

Федеральное государственное бюджетное научное учреждение
«Федеральный исследовательский центр фундаментальной и
трансляционной медицины»

УТВЕРЖДАЮ

Директор ФИЦ ФТМ

_____ М.И. Воевода

02 июня 2023 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОФЕССИОНАЛЬНОЙ
ДЕЯТЕЛЬНОСТИ ВРАЧА»**

Специальность:

31.08.07 Патологическая анатомия

Уровень высшего образования:

подготовка кадров высшей квалификации

Новосибирск

2023 г.

Рабочая программа дисциплины «Виды исследования и адекватные им методы статистического анализа в медицине» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по специальности 31.08.07 Патологическая анатомия (уровень подготовки кадров высшей квалификации), утверждённым приказом Министерства науки и высшего образования Российской Федерации от 02.02.2022 № 110.

Разработчики программы:

Митрофанов И.М., доктор медицинских наук, ведущий научный сотрудник лаборатории патогенеза соматических заболеваний НИИЭКМ ФИЦ ФТМ.

Рабочая программа дисциплины рассмотрена и одобрена на заседании Ученого совета ФИЦ ФТМ (протокол № 6 от 01 июня 2023 г.)

1. Цель и задачи изучения дисциплины, требования к результатам освоения дисциплины

Цель изучения дисциплины:

Цель освоения дисциплины: подготовка высококвалифицированного специалиста – врача-патологоанатома, обладающего универсальными, общепрофессиональными и профессиональными компетенциями в области информационно-коммуникационных технологий, готового к осуществлению самостоятельной профессиональной деятельности.

Задачи освоения дисциплины:

- формирование и совершенствование профессиональных компетенций врача-патологоанатома в области информационно-коммуникационных технологий, позволяющих ему свободно ориентироваться в вопросах специальности, успешно решать свои профессиональные задачи;
- формирование базовых знаний и умений в использовании новейших информационно-коммуникационных технологий необходимых врачу-патологоанатому;
- подготовка врача-патологоанатома, хорошо ориентирующегося в современной профессиональной информации, владеющего необходимыми для работы в медицинских учреждениях программными продуктами;
- подготовка специалиста к самостоятельной профессиональной деятельности с учетом постоянного обновления информационно-коммуникационной среды в учреждениях здравоохранения.

Место дисциплины в структуре образовательной программы

Дисциплина «Информационные технологии в профессиональной деятельности врача» относится к обязательной части образовательной программы.

Требования к результатам освоения дисциплины (модуля):

Формирование универсальных, общепрофессиональных и профессиональных компетенций у обучающихся в рамках изучения дисциплины (модуля) предполагает овладение системой теоретических знаний по выбранной специальности и формирование соответствующих умений и (или) владений.

Код и наименование компетенции, индикатора достижения компетенции	Планируемые результаты обучения по дисциплине		
ОПК-1. Способен использовать информационно-коммуникационные технологии в профессиональной деятельности и соблюдать правила информационной безопасности			
ОПК-1.1 Использует современные информационно-коммуникационные средства и технологии в профессиональной деятельности	Знать:	-основные направления использования современных информационных технологий в работе врача; - организацию работы медицинских информационных систем медицинских организаций, включая возможности использования систем поддержки принятия врачебных и управленческих решений, телемедицинские технологии	

	Уметь:	- использовать современные средства сети Интернет для поиска профессиональной информации по отдельным разделам медицинских знаний в своей практической работе, а также при самостоятельном обучении; - структурировать и формализовать медицинскую информацию
	Владеть:	- навыками поиска необходимой медицинской информации с применением средств сети Интернет; - навыками работы с различными медицинскими системами; использования систем поддержки принятия клинических решений; - навыками анализа содержания медицинских публикаций с позиций доказательной медицины; - навыками использования программных средств для алгоритмизации лечебно-диагностического процесса
ОПК-1.2. Соблюдает правила информационной безопасности	Знать:	- основные требования информационной безопасности, предъявляемые к организации электронного документооборота в здравоохранении и способы их реализации
	Уметь:	- использовать современные подходы, обеспечивающие информационную безопасность в практической работе врача
	Владеть:	- навыками «безопасной» работы в информационной среде медицинской организации
ОПК-6. Способен проводить анализ медико-статистической информации, вести медицинскую документацию и организовывать деятельность находящегося в распоряжении медицинского персонала		
ОПК-6.2. Ведет медицинскую документацию	Знать:	- особенности работы с формализованными медицинскими документами, реализованными в медицинских информационных системах медицинских организаций; - специфику формализованных протоколов врачей различных специальностей
	Уметь:	- грамотно вести медицинскую документацию средствами медицинских информационных систем
	Владеть:	- навыками ведения первичной медицинской документации в медицинских информационных системах; - навыками формирования обобщающих и отчетных документов

