МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДЕНА
Ученым советом ФГБОУ ВО «РГЭУ (РИНХ)»
(протокол № 2 от 29.09.2020)
Председатель ученого совета – ректор
_____ Е.Н. Макаренко

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА -
ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Планирование, создание и организация работы медицинских учреждений в условиях цифровизации»

72 час.

Ростов-на-Дону
2020

ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1. **Цель программы**

Формирование у обучающихся актуальных для шестого технологического уклада экономики и необходимых для профессиональной деятельности глубоких теоретических знаний и профессиональных компетенций в области организации работы медицинского учреждения в части информационных технологий и защиты информации.

2. **Планируемые результаты обучения:**

Слушатель должен приобрести следующие знания, умения и навыки, необходимые для качественного изменения компетенций:

2.1. Знания

2.1.1 актуальной нормативно-правовой базы в сфере защиты информационных систем медицинских организаций от вредоносных воздействий;

2.1.2 актуальной нормативно-правовой базы в сфере проектирования и организации информационных систем в медицинских организациях, защиты персональных данных сотрудников и клиентов (пациентов) медицинских организаций, защиты информационных систем медицинских организаций от вредоносных воздействий;

2.1.3 аппаратной части информационных систем;

2.1.4 основных методов и средств обеспечения безопасности информационных систем;

2.1.5 основных методов обеспечения защиты персональных данных;

2.2. Умения:

2.2.1. выявления основных угроз безопасности информационных систем и охраны персональных данных;

2.2.2. использования основных методов обеспечения защиты информационных систем и охраны персональных данных;

2.2.3. подбора антивирусного программного обеспечения;

2.2.4. подготовки локальных нормативных правовых актов;

2.2.5. поиска составляющих информационной системы;

2.2.6. построения архитектуры информационной системы.

2.3 Навыки:

2.3.1. использования основных методов обеспечения защиты информационных систем и охраны персональных данных;

2.3.2. подбора и использования антивирусного программного обеспечения;

2.3.3. подбора составляющих аппаратной части к информационной системы медицинской организации;

2.3.4. подготовки локальных нормативных правовых актов в соответствии с актуальным профильным нормативным правовым актам Российской Федерации;

2.3.5. подготовки общего перечня информации, содержащейся на сайте медицинской организации.

3. **Категория слушателей**

3.1. Образование: высшее.

3.2. Квалификация: ограничения не устанавливаются.

3.3. Наличие опыта профессиональной деятельности: не требуется.

3.4. Предварительное освоение иных дисциплин: рекомендовано наличие базового уровня знаний по дисциплинам «Информатика» или эквивалентным ей.

4. **Учебный план программы «Планирование, создание и организация работы медицинских учреждений в условиях цифровизации»**

№ п/п	Модуль	Всего, час	Виды учебных занятий		
			Лекции	Практические занятия	Самостоятельная работа
1	Входной контроль	2	0	0	2

2	Модуль 1. Законодательство Российской Федерации в профильных сферах	12	5	0	7
3	Модуль 2. Применение информационных технологий в деятельности медицинской организации	24	4	10	10
4	Модуль 3. Угрозы информационной безопасности.	32	8	10	14
Итоговая аттестация		2	Тест		

5. Календарный план-график реализации образовательной программы

№ п/п	Наименование учебных модулей	Трудоёмкость (час)	Сроки обучения
1	Входной контроль	2	2 ноября 2020 г.
2	Модуль 1. Законодательство Российской Федерации в профильных сферах	12	2-3 ноября 2020 г.
3	Модуль 2 Применение информационных технологий в деятельности медицинской организации	28	5-8 ноября 2020 г.
4	Модуль 3. Угрозы информационной безопасности	28	8-14 ноября 2020 г.
5	Итоговая аттестация	2	16 ноября 2020 г.
Всего:		**72**	**15 дней**

6. Учебно-тематический план программы «Планирование, создание и организация работы медицинских учреждений в условиях цифровизации»

№ п/п	Модуль / Тема	Всего, час	Виды учебных занятий			Форма контроля
			Лекции	Практические занятия	Самостоятельная работа	
	Входной контроль	**2**	**0**	**0**	**2**	**Тест**
1.	**Модуль 1. Законодательство Российской Федерации в профильных сферах**	**12**	**4**	**0**	**8**	
1.1	Обзор законодательства Российской Федерации в сферах здравоохранения, информационных технологий, связи и защиты персональных данных.	**6**	2	0	4	
1.2	Нарушения законодательства Российской Федерации.	**6**	2	0	4	
2.	**Модуль 2. Применение информационных технологий в деятельности медицинской организации**	**28**	**8**	**18**	**2**	
2.1	Проектирование архитектуры информационной сети.	**8**	2	6	0	
2.2	Организация дистанционной работы.	**4**	2	-	2	
2.3	Организация внедрения информационных систем и обучения персонала.	**8**	2	6	0	
2.4	Сайт медицинской организации.	**8**	2	6	0	
3.	**Модуль 3. Угрозы информационной безопасности**	**28**	**8**	**18**	**2**	
3.1	Обзор основных угроз безопасности информационных систем.	**4**	2	0	2	
3.2	Обеспечение безопасности информационных систем.	**8**	2	6	0	
3.3	Обеспечение безопасности персональных данных.	**8**	2	6	0	

