:	зачет (З)				
ИТОГО		1	36		36

2. Структура и содержание дисциплины

Общая трудоемкость модуля дисциплины составляет 1 зачетную единицу, 36 ч.

2.1. Структура дисциплины

№ п/п	Наименование разделов и тем	Семестр	Всего часов	Виды учебной работы					СРС
				Аудиторные часы					
				Л	ЛП	ПЗ	КПЗ	С	
1	**Раздел 1** (Информационная безопасность и защита информации)	3	20	4		4			12
2	**Раздел 2** (Стратегии работы с медицинской информацией)	3	16	2		8			6
2	Зачёт	3							
	Итого		36	6		12			18

2.2. Тематический план лекционных занятий

№ п/п	Наименование раздела, тема практического занятия	Кол-во часов	Семестр	Результат обучения в виде формируемых компетенций
Раздел 1. Информационная безопасность и защита информации				ОПК-1 ИД-1 ОПК-1 ИД-2 ОПК-1
1	**Тема 1.** Нормативно-правовое регулирование информационной безопасности и защиты информации	*2*	*3*	
2	**Тема 2.** Обеспечение информационной безопасности и защиты информации	*2*	*3*	
Раздел 2. Стратегии работы с медицинской информацией				ОПК-1 ИД-4 ОПК-1
1	**Тема 4.** Стратегии поиска медицинской информации	*2*	*3*	
	Итого:	6		

2.3. Тематический план практических занятий

№ п/п	Наименование раздела, тема занятия	Вид занятия (ПЗ, С, КПЗ, ЛП)	Кол-во часов		Семестр	Результат обучения в виде формируемых компетенций
			Аудитор.	СРС		
Раздел 1. Информационная безопасность и защита информации		ПЗ	4	12	3	ОПК-1 ИД-1 ОПК-1 ИД-2 ОПК-1
1	**Тема 1.** Нормативно-правовое регулирование информационной безопасности и защиты информации	ПЗ	2	6	3	
2	**Тема 2.** Обеспечение информационной безопасности и защиты информации	ПЗ	2	6	3	
Раздел 2. Стратегии работы с медицинской информацией		ПЗ	8	6	3	ОПК-1 ИД-3 ОПК-1 ИД-4 ОПК-1
13	**Тема 3.** Функциональные возможности медицинских информационных систем	ПЗ	6	4	3	
14	**Тема 4.** Стратегии поиска медицинской информации	ПЗ	2	2	3	
Итого:			12	18		

2.4 Содержание дисциплины

РАЗДЕЛ 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Тема 1. Нормативно-правовое регулирование информационной безопасности и защиты информации

Содержание темы:

1. Информационная безопасность в системе национальной безопасности РФ.
2. Уголовный кодекс РФ (глава «Преступления в сфере компьютерной информации»).
3. Доктрина информационной безопасности РФ.
4. Основные нормативно-правовые документы в области информационной безопасности и защиты данных.
5. Основные термины и определения правовых понятий в области информационных отношений и защиты информации.
6. *Практическая работа №1 «Формирование терминологического словаря на основе проанализированных основных нормативно-правовых документов в области информационной безопасности и защиты данных».*

Форма контроля и отчетности усвоения материала: конспект лекции, тесты, практическое задание №1.

Использование электронного обучения и дистанционных образовательных технологий: Не предполагается.

Тема 2. Обеспечение информационной безопасности и защиты информации

Содержание темы:

1. Основные свойства защищаемой информации.
2. Угрозы информационной безопасности.
3. Методы защиты от несанкционированного доступа к информации.
4. Субъекты и объекты доступа к информации.
1. *Практическая работа №2 «Формирование перечня конкретных организационных и технических мер обеспечения информационной безопасности и защиты данных медицинской организации».*

Форма контроля и отчетности усвоения материала: конспект лекции, тесты, практическое задание №2.

Использование электронного обучения и дистанционных образовательных технологий: Не предполагается.

Тема 3. Функциональные возможности медицинских информационных систем

Содержание темы:

1. Использование возможностей МИС в соответствии с установленными правилами и политиками безопасности.
2. Правила доступа к МИС и система разграничения прав пользователей.
3. Конфиденциальность и целостность информации, хранящейся в МИС.
4. Правила информационной безопасности при ведении электронной медицинской карты пациента.
5. Соблюдение требований информационной безопасности при работе с системами поддержки принятия врачебных решений.
6. *Практическая работа №3 «Освоение правил информационной безопасности при работе в медицинской информационной системе (МИС».*

Форма контроля и отчетности усвоения материала: тесты, практическое задание №3.

Использование электронного обучения и дистанционных образовательных технологий:
Не предполагается.

Тема 4. Стратегии поиска медицинской информации

Содержание темы:

1. Определение информационного поиска и информационно-поисковой системы.
2. Правила формирования информационного запроса.
3. Виды информационного поиска.
4. Универсальные поисковые системы интернет.
5. Поисковые системы электронных библиотек.
6. Достоверные источники медицинской информации.
7. Этапы и технологии информационного поиска в базах данных доказательной медицины.
8. *Практическая работа №4 «Формирование списка статей или клинических рекомендаций в базах данных PubMed, Cochrane Library.».*

Форма контроля и отчетности усвоения материала: тесты, практическое задание №4.

Использование электронного обучения и дистанционных образовательных технологий:
Не предполагается.