2. Объем дисциплины (модуля) по видам учебной работы

Виды учебной работы	Всего часов	Объем по годам обучения	
Контактная работа обучающегося с преподавателем по видам учебных занятий (КР):	44	1	2
			44
Лекция (Л)	4		4

Семинарское/практическое занятие (СПЗ)	40		40
Самостоятельная работа обучающегося, в том числе подготовка к промежуточной аттестации (СР)	28		28
Вид промежуточной аттестации: Зачет (З), Зачет с оценкой (ЗО), Экзамен (Э)	зачет		
Общий объем дисциплины в часах	72		72
Общий объем дисциплины в зачетных единицах	2		2

3. Содержание дисциплины

Раздел 1. Современные информационно-коммуникационные технологии, применяемые в медицине

Раздел 2. Технические и программные средства, обеспечивающие применение новых информационно-коммуникационных технологий в медицине и научных медико-биологических исследованиях

Раздел 3. Правовые и этические аспекты использования персональных данных в медицинских информационно-коммуникационных технологиях. Врачебная этика и деонтология, правила информационной безопасности.

4. Учебно-тематический план дисциплины

Номер раздела, темы	Наименование разделов, тем	Количество часов					Форма контроля
		Всего	КР	Л	СПЗ	СР	
Раздел 1	Современные информационно-коммуникационные технологии, применяемые в медицине	32	22	2	20	10	Тестирование
Раздел 2	Технические и программные средства, обеспечивающие применение новых информационно-коммуникационных технологий в медицине и научных медико-биологических исследованиях		11	1	10	8	Тестирование
Раздел 3	Правовые и этические аспекты использования персональных данных в медицинских информационно-коммуникационных технологиях		11	1	10	8	Тестирование
	Общий объем	72	44	4	40	28	Зачет

5. Учебно-методическое обеспечение самостоятельной работы обучающихся

Цель самостоятельной работы обучающихся заключается в глубоком усвоении учебного материала и в развитии навыков самообразования. Самостоятельная работа включает: работу с текстами, основной и дополнительной литературой, учебно- методическими пособиями, нормативными материалами, в том числе материалами Интернета, а также проработку конспектов лекций, написание рефератов, участие в работе семинаров, научных конференциях.

Контроль самостоятельной работы осуществляется на семинарских (практических занятиях) занятиях.

6. Оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся

Примерные оценочные средства, включая оценочные задания для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине представлены в Приложении 1 Оценочные средства по дисциплине.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Медицинская информатика: учебник/ под общ. ред. Т.В. Зарубиной, Б.А. Кобринского. – 2-е изд. перераб. и доп.- Москва: ГЭОТАР-Медиа. 2022
2. Медицинская информатика: учебник/ под общ. ред. Т.В. Зарубиной, Б.А. Кобринского. – 2-е изд. перераб. и доп.- Москва: ГЭОТАР-Медиа. 2018- 502 с.
3. Медицинская информатика: учебник/ под общ. ред. Т.В. Зарубиной, Б.А. Кобринского. – 2-е изд. перераб. и доп.- Москва: ГЭОТАР-Медиа. 2016- с. 512

7.2. Дополнительная литература

1. Персональная телемедицина. Телемедицинские и информационные технологии реабилитации и управления здоровьем [Электронный ресурс]/О.Ю. Атьков, Ю.Ю. Кудряшов .- Москва:Практика, 2015.-248 с.- Режим доступа:<http://books-up.ru>

7.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Официальный сайт ФИЦ ФТМ: адрес ресурса – <https://frcftm.ru/>, на котором содержатся сведения об образовательной организации и ее подразделениях, локальные нормативные акты, сведения о реализуемых образовательных программах, их учебно-методическом и материально-техническом обеспечении, а также справочная, оперативная и иная информация.
- 2.Springer Journals [Электронный ресурс]: база данных – Режим доступа: <https://link.springer.com/> – Доступ открыт со всех компьютеров сети Центра.
- 3.Федеральная электронная медицинская библиотека [Электронный ресурс]: электронно-библиотечная система (ЭБС) / ЦНМБ Первого Московского государственного медицинского Центра им. И.М.Сеченова. – Режим доступа: <http://feml.scsml.rssi.ru/feml> – Свободный доступ.