№ п/п	Модуль / Тема	Всего, час	Виды учебных занятий			Форма контроля
			Лекции	Практические занятия	Самостоятельная работа	
3.4	Составление локальных нормативных правовых актов.	**8**	2	6	0	
	Итоговая аттестация	**2**	**0**	**0**	**2**	**Тест**
	Всего	**72**	**20**	**36**	**16**	

7. Учебная (рабочая) программа повышения квалификации «Планирование, создание и организация работы медицинских учреждений в условиях цифровизации»

Модуль 1. Законодательство Российской Федерации в профильных сферах (12 час.)
Тема №1.1. Обзор законодательства Российской Федерации в сферах здравоохранения, информационных технологий, связи и защиты персональных данных (6 час.).
Права и обязанности организаций при оказании медицинской помощи гражданам с использованием информационных технологий. Права и обязанности граждан при получении медицинской помощи. Организация различных сфер деятельности (информационная система, сайт, оказание телемедицинских услуг, защита персональных данных сотрудников и клиентов (пациентов)) медицинской организации в соответствии с законодательством Российской Федерации.
Решение ситуационной задачи по вопросу применения законодательства Российской Федерации в сферах здравоохранения, информационных технологий, связи и защиты персональных данных **(самостоятельная работа)**.
Тема №1.2. Нарушения законодательства Российской Федерации (6 час.).
Обзор основных нарушений законодательства Российской Федерации в различных сферах деятельности (информационная система, сайт, оказание телемедицинских услуг, защита персональных данных сотрудников и клиентов (пациентов)) медицинской организации.
Решение ситуационной задачи по вопросу нарушения законодательства Российской Федерации **(самостоятельная работа)**.

Модуль 2. Применение информационных технологий в деятельности медицинской организации (28 час.)
Тема №2.1. Проектирование архитектуры информационной сети (8 час.).
Проектирование архитектуры информационной сети медицинской организации. Обзор рынка аппаратного обеспечения информационной сети медицинской организации. Обзор рынка программного и аппаратного обеспечения информационной сети медицинской организации. Оценка и подбор составляющих аппаратной части информационной системы медицинской организации. Оценка времени прокладки коммуникационных кабелей локальных вычислительных сетей.
Тема №2.2. Организация дистанционной работы (4 час.).
Управление ресурсами медицинской организации через ERP-систему. Организация взаимодействия сотрудников медицинской организации в условиях дистанционного общения (в том числе и во время карантина). Организация дистанционной работы обеспечивающего персонала медицинской организации в период карантина. Организация независимого электронного контроля оценки качества системы менеджмента качества медицинской организации на основе системного подхода. Организация прозрачной системы администрирования организации. Организация работы телемедицинских консультаций. Организация электронного администрирования процессов оформления пациентов в медицинской организации. Организация электронного администрирования процессов обеспечения сохранности и использования медицинских документов пациентов. Организация электронного документооборота медицинской организации и мониторинг его исполнения. Организация прозрачной системы контроля качества деятельности организации.

Решение ситуационной задачи по вопросу организации дистанционной работы **(самостоятельная работа)**.

Тема №2.3. Организация внедрения информационных систем и обучения персонала (8 час.).

Внедрение информационных систем в деятельность медицинской организации. Внедрение прозрачной электронной системы менеджмента качества в медицинской организации. Внедрение электронного мониторинга осведомленности и обучения персонала. Организация обучения персонала для работы в информационной системе медицинской организации. Организация обучения персонала навыкам коммуникации в электронной среде.

Тема №2.4. Сайт медицинской организации (8 час.).

Подготовка общего перечня информации, размещаемой на сайте медицинской организации. Доведение до сведения граждан информации о деятельности медицинской организации. Ведение санитарно-просветительской работы среди населения посредством электронных технологий. Упрощение гражданам доступности медицинской помощи посредством внедрения электронный информационных технологий.

Модуль 3. Угрозы информационной безопасности (28 час.)

Тема №3.1. Обзор основных угроз безопасности информационных систем (4 час.).

Основные угрозы безопасности охраны персональных данных. Основные методы и средства выявления угроз безопасности информационных систем. Основные приёмы получения несанкционированного доступа к данным посредством использования навыков социальной инженерии.

Решение ситуационной задачи по вопросу нахождения и/или устранения угроз безопасности информационных систем **(самостоятельная работа)**.

Тема №3.2. Обеспечение безопасности информационных систем (8 час.).