2.5 Учебно-методическое обеспечение самостоятельной работы

Наименование раздела, тема	Вид самостоятельной работы обучающегося (аудиторной и внеаудиторной)	Кол-во часов	Семестр
РАЗДЕЛ 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ		***12***	***3***
Тема 1. Нормативно-правовое регулирование информационной безопасности и защиты информации	Изучение учебной литературы. Изучение нормативных документов. Разработка «Политики информационной безопасности медицинской организации». Подготовка к текущему контролю.	*6*	*3*
Тема 2. Обеспечение информационной безопасности и защиты информации	Изучение учебной литературы. Изучение нормативных документов. Разработка «Политики информационной безопасности медицинской организации». Подготовка к текущему контролю.	*6*	*3*
РАЗДЕЛ 2. СТРАТЕГИИ РАБОТЫ С МЕДИЦИНСКОЙ ИНФОРМАЦИЕЙ		***6***	***3***
Тема 3. Функциональные возможности медицинских информационных систем	Изучение учебной литературы. Изучение инструктивных документов по работе с МИС. Подготовка к текущему контролю.	*4*	*3*
Тема 4. Стратегии информационного поиска медицинской информации	Изучение учебной литературы. Изучение инструктивных документов по работе с PubMed, Cochrane Library. Знакомство с сайтами Минздрава России, профессиональных ассоциаций; онлайн-платформами для непрерывного медицинского образования (НМО). Участие в онлайн-конференциях и	*2*	*3*

Наименование раздела, тема	Вид самостоятельной работы обучающегося (аудиторной и внеаудиторной)	Кол-во часов	Семестр
	вебинарах. Подготовка к текущему контролю.		
	Всего:	***18***	

3. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

3.1. Занятия, проводимые в интерактивной форме

№ п/п	Наименование раздела дисциплины	Вид учебных занятий	Кол-во час	Формы интерактивного обучения	Кол-во час
1	***РАЗДЕЛ 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ***		*4*		
2	**Тема 2.** Обеспечение информационной безопасности и защиты информации	*Практическое занятие*	2	*Кейс метод*	*2*
3	***РАЗДЕЛ 2. СТРАТЕГИИ РАБОТЫ С МЕДИЦИНСКОЙ ИНФОРМАЦИЕЙ***		*8*		
4	**Тема 4.** Стратегии информационного поиска медицинской информации	*Практическое занятие*	*2*	*Работа в малых группах*	*2*
	Итого:		*12*		*4*

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Контрольно-диагностические материалы для промежуточной аттестации.
Зачет проводится в виде письменного опроса.

4.2. Оценочные средства (представлены в приложении 1)

4.3. Критерии оценки по дисциплине в целом

Характеристика ответа	Оценка ECTS	Баллы в РС	Оценка итоговая
Дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи. Знания об объекте демонстрируются на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ формулируется в терминах науки, изложен литературным языком, логичен,	A -B	100-91	5

доказателен, демонстрирует авторскую позицию студента. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа.			
Дан полный, развернутый ответ на поставленный вопрос, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Ответ изложен литературным языком в терминах науки. В ответе допущены недочеты, исправленные студентом с помощью преподавателя.	C-D	90-81	4
Дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. Студент может конкретизировать обобщенные знания, доказав на примерах их основные положения только с помощью преподавателя. Речевое оформление требует поправок, коррекции.	E	80-71	3
Дан неполный ответ, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, теорий, явлений, вследствие непонимания студентом их существенных и несущественных признаков и связей. В ответе отсутствуют выводы. Умение раскрыть конкретные проявления обобщенных знаний не показано. Речевое оформление требует поправок, коррекции.	Fx- F	<70	2 Требуется пересдача / повторное изучение материала

5. ИНФОРМАЦИОННОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Информационное обеспечение дисциплины

№ п/п	Наименование и краткая характеристика библиотечно-информационных ресурсов и средств обеспечения образовательного процесса, в том числе электронно-библиотечных систем (ЭБС) и электронных образовательных ресурсов (электронных изданий и информационных баз данных)
1	ЭБС «Консультант Студента» : сайт / ООО «КОНСУЛЬТАНТ СТУДЕНТА». – Москва, 2013-2025. - URL: https://www.studentlibrary.ru. - Режим доступа: по IP-адресу университета, удаленный доступ по логину и паролю. - Текст : электронный.
2	Справочно-информационная система «MedBaseGeotar» : сайт / ООО «КОНСУЛЬТАНТ СТУДЕНТА». – Москва, 2024-2025. – URL: https://mbasegeotar.ru - Режим доступа: по IP-адресу университета, удаленный доступ по логину и паролю. - Текст : электронный.
3	Электронная библиотечная система «Медицинская библиотека «MEDLIB.RU» (ЭБС «MEDLIB.RU») : сайт / ООО «Медицинское информационное агентство». - Москва, 2016-2025. - URL: https://www.medlib.ru. - Режим доступа: по IP-адресу университета, удаленный доступ по логину и паролю. - Текст : электронный.
4	«Электронная библиотечная система «Букап» : сайт / ООО «Букап». - Томск, 2012-2025. - URL: https://www.books-up.ru. - Режим доступа: по IP-адресу университета, удаленный доступ по логину и паролю. - Текст : электронный.
5	«Электронные издания» издательства «Лаборатория знаний» / ООО «Лаборатория знаний». - Москва, 2015-2025. - URL: https://moodle.kemsma.ru. – Режим доступа: по логину и паролю. - Текст : электронный.

6	База данных ЭБС «ЛАНЬ» : сайт / ООО «ЭБС ЛАНЬ» - СПб., 2017-2025. - URL:https://.e.lanbook.com. - Режим доступа: по IP-адресу университета, удаленный доступ по логину и паролю. - Текст : электронный.
7	«Образовательная платформа ЮРАЙТ» : сайт / ООО «ЭЛЕКТРОННОЕ ИЗДАТЕЛЬСТВО ЮРАЙТ». - Москва, 2013-2025. - URL: https://urait.ru. - Режим доступа: по IP-адресу университета, удаленный доступ по логину и паролю. – Текст : электронный.
8	«JAYPEE DIGITAL» (Индия) - комплексная интегрированная платформа медицинских ресурсов : сайт - URL: https://www.jaypeedigital.com/ - Режим доступа: по IP-адресу университета, удаленный доступ по логину и паролю. - Текст : электронный.
9	Информационно-справочная система «КОДЕКС»: код ИСС 89781 «Медицина и здравоохранение»: сайт / ООО «ГК «Кодекс». - СПб., 2016 -2025. - URL: http://kod.kodeks.ru/docs. - Режим доступа: по IP-адресу университета, удаленный доступ по логину и паролю. - Текст : электронный.
10	Электронная библиотека КемГМУ (Свидетельство о государственной регистрации базы данных № 2017621006 от 06.09. 2017 г.). - Кемерово, 2017-2025. - URL: http://www.moodle.kemsma.ru. - Режим доступа: по логину и паролю. - Текст : электронный.
	Интернет-ресурсы:
	Компьютерные презентации:
	Электронные версии конспектов лекций:
	Учебные фильмы:

5.2. Учебно-методическое обеспечение дисциплины

№ п/п	Библиографическое описание рекомендуемого источника литературы
	Основная литература
1	Баланов, А. Н. Защита информационных систем. Кибербезопасность: учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург: Лань, 2025. — 280 с. // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/438971. – Текст: электронный.
2	Зенков, А. В. Информационная безопасность и защита информации: учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 107 с. — (Высшее образование) // ЭБС «Образовательная платформа «Юрайт». - URL: https://urait.ru . - Режим доступа: по IP-адресу университета, удаленный доступ по логину и паролю. – Текст : электронный.
6	Медицинские информационные системы: учебное пособие / Т. Г. Авачева, М. Н. Дмитриева, Н. В. Дорошина [и др.]. — Рязань: РязГМУ, 2019. — 132 с. // Лань : электронно-библиотечная система. - URL: http://www.e.lanbook.com. - Режим доступа: по IP-адресу университета, удаленный доступ по логину и паролю. - Текст : электронный.
5	Омельченко, В. П. Информационные технологии в профессиональной деятельности : учебник / В. П. Омельченко, А. А. Демидова. –Москва: ГЭОТАР-Медиа, 2024. – 416 с. // ЭБС «Консультант студента». – URL: htpps://www.studentlibrary.ru. – Режим доступа: по IP-адресу университета, удаленный доступ по логину и паролю. –Текст : электронный.
3	Суворова, Г. М. Информационная безопасность: учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 277 с. // ЭБС «Образовательная платформа «Юрайт». — URL: https://urait.ru. — Режим доступа: по IP-адресу университета, удаленный доступ по логину и паролю. – Текст : электронный.
4	Хрипунова, А. А. Информационные технологии в медицине и здравоохранении: учебно-методическое пособие / А. А. Хрипунова, Е. В. Максименко. – Ставрополь: СтГМУ, 2021. – 88 с. // Лань: электронно-библиотечная система. - URL: http://www.e.lanbook.com. – Режим доступа: по IP-адресу университета, удаленный доступ по логину и паролю. –Текст :

№ п/п	Библиографическое описание рекомендуемого источника литературы
	электронный.
	Дополнительная литература
1	Ермакова, А. Ю. Методы и средства криптографической защиты информации: учебное пособие / А. Ю. Ермакова, В. В. Лебедев. — Москва: РТУ МИРЭА, 2024. — 230 с. // Лань: электронно-библиотечная система. - URL: http://www.e.lanbook.com. – Режим доступа: по IP-адресу университета, удаленный доступ по логину и паролю. – Текст: электронный.

5.3. Методические разработки кафедры

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения: учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещение для самостоятельной работы, помещение для хранения и профилактического обслуживания учебного оборудования

Основное оборудование: доски, столы, стулья

Технические средства: мультимедийный комплекс (ноутбук, проектор, экран), аудиоколонки, ноутбуки с выходом в интернет, принтер, наборы мультимедийных презентаций, таблицы, схемы, компьютер с выходом в Интернет для обеспечения доступа к электронной информационно - образовательной среде КемГМУ, принтер.

Оценочные средства на печатной основе: тестовые задания по изучаемым темам, ситуационные задачи.

Учебные материалы: учебники, учебные пособия, раздаточные дидактические материалы.

Программное обеспечение:

Microsoft Windows 7 Professional
Microsoft Office 10 Standard
Microsoft Windows 8.1 Professional
Microsoft Office 13 Standard
Linux лицензия GNUGPL
LibreOffice лицензия GNU LGPLv3
Антивирус Dr.Web Security Space
Kaspersky Endpoint Security Russian Edition для бизнеса.

Приложение 1

Оценочные средства

Список вопросов для подготовки к зачету (*в полном объеме*):

1. Виды и основные свойства защищаемой информации
2. Уровни правовой защиты информации
3. Значение информационной безопасности в системе национальной безопасности РФ
4. Основное содержание Доктрины информационной безопасности РФ
5. Понятие информационной безопасности
6. Конфиденциальность информации, как ограничение доступа к информации
7. Угроза информационной безопасности
8. Программные и аппаратные средства защиты информации
9. Организационно-технические решения, предназначенные для предотвращения атак, контроля доступа и мониторинга информационных процессов
10. Несанкционированный доступ к информации, его место в проблеме информационной безопасности
11. Вирусы и антивирусные программы
12. Политика информационной безопасности медицинской организации
13. Определение и классификация медицинских информационных систем
14. Автоматизированные системы консультативной помощи в принятии врачебных решений и медицинские информационные справочные системы
15. Автоматизированное рабочее место врача (АРМ). Основные виды АРМ и их особенности
16. Авторизация, идентификация и аутентификация пользователей в медицинских информационных системах
17. Информационные системы отделений медицинских учреждений
18. Защита информации в медицинских информационных системах
19. Система ведения электронной медицинской карты
20. Функциональные возможности медицинских информационных систем
21. Информационный поиск в медицинских базах данных
22. Онлайн-платформы для непрерывного медицинского образования

Тестовые задания *(пример)*:

Инструкция: выберите один правильный вариант ответа.