4.eLIBRARY.RU [Электронный ресурс]: электронная библиотека – URL: <http://www.elibrary.ru/>. – Доступ к подписке журналов открыт со всех компьютеров сети Центра.

5.Российская государственная библиотека [Электронный ресурс]: сайт. – Режим доступа: <http://www.rsl.ru> – Свободный доступ.

6.Consilium Medicum [Электронный ресурс]: сайт. – Режим доступа: <http://www.consilium-medicum.com/> – Свободный доступ.

7.PubMed: US National Library of Medicine National Institutes of Health [Электронный ресурс]: сайт. – URL: <http://www.ncbi.nlm.nih.gov/pubmed>.

8.ScienceDirect. Ресурсы открытого доступа [Электронный ресурс]: сайт. – Режим доступа: <http://www.sciencedirect.com/science/jrnallbooks/open-access>.

9.КиберЛенинка: научная электронная библиотека [Электронный ресурс]: сайт. – Режим доступа: <http://cyberleninka.ru/> – Свободный доступ.

8. Материально-техническое обеспечение дисциплины

8.1. Перечень помещений и оборудования для проведения учебных занятий по дисциплине

№	Помещение (площадь)	Перечень оборудования	Адрес, наименование организации
2	Конференц-зал, ком. 611	Ноутбук Asus F3Ka TL60 (1 шт.); проектор Epson EB-93 (1 шт.).	Институт молекулярной патологии и патоморфологии ФИЦ ФТМ
3	Помещение для самостоятельной работы обучающихся № 409	Технические средства обучения: Компьютер Asus – 1 шт. Компьютер Interlink – 4 шт. Специализированная мебель: Стол компьютерный – 10 шт. Кресло компьютерное- 10 шт. Стол – 1 шт. Стул – 1 шт. Перечень лицензионного программного обеспечения: Linux Mint, Libre Office Помещение обеспечено доступом к сети «Интернет» и электронной информационно-образовательной среде ФИЦ ФТМ.	Учебно-методический центр ФИЦ ФТМ

9. Методические указания для обучающихся по изучению дисциплины

Преподавание дисциплины осуществляется в соответствии с Федеральным государственным образовательным стандартом высшего образования.

Основными формами получения и закрепления знаний по данной дисциплине являются занятия лекционного и практического типа, самостоятельная работа обучающегося, в том числе под руководством преподавателя, прохождение контроля.

Учебный материал по дисциплине разделен на 9 тем.

Изучение дисциплины, согласно учебному плану, предполагает самостоятельную работу обучающихся. Самостоятельная работа включает в себя изучение учебной, учебно-методической и специальной литературы, её конспектирование, подготовку к семинарам (практическим занятиям), текущему контролю успеваемости и промежуточной аттестации (зачету).

Текущий контроль успеваемости по дисциплине (модулю) и промежуточная аттестация осуществляются в соответствии с Положением о проведении текущего контроля успеваемости и организации и проведения промежуточной аттестации обучающихся, устанавливающим формы проведения промежуточной аттестации, ее периодичность и систему оценок.

10. Методические рекомендации преподавателю по организации учебного процесса по дисциплине

Преподавание дисциплины осуществляется в соответствии с Федеральными государственными образовательными стандартами высшего образования.

При изучении дисциплины (модуля) рекомендуется использовать следующий набор средств и способов обучения:

- рекомендуемую основную и дополнительную литературу;
- задания для подготовки к семинарам (практическим занятиям) – вопросы для обсуждения и др.;
- задания для текущего контроля успеваемости (задания для самостоятельной работы обучающихся);
- вопросы и задания для подготовки к промежуточной аттестации по итогам изучения дисциплины, позволяющие оценить знания, умения и уровень приобретенных компетенций.

При проведении занятий лекционного и семинарского типа, в том числе в форме вебинаров и on-line курсов необходимо строго придерживаться учебно-тематического плана дисциплины (модуля), приведенного в разделе 4 данного документа. Необходимо уделить внимание рассмотрению вопросов и заданий, включенных в оценочные задания, при необходимости, решить аналогичные задачи с объяснением алгоритма решения.

Следует обратить внимание обучающихся на то, что для успешной подготовки к текущему контролю успеваемости и промежуточной аттестации нужно изучить материалы основной и дополнительной литературы, список которых приведен в разделе 7 данной рабочей программы дисциплины (модуля) и иные источники, рекомендованные в подразделах «Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и «Перечень профессиональных баз данных и информационных справочных систем», необходимых для изучения дисциплины (модуля).

Текущий контроль успеваемости и промежуточная аттестация осуществляются в соответствии с Положением о проведении текущего контроля успеваемости и организации и проведения промежуточной аттестации обучающихся, устанавливающим формы проведения промежуточной аттестации, ее периодичность и систему оценок, с которыми необходимо ознакомить обучающихся на первом занятии.

**ОЦЕНОЧНЫЕ СРЕДСТВА ПО ДИСЦИПЛИНЕ
«ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОФЕССИОНАЛЬНОЙ
ДЕЯТЕЛЬНОСТИ ВРАЧА»**

Специальность:
31.08.07 Патологическая анатомия

Уровень высшего образования:
подготовка кадров высшей квалификации

Новосибирск

2023 г.

1.Перечень компетенций, формируемых в процессе изучения дисциплины

Код и наименование компетенции, индикатора достижения компетенции	Планируемые результаты обучения по дисциплине	
ОПК-1. Способен использовать информационно-коммуникационные технологии в профессиональной деятельности и соблюдать правила информационной безопасности		
ОПК-1.1 Использует современные информационно-коммуникационные средства и технологии в профессиональной деятельности	Знать:	-основные направления использования современных информационных технологий в работе врача; - организацию работы медицинских информационных систем медицинских организаций, включая возможности использования систем поддержки принятия врачебных и управленческих решений, телемедицинские технологии
	Уметь:	- использовать современные средства сети Интернет для поиска профессиональной информации по отдельным разделам медицинских знаний в своей практической работе, а также при самостоятельном обучении; - структурировать и формализовать медицинскую информацию
	Владеть:	- навыками поиска необходимой медицинской информации с применением средств сети Интернет; - навыками работы с различными медицинскими системами; использования систем поддержки принятия клинических решений; - навыками анализа содержания медицинских публикаций с позиций доказательной медицины; - навыками использования программных средств для алгоритмизации лечебно-диагностического процесса
ОПК-1.2. Соблюдает правила информационной безопасности	Знать:	- основные требования информационной безопасности, предъявляемые к организации электронного документооборота в здравоохранении и способы их реализации
	Уметь:	- использовать современные подходы, обеспечивающие информационную безопасность в практической работе врача
	Владеть:	- навыками «безопасной» работы в информационной среде медицинской организации
ОПК-6. Способен проводить анализ медико-статистической информации, вести медицинскую документацию и организовывать деятельность находящегося в распоряжении медицинского персонала		
ОПК-6.2. Ведет медицинскую документацию	Знать:	- особенности работы с формализованными медицинскими документами, реализованными в медицинских информационных системах медицинских организаций;

		- специфику формализованных протоколов врачей различных специальностей
	Уметь:	- грамотно вести медицинскую документацию средствами медицинских информационных систем
	Владеть:	- навыками ведения первичной медицинской документации в медицинских информационных системах; - навыками формирования обобщающих и отчетных документов

2. Критерии и шкалы оценивания компетенций

В ходе текущего контроля успеваемости (устный или письменный опрос, подготовка и защита реферата, доклад, презентация, тестирование и пр.) при ответах на учебных занятиях, а также промежуточной аттестации в форме экзамена и (или) зачета с оценкой обучающиеся оцениваются по четырёхбалльной шкале: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» – выставляется ординатору, если он глубоко усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет связывать теорию с практикой, свободно справляется с задачами и вопросами, не затрудняется с ответами при видоизменении заданий, умеет принять правильное решение и грамотно его обосновывать, владеет разносторонними навыками и приемами выполнения практических задач, комплексной оценкой предложенной ситуации, правильно выбирает тактику действий.

Оценка «хорошо» – выставляется ординатору, если он твердо знает программный материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, но недостаточно полно раскрывает междисциплинарные связи, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения, комплексной оценкой предложенной ситуации, правильно выбирает тактику действий.

Оценка «удовлетворительно» – выставляется ординатору, если он имеет поверхностные знания программного материала, не усвоил его деталей, допускает неточности, оперирует недостаточно правильными формулировками, нарушает логическую последовательность в изложении программного материала, испытывает затруднения при выполнении практических задач, испытывает затруднения с комплексной оценкой предложенной ситуации, не полностью отвечает на вопросы, при помощи наводящих вопросов преподавателя, выбор тактики действий возможен в соответствии с ситуацией при помощи наводящих вопросов.