Потенциальные угрозы, против которых направлены технические меры защиты информации …

А потери информации из-за халатности обслуживающего персонала

Б потери информации из-за не достаточной установки резервных систем электропитании и оснащение помещений замками

В процессы преобразования, при котором информация удаляется

Г потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей

Ответ: **Г**

По доступности информация классифицируется на …

А открытую информацию и государственную тайну

Б конфиденциальную информацию и информацию свободного доступа

В информацию с ограниченным доступом и общедоступную информацию

Г противозаконную и официальную информацию

Ответ: **В**

Ситуационные задачи *(пример)*:

1) Для работы в личном кабинете электронной образовательной среды вуза необходимо придумать персональный пароль. Вам предложили, чтобы его не забыть, пароль составить из даты рождения и имени студента. Какие правила обеспечения информационной безопасности нарушены?

Решение:

Запрещается использовать в качестве пароля «пустой» пароль, имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

2) Вы являетесь сотрудником медицинского учреждения, использующего комплексную медицинскую информационную систему (МИС). Вам необходимо получить письменное согласие пациента на обработку его персональных данных. Пациент высказывает опасения по поводу безопасности хранения медицинской информации о нем в электронном виде. Какими аргументами Вы можете убедить пациента, что хранить информацию о пациенте в электронном виде безопаснее, чем в бумажном? Опишите, какие механизмы защиты персональных медицинских данных о пациенте реализованы в МИС?

Решение:

Похитить данные из МИС без наличия прав доступа к ним технически очень сложно и затратно, так как сервер, на котором находятся данные, как правило, хорошо охраняется. К бумажному документу непосредственный, хоть и не санкционированный, доступ осуществить гораздо легче. Кроме при повреждении бумажного документа, данные зачастую невозможно восстановить, а электронные данные обычно имеют резервную копию или распределенное хранение и имеют больше возможностей для восстановления.

Система прав доступа. Системы идентификации и аутентификации пациента. Система логирования (журналирования) доступа работников к данным. Ограничение физического доступа к серверу и рабочим станциям несанкционированных лиц. Ограничение количества и защита каналов связи с внешними системами.

Перечень практических заданий *(полный перечень)*

Практическая работа №1 «Формирование терминологического словаря на основе проанализированных основных нормативно-правовых документов в области информационной безопасности и защиты данных».

Задание 1. Изучить нормативные документы в сфере информационной безопасности и защиты информации:

Доктрина информационной безопасности РФ. Указ Президента РФ № 646 от 05.12.2016 "Об утверждении Доктрины информационной безопасности Российской Федерации"

Федеральный закон "Об информации, информационных технологиях и о защите информации" № 149-ФЗ от 27.07.2006

Федеральный закон "О персональных данных" № 152-ФЗ от 27.07.2006

Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" № 187-ФЗ от 26.07.2017

Сформировать терминологический словарь на основе проанализированных основных нормативно-правовых документов.

Задание 2. Подготовить сообщения по следующим вопросам:

Современное состояние информационной безопасности как составной части национальной безопасности Российской Федерации.

Основные принципы государственной политики и правовые отношения в информационной сфере согласно Доктрине информационной безопасности Российской Федерации.

Угрозы информационной безопасности и методы защиты информации.

Объекты критической информационной инфраструктуры.

Оператор персональных данных и их защита.

Проблемы защиты персональных данных в интернете.

Правовые аспекты применения электронной цифровой подписи.

Результат выполнения 2-го задания: сообщения по вопросам о информационной безопасности и защите информации.

Практическая работа №2 «Формирование перечня конкретных организационных и технических мер обеспечения информационной безопасности и защиты данных медицинской организации».
Задания описаны в кейсе «Комплексный подход к организации информационной безопасности» (см. далее).

Практическая работа №3 «Освоение правил информационной безопасности при работе в медицинской информационной системе (МИС)»
Задания описаны в кейсе «Соблюдение требований законодательства Российской Федерации о защите персональных данных» (см. далее).

Практическая работа №4 «Формирование списка статей или клинических рекомендаций в базах данных PubMed, Cochrane Library»

Задание 1. Найти не менее 10 достоверных источников доказательной медицинской информации по заданной теме. Номер темы соответствует порядковому номеру студента в журнале.

В качестве достоверных источников принимаются научные статьи или нормативные документы, найденные в Интернете на профильных сайтах ИАС Scopus, WoS, E-library, PubMed, Кокрейновской библиотеки, а также из перечня ресурсов, рекомендуемых университетской библиотекой.

Для этого: **з**апустить поиск в PubMed.

Осуществить поиск с помощью фильтров: по типу статьи, доступности текста, дате публикации, виду, языку, полу, теме, категории журнала и возрасту.

Чтобы применить фильтры к вашему поиску, щелкните фильтр на боковой панели.

При выборе фильтров на странице результатов появится сообщение "Filters applied".

Нажмите на примененный фильтр, чтобы отключить его.

Чтобы отключить все примененные фильтры, нажмите ссылку "Clear all" или кнопку "Reset all filters".

Результат: Найденные источники необходимо оформить в виде библиографического списка цитирований в соответствии с ГОСТ. В конце библиографической ссылки необходимо добавить ссылку на электронный ресурс, например, «URL: http://cyberleninka.ru/article/n/ bazisnye-printsipy-i-metodologiya-dokazatelnoy-meditsiny.pdf (дата обращения: 05.02.2025)»

Тестовые задания (*текущий контроль*):
Правильный ответ выделен полужирным

1. В какой форме может быть оказана телемедицинская услуга…
   а) в форме телемедицинской консультации и/или телемедицинского консилиума, а также в иных формах, предусмотренных федеральным законодательством
   б) только в форме телемедицинского консилиума
   в) только в форме телемедицинской консультации

2. Интернет вещей – это**…**
   а) покупка товаров через интернет

б) ***вид цифровых технологий***
в) передача вещей между пользователями

3. Дайте определение понятия "персональные данные". Какие основные принципы обработки персональных данных установлены законодательством?