Оценка «неудовлетворительно» – выставляется ординатору, который не знает значительной части программного материала, допускает грубые ошибки, неуверенно, с большими затруднениями решает практические задачи или не справляется с ними самостоятельно, не владеет комплексной оценкой ситуации, неверно выбирает тактику действий, приводящую к ухудшению ситуации, нарушению безопасности пациента.

В ходе текущего контроля успеваемости (устный или письменный опрос, подготовка и защита реферата, доклад, презентация, тестирование и пр.) при ответах на учебных занятиях, а также промежуточной аттестации в форме зачета обучающиеся оцениваются по двухбалльной шкале:

Оценка «зачтено» – выставляется ординатору, если он продемонстрировал знания программного материала: подробно ответил на теоретические вопросы, справился с выполнением заданий и (или) ситуационных задач, предусмотренных программой ординатуры, ориентируется в основной и дополнительной литературе, рекомендованной рабочей программой дисциплины (модуля).

Оценка «не зачтено» – выставляется ординатору, если он имеет пробелы в знаниях программного материала: не владеет теоретическим материалом и допускает грубые, принципиальные ошибки в выполнении заданий и (или) ситуационных задач, предусмотренных рабочей программой дисциплины (модуля).

Шкала оценивания (четырёхбалльная или двухбалльная), используемая в рамках текущего контроля успеваемости определяется преподавателем, исходя из целесообразности применения той или иной шкалы. Если текущий контроль успеваемости и (или) промежуточная аттестация, предусматривает тестовые задания, то перевод результатов тестирования в четырёхбалльную шкалу осуществляется по схеме:

Оценка «Отлично» – 90-100% правильных ответов;

Оценка «Хорошо» – 80-89% правильных ответов;

Оценка «Удовлетворительно» – 71-79% правильных ответов;

Оценка «Неудовлетворительно» – 70% и менее правильных ответов.

Перевод результатов тестирования в двухбалльную шкалу:

Оценка «Зачтено» – 71-100% правильных ответов;

Оценка «Не зачтено» – 70% и менее правильных ответов.

Для промежуточной аттестации, состоящей из двух этапов (тестирование + устное собеседование) оценка складывается по итогам двух пройденных этапов. Обучающийся, получивший положительные оценки за тестовое задание и за собеседование считается аттестованным. Промежуточная аттестация, проходящая в два этапа, как правило, предусмотрена по дисциплинам (модулям), завершающихся экзаменом или зачетом с оценкой.

Обучающийся, получивший неудовлетворительную оценку за первый этап (тестовое задание) не допускается ко второму этапу (собеседованию).

3.Оценочные средства по дисциплине «Информационные технологии в профессиональной деятельности врача»

Вид оценочного средства: фонд тестовых заданий

№ по компетенции	Вопрос	Варианты ответов	Правильный ответ
1	Вопрос. Задачи информационной безопасности	Варианты ответов. № 1. ограничение права личности и общества на получение информации; № 2. борьба с криминальными угрозами в сфере информационных и телекоммуникационных систем, с телефонным терроризмом, отмыванием денег и т.д.; № 3. защита личности, организации, общества и государства от информационно-психологических угроз; № 4. формирование имиджа, борьба с клеветой, слухами, дезинформацией;	Ответ 2, 3, 4

		№ 5. обеспечение субъективной информацией.	
2	Вопрос. Использование искусственного интеллекта в обработке данных медицинских визуализационных исследований уровень диагностики	Варианты ответов. № 1. Снижает № 2. Повышает № 3. Не влияет на уровень диагностики	Ответ 2
3	Вопрос. Защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры является определением для термина	Варианты ответов. № 1. база данных; № 2. информационный процесс; № 3. защита информации; № 4. информационная безопасность; № 5. информационная система.	Ответ 4
4	Вопрос. Система поддержки принятия врачебных решений в автоматизированной медицинской информационной системе может включать элементы искусственного интеллекта	Варианты ответов. № 1. Утверждение верно № 2. Утверждение ошибочно	Ответ 1
5	Вопрос Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные	Варианты ответов № 1. единая государственная информационная система в сфере здравоохранения; № 2. лабораторная информационная система медицинской организации; № 3. ГосСОПКА;	Ответ 3

	ресурсы Российской Федерации	№ 4. ФСТЭК; № 5. медицинская информационная система медицинской организации.	
6	Вопрос. Отключать средства защиты Информационной системы с персональными данными без согласования с администратором пользователь	Варианты ответов. № 1. Имеет право № 2. Не имеет право	Ответ 2
7	Вопрос. Информация, защита которой от несанкционированного распространения является обязанностью субъекта в силу выполняемых им профессиональных функций	Варианты ответов. № 1. профессиональная тайна; № 2. интеллектуальные данные	Ответ 1
8	Вопрос. Медицинская информационная система (МИС) это	система автоматизации документооборота для медицинских учреждений, в которой объединены система поддержки принятия врачебных решений, электронные медицинские карты пациентов, данные медицинских исследований в цифровой форме, данные мониторинга состояния пациента с медицинских приборов, средства общения между сотрудниками, финансовая и административная информация	
9	Вопрос. К силам обеспечения безопасности оператора информационной системы в сфере здравоохранения относятся	Варианты ответов № 1. ГосСОПКА; № 2. подразделения (работники) оператора, ответственные за обеспечение безопасности информационных систем; № 3. иные подразделения (работники), участвующие в обеспечении безопасности информационных систем и (или)	Ответ 2, 3, 4, 5

		информационно-телекоммуникационных систем оператора; № 4. подразделения (работники) оператора, эксплуатирующие информационные системы; № 5. подразделения (работники), обеспечивающие функционирование (сопровождение, обслуживание, ремонт) технических средств информационных систем; № 6. федеральная служба безопасности.	
10	Вопрос. Уровень научной обоснованности организации медицинской помощи с применением медицинских информационных систем	Варианты ответов. № 1. повышается № 2. снижается	Ответ 1
11	Вопрос. К физическим угрозам в сфере информационной безопасности относится	Варианты ответов. № 1. хищение программных или аппаратных ключей и средств криптографической защиты данных; № 2. хищение носителей информации; № 3. уничтожение или разрушение средств обработки информации и связи; № 4. воздействие на персонал; № 5. внедрение электронных устройств перехвата информации в технические средства и помещения № 6. закупки несовершенных или устаревших информационных технологий.	Ответ 1, 2, 3, 4
12	Вопрос. Уровень доступности коммуникаций между врачами, специалистами и пациентами при использовании информационно-	Варианты ответов. № 1. повышается № 2. снижается	Ответ 1

	коммуникационных технологий		
13	Вопрос. Меры информационной безопасности программно-технического уровня	Варианты ответов. № 1. программная защита передаваемой информации и каналов связи; № 2. идентификация и аутентификация пользователей; № 3. организация учета, хранения, использования и уничтожения документов и носителей информации;	Ответ 2, 3
14	Вопрос. В организации не допускается обработка следующих категорий персональных данных	Варианты ответов. № 1. Расовая принадлежность № 2. Политические взгляды № 3. Философские убеждения № 4. Состояние интимной жизни № 5. Национальная принадлежность № 6. Религиозные убеждения № 7. Все вышеперечисленное	Ответ 7
15	Вопрос. Общее руководство по вопросам обеспечения информационной безопасности осуществляет	Варианты ответов. № 1. структурное подразделение по информационной безопасности; № 2. специалист по информационной безопасности; № 3. работники, обеспечивающие функционирование информационных систем в сфере здравоохранения № 4. руководитель организации сферы здравоохранения или его заместитель;	Ответ 4
16	Вопрос. Использовать в неслужебных целях компоненты программного и аппаратного обеспечения ПЭВМ	Варианты ответов. № 1. можно № 2. нельзя	Ответ 2
17	Вопрос. Базовый отраслевой документ стратегического планирования, определяющий	Варианты ответов. № 1. Приказ Минздрава России от 24.12.2018 N 911н «Об утверждении требований к государственным информационным системам в	Ответ 4

	направления развития системы обеспечения информационной безопасности в сфере здравоохранения, систему взглядов, принципы, подходы и требования к обеспечению защиты информации, обрабатываемой в информационных системах в сфере здравоохранения	сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций»; № 2. Постановление Правительства Российской Федерации от 09.02.2022 № 140 «О единой государственной информационной системе в сфере здравоохранения»; № 3. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 05.12.2016 №646; № 4. Концепция информационной безопасности в сфере здравоохранения утверждена протоколом президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 10.03.2022 N 7; № 5. Федеральный закон «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 N 323-ФЗ.	
18	Вопрос. Использовании в пароли имен, фамилий, легко вычисляемых названий надежность пароля	Варианты ответов. № 1. Снижает № 2. Повышает	Ответ 1
19	Вопрос. К программным угрозам относятся	Варианты ответов. № 1. хищение информации из библиотек, архивов, банков и баз данных; № 2. компьютерные вирусы и вредоносные программы; № 3. использование ошибок и «дыр» в программном обеспечении;	Ответ 2, 3, 4