Ответ: Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Основные принципы: законность, справедливость, конфиденциальность, точность, достаточность, целесообразность, хранение не дольше необходимого срока.

4. При проведении телемедицинских консультаций используется такой термин, как «телематика». Опишите, что понимается под этим термином.

Ответ: телематика - это соединение телекоммуникаций (включающее телефонную и другие виды связи) и информатики (различных компьютерных систем);
медицинская телематика включает услуги и системы, связанные с оказанием медицинской помощи на расстоянии посредством информационно-коммуникационных технологий

5. Электронная медицинская карта (ЭМК) и искусственный интеллект связаны между собой. Опишите, каким образом происходит эта взаимосвязь.

Ответ: использование распознавания голоса и разговорного искусственного интеллекта (ИИ) для помощи врачам во вводе информации в электронную медицинскую карту; объединение, анализ и обновление данных из электронной медицинской карты пациента

6. Укажите, какую информацию о сотруднике медицинского учреждения необходимо размещать на сайте.

Ваш ответ: ……

Эталонный ответ: ФИО, точное название должности, график приема и порядок записи на диагностику (консультацию, прием); сведения об образовании/сертификации.

7. При проведении телемедицинских консультаций используется такой термин, как «телематика». Опишите, что понимается под этим термином.

Ваш ответ: ……

Примерный ответ: область информатики, охватывающая сферу телекоммуникаций

8. При проведении телемедицинской консультации врач-консультант запросил у лечащего врача рентгенограмму. Опишите, к какому виду медицинской информации относится рентгенограмма и как врач-консультант может её получить.

Ваш ответ: ……

Примерный ответ: Рентгенограмма – это графическое изображение снимка внутренних органов, полученного в результате просвечивания рентгеновским излучением. Может храниться на пленке или в цифровом формате. Программное обеспечение телемедицинских консультаций позволяет лечащему врачу удаленно загружать в систему рентгенограмму и другие результаты исследования пациента. Врач-консультант со своей стороны (в этой же системе) может ознакомиться с ними в полном объеме.

9. Опишите какие требования обязательны для электронного медицинского документа, заполняемого в медицинском учреждении.

Ваш ответ: ……

Примерный ответ: Образ электронного медицинского документа должен содержать:
а) наименование медицинской организации и ее адрес;
б) персональные данные гражданина, являющегося получателем медицинской услуги;

в) текст электронного медицинского документа;
г) дату составления электронного медицинского документа

10. Фишинг -

а) **Вид интернет-мошенничества с целью получения конфиденциальных данных**
б) Вид компьютерного вируса
в) Способ взлома веб-сайта
г) Метод защиты информации

11. Перечислите основные угрозы информационной безопасности.

Ответ: Угрозы: несанкционированный доступ, вредоносное ПО, утечка информации, нарушение целостности данных, отказ в обслуживании, социальная инженерия.

12. Приведите примеры конкретных атак, использующих эти угрозы.

Ответ: Примеры: Несанкционированный доступ: подбор пароля. Вредоносное ПО: заражение вирусом. Утечка: кража данных из базы. Нарушение целостности: случайное удаление файла. DoS: перегрузка сервера запросами. Социальная инженерия: фишинговое письмо.

13. Телемедицинские технологии - это …

а) комплекс средств и методов дистанционного оказания медицинской помощи, реализуемой с применением телекоммуникационных систем
б) современный способ доставки медицинской информации
в) способ разработки информационных систем, основанных на применении высокотехнологичной медицинской помощи

14. Перечислите основные угрозы информационной безопасности.

Ответ: Угрозы: несанкционированный доступ, вредоносное ПО, утечка информации, нарушение целостности данных, отказ в обслуживании, социальная инженерия.

15. Приведите примеры конкретных атак, использующих эти угрозы.

Ответ: Примеры: Несанкционированный доступ: подбор пароля. Вредоносное ПО: заражение вирусом. Утечка: кража данных из базы. Нарушение целостности: случайное удаление файла.DoS: перегрузка сервера запросами. Социальная инженерия: фишинговое письмо.

16. Сформулируйте основную цель формирования единой государственной информационной системы здравоохранения.

Ответ: цель - повышение уровня качества и доступности медицинских услуг за счёт цифровизации и объединения всех данных в единую систему

17. Сформулируйте базовые функции экспертных информационных медицинских систем.

Ответ: 1) приобретение знаний; 2) представление знаний; 3) управление процессом поиска решения; 4) разъяснение принятого решения

18. Охарактеризуйте, возможные угрозы и риски применения искусственного интеллекта (ИИ) в практической медицине.

Ответ: ИИ может принимать неправильные решения, связанные с: 1) искажением первичных медицинских знаний; 2) отсутствием знаний или недостоверными знаниями о предметной области; 3) проблемами с ответственностью; 4) нарушением этики при сборе данных; 5) риском монополизации и использования ИИ; 6) недостаточным количеством и качеством медицинских данных

19. При создании информационной медицинской системы (МИС) необходимо ориентироваться на интероперабельность для нормального функционирования МИС.

Напишите, что подразумевается под данным термином и для чего нужна интероперабельность.

Ваш ответ: ……

Примерный ответ: Интероперабельность -это способность программного продукта или системы взаимодействовать и функционировать с другими программными продуктами или системами. Интероперабельность МИС нужна для интегрирования в нее уже существующих разнородных систем и накопленных в них данных.

20. Существуют различные виды медицинской информации: звуковая, визуальная, статистическая, текстовая. Опишите, к какому виду медицинской информации относится история болезни, описываемая в электронной медицинской карте (ЭМК).

Ваш ответ: ……

Примерный ответ: История болезни относится к текстовой информации. Результаты исследований могут быть мультимедийны.

21. В телемедицине используется такое определение, как автоматизированный скрининг. Дайте определение данному термину и опишите каким образом он реализуется.