		№ 4. установка «закладных» устройств.	
20	Вопрос. Для обеспечения надежности пароля длина его должна быть не менее	Варианты ответов. № 1. 3 символов № 2. 4 символов № 3. 6 символов	Ответ 3
21	Вопрос. Документы стратегического планирования, на основании которых разработана Концепция информационной безопасности в сфере здравоохранения (утверждена протоколом президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 10.03.2022 N 7	Варианты ответов. № 1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; № 2. Федеральный закон от 29.06.2015 № 162-ФЗ «О стандартизации в Российской Федерации»; № 3. Основы государственной политики Российской Федерации в области международной информационной безопасности, утвержденные Указом Президента Российской Федерации от 12 апреля 2021 г. № 213; № 4. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. №646; № 5. Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 02.07.2021 № 400.	Ответ 3, 4, 5
22	Вопрос. В случае утери (компрометации) ключа (пароля) информировать об этом Администратора информационной безопасности	Варианты ответов. № 1. Необходимо в любом случае № 2. Не нужно № 3. Можно, на усмотрение пользователя	Ответ 1
23	Вопрос. Источниками внутренних информационных угроз являются	Варианты ответов. № 1. программное обеспечение; № 2. сотрудники организации; № 3. аппаратные средства; № 4. стихийные бедствия;	Ответ 1, 2, 3

		№ 5. стихийные бедствия	
24	Вопрос. Доступность для пациентов к консультациям врачей и консилиумам с внедрением в клиническую практику информационно-коммуникационных технологий	Варианты ответов. № 1. повысилась № 2. Осталась на прежнем уровне № 3. снизилась	Ответ 1
25	Вопрос. К организационно-правовым угрозам относятся	Варианты ответов. № 1. закупки несовершеннолетних или устаревших информационных технологий и средств информатизации; № 2. нарушение требований законодательства и задержка в принятии необходимых нормативно-правовых решений в информационной сфере; № 3. уничтожение или разрушение средств обработки информации и связи	Ответ 1, 2
26	Вопрос. Хранить в тайне пользователем персональный пароль доступа в информационную медицинскую систему входит в его	Варианты ответов. № 1. Права № 2. Обязанности	Ответ 2
27	Вопрос. Оператор информационных систем в сфере здравоохранения должен проводить организационные мероприятия, направленные на повышение уровня знаний работников по вопросам обеспечения безопасности информационных систем в сфере здравоохранения и о	Варианты ответов. № 1. не реже одного раза в год; № 2. ежемесячно; № 3. раз в три года	Ответ 1

	возможных угрозах безопасности информации		
28	Вопрос. Особенности обеспечения информационной безопасности при использовании информационно-коммуникационных технологий в области медицины могут регулироваться на уровне	Варианты ответов. № 1. федеральном № 2. региональном № 3. На уровне медицинской организации № 4. Верно все вышеперечисленное	Ответ 4
29	Вопрос. Основные категории интересов субъектов информационной безопасности, связанных с использованием информационных систем	Варианты ответов. № 1. простота; № 2. доступность; № 3. конфиденциальность; № 4. целостность; № 5. открытость.	Ответ 2, 4
30	Вопрос. В соответствии с правилами информационной безопасности индивидуальный ключ (пароль) для доступа в медицинскую информационную систему другим сотрудникам доверять (раскрывать)	Варианты ответов. № 1. Можно № 2. Нельзя	Ответ 2
31	Вопрос. Принцип, который рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности,	Варианты ответов. № 1. разнообразия защитных средств. № 2. разделения обязанностей; № 3. обеспечения всеобщей поддержки мер безопасности;	Ответ 1

	несовместимыми между собой навыками (например, умением преодолевать высокую ограду и знанием слабостей нескольких операционных систем), называется принцип		
32	Вопрос. Электронная история болезни полностью заменяет бумажный вариант истории болезни	Варианты ответов. № 1. Утверждение верно № 2. Утверждение ошибочно	Ответ 2
33	Вопрос. По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации	Варианты ответов. № 1. физические; № 2. программные; № 3. организационно-правовые; № 4. информационные; № 5. радиоэлектронные; № 6. литературные	Ответ 1, 2, 3, 4, 5
34	Вопрос. Информационно-коммуникационные технологии могут использоваться в медицине с помощью	Варианты ответов. № 1. Персонального компьютера № 2. Планшета № 3. Мобильного телефона № 4. Верно все вышеперечисленное	Ответ 4
35	Вопрос. Режим секретности включает следующие группы мер	Варианты ответов. № 1. порядок и правила делопроизводства с секретными или конфиденциальными документами и иными носителями защищаемой информации. Возможно разделение потоков документальной информации по степени секретности сведений, содержащихся в документах, а также разделение потоков информации, документов, содержащих государственную и коммерческую тайну; № 2. воспитательно-профилактическую работу, уровень и содержание которой должны соответствовать уровню требуемой защиты информации с	Ответ 1, 2, 3