Ваш ответ: ……

Примерный ответ: Это автоматизированный предварительный медицинский осмотр. Реализуется как компьютерная программа, интегрированная в базу данных о пациентах, которая генерирует рекомендации, специфические для конкретного пациента. Данная информация служит поддержкой для принятия решений врачу при планировании телемедицинской консультации пациента.

22. Электронная медицинская карта (ЭМК) и система принятия врачебных решений на основе искусственного интеллекта связаны между собой. Опишите, каким образом происходит эта взаимосвязь в процессе постановки диагноза.

Ваш ответ: ……

Примерный ответ: В процессе постановки диагноза данные ЭМК конкретного пациента являются входными для системы ИИ, обученной на огромном количестве аналогичных данных других пациентов, которым диагноз уже поставлен и подтвержден врачом. На выходе система ИИ предлагает врачу наиболее вероятный диагноз для данного пациента.

23. Каким образом интеллектуальная система поддержки принятия врачебных решений позволяет поставить диагноз. Напишите, что запрашивает система у врача и что она проверяет в своей базе знаний.

Ваш ответ: ……

Примерный ответ: Система запрашивает данные анамнеза и результаты исследований пациента. Система проверяет полученные сведения на предмет совпадений, ищет в базе знаний кейс, наиболее подходящий к данному случаю, и выдает предварительное заключение (варианты диагноза со степенью их вероятности).

24. Сформулируйте определение инфраструктуры информационной системы.

Ваш ответ: ……

Эталонный ответ: инфраструктура ИС – это совокупность базовых технологических компонент: вычислительных систем, систем хранения и передачи данных, являющаяся основой для функционирования любых информационных сервисов.

25. Перечислите основные виды информационных ресурсов медицинских информационных систем.

Ваш ответ: ……

Эталонный ответ: Интегрированная электронная медицинская карта. Персональная медицинская карта. Электронный рецепт. Регистровая платформа. Индекс пациентов. Нормативно-справочная информация.

26. Перечислите основные виды удаленных информационных сервисов медицинских информационных систем.

Ваш ответ: ……

Эталонный ответ: Запись на прием к врачу. Обмен данными лабораторных и инструментальных исследований. Телемедицинские консультации. Мониторинг пациентов. Запись на медицинские осмотры (диспансеризацию). Вызов врача на дом. Сервис оповещения участковых врачей.

27. Приведите функциональную классификацию медицинских информационных систем.

Ваш ответ: ……

Эталонный ответ: 1. Медико-технологические ИС (МТИС). 2. Информационно-справочные системы (ИСС). 3. Статистические ИС (СМИС) органов управления здравоохранением. 4. Научно-исследовательские ИС (НИИС). 5. Обучающие ИС (ОМИС).

28. Перечислите основные виды обеспечения информационной системы.

Ваш ответ: ……

Эталонный ответ: материально-техническое и коммуникационное, программное, информационное, организационное, правовое.

29. Перечислите основные приоритетные направления внедрения информационных систем в здравоохранении.

Ваш ответ: ……

Эталонный ответ: создание единого цифрового контура здравоохранения на базе ЕГИСЗ: мониторинг здоровья населения, информационная поддержка программ борьбы с социально-значимыми заболеваниями, информатизация органов управления здравоохранением, оптимизация использования ресурсов здравоохранения.

30. Перечислите базовые элементы медицинской информационной системы.

Ваш ответ: ……

Эталонный ответ: коммуникационная инфраструктура, клиент-серверное оборудование, клиент-серверное ПО, медицинские базы данных.

Кейс «Соблюдение требований законодательства Российской Федерации о защите персональных данных»

Цель:

Оценка знаний обучающихся по основным аспектам защиты персональных данных, в том числе, общие требования: при обработке персональных данных и гарантии защиты, при хранении, использовании и передаче персональных данных; права граждан в целях обеспечения защиты персональных данных; ответственность за нарушение норм, регулирующих обработку и защиту персональных данных.

Контекст:

Стоматологическая клиника проводила рекламную акцию, в рамках которой собирала у пользователей персональные данные (имя, номер телефона, адрес электронной почты) для рассылки новостей и актуальных акций. После окончания рекламной акции стоматологическая клиника решила использовать эти данные для массовой рассылки рекламных сообщений по e-mail, не используя функцию «скрытая копия» и не получив от пользователей явного согласия на такую обработку.

Задания:

1) Изучите статьи Федерального закона № 152-ФЗ «О персональных данных»

2) Определите какие нормы Федерального закона № 152-ФЗ «О персональных данных» были нарушены

3) Оцените ответственность организации за нарушение закона о защите персональных данных

4) Сформулируйте меры, которые стоматологическая клиника должна предпринять для устранения нарушений и предупреждения аналогичных ситуаций в дальнейшем

5) Опишите ошибки стоматологической клиники

Предоставленные материалы:

Федеральный закон № 152-ФЗ «О персональных данных» в актуальной редакции

Приказ Минздрава России № 911н «Об утверждении Требований к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных медицинских организаций»

Эталоны ответов:

Нормы Федерального закона № 152-ФЗ «О персональных данных», которые были нарушены:

Статья 7 Федерального закона № 152-ФЗ устанавливает обязанность оператора обеспечивать защиту персональных данных от неправомерного или случайного доступа третьих лиц; в данной ситуации, сбор и обработка данных осуществлялись без явного согласия субъектов персональных данных, что является нарушением принципа законности.

Статья 8 запрещает передачу персональных данных третьим лицам без предварительного согласия субъекта персональных данных, кроме случаев, прямо указанных в законе; в данной ситуации, адреса e-mail были переданы третьим лицам.

Статья 9 регламентирует получение согласия субъекта персональных данных на обработку, если такая обработка не предусмотрена законом или не является необходимой для исполнения договора; в данной ситуации, клиника не получила согласия на использование данных для рассылки рекламных материалов после окончания акции

Статья 18 требует соблюдения принципов прозрачности и правомерности обработки персональных данных, включая уведомление субъектов данных о цели сбора и способах обработки; в данной ситуации, использование данных в целях, не согласованных с пользователями, может считаться нарушением конфиденциальности.

Ответственность организации за нарушение закона о защите персональных данных:

Нарушение законодательства о персональных данных может повлечь наложение штрафов на должностных лиц и организацию.

Пользователи, чьи права были нарушены, могут потребовать компенсации морального вреда, а также возмещения убытков, причиненных незаконной обработкой персональных данных.

Обязанность информирования Роскомнадзора и субъекта персональных данных о факте утечки данных; с 30 мая 2025 года компаниям запрещено скрывать утечки персональных данных, за молчание грозит штраф до 3 млн рублей. В случае утечки необходимо в течение 24 часов сообщить об инциденте в Роскомнадзор, а в течение 72 часов направить отчёт о результатах расследования.

Возможность отзыва лицензии на предоставление услуг связи и другие виды ограничений деятельности.

Меры, которые стоматологическая клиника должна предпринять для устранения нарушений и предупреждения аналогичных ситуаций в дальнейшем:

Прекратить рассылку рекламных материалов по собранным данным без согласия пользователей.

Организовать внутреннее расследование обстоятельств произошедшего, выявление виновных лиц и применение дисциплинарных взысканий.

Разработать и внедрить процедуры и политики по защите персональных данных, соответствующие требованиям 152-ФЗ.

Получить явное согласие пользователей на обработку их персональных данных, включая рассылку рекламных материалов, в соответствии с законодательством.

Обучить персонал правилам работы с персональными данными, включая сбор, обработку, хранение и уничтожение данных.

Провести аудит системы защиты персональных данных и устранить выявленные уязвимости.

Ошибки стоматологической клиники:

Отсутствует согласие гражданина на обработку персональных данных

Игнорируются требования к защите персональных данных

Кейс «Комплексный подход к организации информационной безопасности»

Цель:

Оценка знаний обучающихся по основным аспектам комплексной стратегии информационной безопасности, включающей политики и средства контроля безопасности, которые минимизируют угрозы и предотвращают несанкционированный доступ к данным.

Контекст:

Стоматологическая клиника столкнулась с потенциальной угрозой утечки медицинских данных пациентов (инцидент). Медицинская информационная система, которая хранит персональные данные пациентов, включая медицинские записи, подверглась несанкционированному доступу. Необходимо провести расследование и предложить меры по предотвращению подобных инцидентов в будущем.

Задания:

1) Изучите нормативно-законодательные акты

2) Определите основные стратегические меры по анализу инцидента

3) Опишите потенциальные угрозы и риски, связанные с данной ситуацией

4) Предложите конкретные меры по реагированию на инцидент, включая организационные, технические и правовые аспекты

5) Сформулируйте рекомендации по предотвращению подобных инцидентов

Предоставленные материалы:

Уголовный кодекс РФ (глава «Преступления в сфере компьютерной информации»)

Доктрина информационной безопасности РФ

Федеральный закон № 152-ФЗ «О персональных данных» в актуальной редакции

Приказ ФСТЭК России № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

Приказ Минздрава России № 911н «Об утверждении Требований к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных медицинских организаций»

Эталоны ответов:

Основные стратегические меры по анализу инцидента:

Отключить зараженные компьютеры от сети, чтобы предотвратить дальнейшее распространение вируса.

Провести антивирусную сканирование и лечение зараженных систем.

Восстановить данные из резервных копий, если таковые имеются.

Сообщить сотрудникам о произошедшем и предоставить рекомендации по безопасности.

Определить, какие данные были скомпрометированы

Оценить масштаб утечки (количество затронутых пациентов, период времени, в течение которого данные были доступны).

Установить возможные причины и способы несанкционированного доступа.

Определить, какие именно сотрудники имели доступ к системе и как они могли быть вовлечены.

В зависимости от типа и масштаба утечки, необходимо уведомить соответствующие государственные органы.

Потенциальные угрозы и риски:

Вредоносное ПО: вирус, распространяющийся через вложение, может нанести серьезный ущерб системе, включая шифрование данных, кражу паролей, перехват трафика и т.д.

Утечка конфиденциальной информации: в результате заражения, злоумышленник может получить доступ к важным данным организации (финансовые документы, персональные данные пациентов, персональные данные сотрудников и т.д.)

Нарушение доступности информации: вирус может привести к выходу из строя рабочих станций или серверов, что затруднит или сделает невозможным выполнение рабочих задач.

Меры по реагированию на инцидент, включая организационные, технические и правовые аспекты:

Организационные:

- Внедрение строгой политики паролей и многофакторной аутентификации.
- Регулярное обучение сотрудников по вопросам информационной безопасности.
- Усиление контроля за доступом к данным и мониторинг действий сотрудников.
- Разработка и внедрение процедуры реагирования на инциденты информационной безопасности.

Технические:

- Внедрение шифрования данных при хранении и передаче.
- Установка и настройка межсетевого экрана (firewall).
- Регулярное обновление программного обеспечения.
- Внедрение системы обнаружения вторжений.
- Создание резервных копий данных.
- Аудит системы безопасности.

Правовые:

- Анализ соответствия требованиям законодательства в области защиты персональных данных.
- Внесение изменений в политики обработки данных для соответствия требованиям законодательства.

Рекомендации по предотвращению подобных инцидентов:

Регулярный мониторинг системы безопасности и анализ журналов событий.

Тестирование системы на проникновение угроз.

Проведение аудита информационной безопасности.

Разработка и внедрение плана обеспечения непрерывности контроля за информационной безопасностью.