		целью предотвратить или значительно уменьшить риск утечки засекреченной информации через сотрудников объекта, работающих с такой информацией; № 3. установление пропускного и внутри объектового режима, соответствующего степени секретности информации, имеющейся на объекте; № 4. разрешительную систему, определяющую порядок доступа в служебных целях конкретных сотрудников к определенной защищаемой информации и в конкретные помещения, где ведутся конфиденциальные или секретные работы. № 5. просветительская работа	
36	Вопрос. Персональные компьютеры и съемные носители информации надо проверять на наличие вирусов	Варианты ответов. № 1. Иногда № 2. Регулярно (постоянно) № 3. Никогда	Ответ 2
37	Вопрос. Сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии, которые воспринимают информационные системы (живые организмы, управляющие машины и др.) в процессе жизнедеятельности и работы является определением для термина	Варианты ответов. № 1. показатели; № 2. информация; № 3. данные	Ответ 2
38	Вопрос. Инструктаж при использовании медицинских информационных технологий	Варианты ответов. № 1. обязателен № 2. Не нужен № 3. Нужен в особых случаях	Ответ 1
39	Вопрос.	Варианты ответов.	Ответ 1, 2

	Субъектами информационной безопасности могут быть	№ 1. органы и структуры, которые в той или иной мере занимаются обеспечением информационной безопасности; № 2. предприятия и организации независимо от формы собственности. № 3. общественное сознание	
40	Вопрос. Конфиденциальность персональных данных это	обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания	
41	Вопрос. Уровни для защиты интересов субъектов информационных отношений	Варианты ответов. № 1. административный; № 2. процедурный; № 3. информационный; № 4. региональный; № 5. программно-технический; № 6. законодательный	Ответ 1, 2, 5, 6
42	Вопрос. Персональные данные это	любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).	
43	Вопрос. Новые информационные технологии в профессиональной деятельности врача повышают эффективность его работы	Варианты ответов. № 1. Утверждение верно № 2. Утверждение ошибочно	Ответ 1
44	Вопрос. “Дерево решений” это	Варианты ответов. № 1. Психологический подход в общении врача с пациентом № 2. Представитель флоры Южной Америки № 3. Математический инструмент, применяемый для анализа данных, включая медико-биологические № 4.	Ответ 3

45	Вопрос. Техническое устройство, которое в наибольшей степени необходимо для использования информационных медицинских систем	Варианты ответов. № 1. Сотовый телефон № 2. Видеомаягнитофон № 3. Персональный компьютер	Ответ 3
46	Вопрос. ДОКА+ это	Варианты ответов. № 1. Медицинская информационная система, которая используется в лечебных учреждениях, включая клинику ФИЦ ФТМ № 2. Сокращенное наименование высокого профессионала в своей трудовой деятельности	Ответ 1
47	Вопрос. На современном этапе информационные медицинские технологии	Варианты ответов. № 1. Не развиваются № 2. Развиваются в высоком темпе № 3. Деградируют	Ответ 2
48	Вопрос. Понятия “нейросети” и “искусственный интеллект”	Варианты ответов. № 1. Тожественные № 2. Понятие “нейросети” шире понятия “искусственный интеллект” № 3. Не имеют отношения друг к другу № 4. Понятие “искусственный интеллект” шире понятия “нейросети”	Ответ 4
49	Вопрос. Все медицинские учреждения и подразделения в мире на современном этапе оснащены медицинскими информационными компьютеризированными системами	Варианты ответов. № 1. Утверждение верно № 2. Утверждение ошибочно	Ответ 2
50	Вопрос. Новые медико-информационные	Варианты ответов. № 1. Клинической медицине № 2. Медицинской науки	Ответ 5

	технологии способствуют развитию	№ 3. Медицинскому образованию № 4. Интеграции научных медико-биологических направлений № 5. Все выше перечисленное	
--	-------------------------------------	--	--