Кейс «Способы лечения воспалительных заболеваний пародонта и слизистой оболочки полости рта, у больных красным плоским лишаем слизистой оболочки полости рта»

Цель:

Рационализация лечебно-гигиенических протоколов ведения больных с десневыми проявлениями осложненных форм красного плоского лишая слизистой оболочки рта, основанная на оригинальных методиках проявления топических ингибиторов кальциневрина в качестве средств патогенетического воздействия и выборе безопасных средств, методов и технологий гигиены полости рта, повышает эффективность пародонтологического лечения и качество жизни больных с КПЛ-ассоциированными заболеваниями пародонта.

Контекст:

Патогенетические особенности красного плоского лишая слизистой оболочки рта предполагают частое вовлечение в процесс пародонтального комплекса с развитием специфических КПЛ-ассоциированных заболеваний пародонта, требующих своевременной диагностики, особых подходов к дифференциальной диагностике, систематизации и лечению. Тяжесть и манифестный характер клинических проявлений заболеваний пародонта у больных красным плоским лишаем полости рта определяются формой заболевания и приводят к снижению стоматологических составляющих качества жизни по данным индекса.

Задания:

1. Составление комбинации из ключевых слов для поискового запроса для русскоязычных БАЗ ДАННЫХ (БД) - количество таких комбинаций.

2. Составление комбинации из ключевых слов для поискового запроса для англоязычных БАЗ ДАННЫХ (БД) - количество таких комбинаций.
3. Определение класса международной патентной классификации для патентного поиска в русскоязычной и англоязычной БД, см. ссылку http://wwwl.fips. m/wps/portal/oficjpub_ru/#page=classification&type=IZPM&leveHinterContent
4. Проведение поиска по русскоязычной БД (отечественным изобретениям) (http://wwwl.fips.ru/wps/wcm/connect/content ru/ru/infomi resources/infomiretrieval systein/) или http://wwwl.fips.m/wps/portal/IPS_Ru
   - с сохранением экранной копии (Prt Sc):
   - страницы сайта с введенными поисковыми запросами;
   - страницы сайта с результатами поиска и копиями наиболее релевантных источников информации;
   - включая номера патентов/заявок - количество найденных русскоязычных документов всего;
   -количество наиболее релевантных документов и их сохраненные копии
5. Проведение поиска по БД зарубежных изобретений Espacenet Patent search https://worldwide.espacenet.com/
   - с сохранением экранной копии (Prt Sc):
   - сайта с введенными поисковыми запросами;
   - страницы сайта с результатами поиска и копиями наиболее релевантных источников информации, включая номера патентов/заявок - количество найденных зарубежных документов всего;
   - количество наиболее релевантных документов и их сохраненные копии.
6. Определение основных тенденций по теме исследования по итогам проведенного патентного поиска - количество выявленных тенденций ссылками на номера наиболее релевантных документов.
7. Количество источников современных изданий.

Кейс «Способ диагностики (определения) стадии ВИЧ-инфекции»

Цель:

Использование при диагностике острой ВИЧ-инфекции критерия прогностичности, рассчитанного на основании уровня антигена ВИЧ р24, что позволит прогнозировать срок сероконверсии и сократить число арбитражных исследований. Исследование простых быстрых тестов в клинических подразделениях у больных с симптомами СПИД - ассоциированных заболеваний позволит сократить длительность диагностики ВИЧ-инфекции и своевременно начать специфическое лечение.

Контекст:

Увеличение объема лабораторных исследований в Санкт-Петербурге за последний 5 лет произошло на фоне внедрения комбинированных (Аг/Ат) иммуноферментных тест-систем 4-го поколения, имеющих высокую чувствительность и специфичность, что способствовало достоверному сокращению доли ложноположительных и ложноотрицательных проб. Наибольшая диагностическая эффективность установлена на иммуноферменных тест-системах, изготовленных на основе смеси гликопротеина gp 160, синтетических пептидов ВИЧ1 и ВИЧ2, воспроизводящих иммунодоминантные эпитопы белков оболочки, и моноклональных антител к антигену ВИЧ р24. Высокая частота повторных исследований в арбитражных лабораториях (до 5,8 на 1вновь выявленного ВИЧ-инфицированного в год) значительно увеличивает расходы на этиологическую диагностику ВИЧ-инфекции. Использование комбинированных тест-систем 4-го поколения (Аг/Ат) позволяет сократить число референс-исследований и при получении первого положительного результата референе-ИФА проводить экспертное исследование методом ИБ.

Задания:

1. Составление комбинации из ключевых слов для поискового запроса для русскоязычных БАЗ ДАННЫХ (БД) - количество таких комбинаций.

2. Составление комбинации из ключевых слов для поискового запроса для англоязычных БАЗ ДАННЫХ (БД) - количество таких комбинаций.
3. Определение класса международной патентной классификации для патентного поиска в русскоязычной и англоязычной БД, см. ссылку http://wwwl.fips. m/wps/portal/oficjpub_ru/#page=classification&type=IZPM&leveHinterContent
4. Проведение поиска по русскоязычной БД (отечественным изобретениям) (http://wwwl.fips.ru/wps/wcm/connect/content ru/ru/infomi resources/infomiretrieval systein/) или http://wwwl.fips.m/wps/portal/IPS_Ru
   - с сохранением экранной копии (Prt Sc):
   - страницы сайта с введенными поисковыми запросами;
   - страницы сайта с результатами поиска и копиями наиболее релевантных источников информации;
   - включая номера патентов/заявок - количество найденных русскоязычных документов всего;
   -количество наиболее релевантных документов и их сохраненные копии
5. Проведение поиска по БД зарубежных изобретений Espacenet Patent search https://worldwide.espacenet.com/
   - с сохранением экранной копии (Prt Sc):
   - сайта с введенными поисковыми запросами;
   - страницы сайта с результатами поиска и копиями наиболее релевантных источников информации, включая номера патентов/заявок - количество найденных зарубежных документов всего;
   - количество наиболее релевантных документов и их сохраненные копии.
6. Определение основных тенденций по теме исследования по итогам проведенного патентного поиска - количество выявленных тенденций ссылками на номера наиболее релевантных документов.
7. Количество источников современных изданий.