Основные методы и средства обеспечения безопасности информационных систем, их внедрение. Мероприятия, направленные на обеспечение безопасности информационных систем. Основные тенденции рынка антивирусного программного обеспечения. Подборка и использование антивирусного программного обеспечения.

Тема №3.3. Обеспечение безопасности персональных данных (8 час.).

Использование основных методов обеспечения защиты персональных данных. Выявление основных угроз безопасности охраны персональных данных сотрудников и клиентов (пациентов) медицинской организации. Организация электронного администрирования процессов по обеспечению сохранности использования медицинских документов клиентов (пациентов) медицинской организации. Проведение мероприятий по профилактике утечки персональных данных сотрудников и клиентов (пациентов) медицинской организации и их защите в информационных системах медицинской организации.

Тема №3.4. Составление локальных нормативных правовых актов (8 час.).

Подготовка информированного добровольного согласия на медицинское вмешательство и на отказ от медицинского вмешательства клиентов (пациентов) медицинской организации. Подготовка локальных нормативных правовых актов по вопросу обеспечения безопасности информационных систем медицинской организации. Подготовка локальных нормативных правовых актов по вопросу обработки персональных данных сотрудников и клиентов (пациентов) медицинской организации. Проверка подготовленных локальных нормативных правовых актов на согласованность с законодательством Российской Федерации.

Описание практико-ориентированных заданий и кейсов

Номер темы/модуля	Наименование практического занятия	Описание
Модуль 1.	**Законодательство Российской Федерации в профильных сферах**	

Номер темы/модуля	Наименование практического занятия	Описание
1.1	Обзор законодательства Российской Федерации в сферах здравоохранения, информационных технологий, связи и защиты персональных данных	Тестирование знаний законодательства Российской Федерации в сферах здравоохранения, информационных технологий, связи и защиты персональных данных.
1.2	Нарушения законодательства Российской Федерации	Тестирование знаний основных нарушений законодательства Российской Федерации в сферах здравоохранения, информационных технологий, связи и защиты персональных данных.
Модуль 2.	**Применение информационных технологий в деятельности медицинской организации**	
2.1	Проектирование архитектуры информационной сети	Тестирование знания о проектировании архитектуры информационной сети.
2.2	Организация дистанционной работы	Составить план по переводу функционирования медицинской организации в дистанционный режим: 1. Провести инвентаризацию бизнес-процессов, которые возможно и невозможно реализовывать в дистанционном режиме. 2. Подготовить перечень кадров, которые будут и не будут переведены в дистанционный режим работы. 3. Подготовить распоряжение о переводе сотрудников в дистанционный режим работы.
2.3	Организация внедрения информационных систем и обучения персонала	Составить план организационных мероприятий для внедрения дистанционной системы работы: 1. Провести инвентаризацию бизнес-процессов, которые возможно реализовывать в дистанционном режиме. 2. Осуществить подбор кадров под бизнес-процессы, которые возможно реализовывать в дистанционном режиме. 3. Осуществить закупку аппаратного и программного обеспечения под бизнес-процессы, которые возможно реализовывать в дистанционном режиме. 4. Осуществить обучение кадров работе на новом оборудовании для реализации бизнес-процессов, которые возможно реализовывать в дистанционном режиме.
2.4	Сайт медицинской организации.	Адаптация сайта под работу в дистанционном режиме: 1. Провести инвентаризацию бизнес-процессов, которые возможно реализовывать в дистанционном режиме. 2. Разместить информацию о бизнес-процессах, которые возможно реализовывать в дистанционном режиме, на сайте медицинской организации. 3. Разработать положение о взаимодействии с гражданами в дистанционном режиме.
Модуль 3.	**Угрозы информационной безопасности**	
3.1	Обзор основных угроз безопасности информационных систем	Тестирование знаний об основных угрозах безопасности информационных систем.
3.2	Обеспечение безопасности информационных систем	Тестирование знаний об обеспечении безопасности информационных систем.
3.3	Обеспечение безопасности персональных данных	Разработать положение об обеспечении защиты персональных данных в медицинской организации

Номер темы/модуля	Наименование практического занятия	Описание
3.4	Составление локальных нормативных правовых актов	Разработать правила пользования компьютерами с целью недопущению возможности утечки персональных данных

8. Оценочные материалы по образовательной программе

8.1. Вопросы аттестации

Вопросы входного тестирования	Вопросы промежуточного тестирования	Вопросы итогового тестирования
1. Какой основной нормативный правовой акт, регулирующет отношения, связанные с обработкой персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» Приказ Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 17 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» 2. Какой основной нормативный правовой акт, регулирующет отношения, связанные с созданием и эксплуатацией всех сетей связи и сооружений связи, использованием радиочастотного спектра, оказанием услуг электросвязи и почтовой связи на территории Российской Федерации и на находящихся под юрисдикцией Российской Федерации территориях: Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» 3. Какой основной нормативный правовой акт, регулирующет отношения, возникшие при осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации: Федеральный закон от 07.07.2003 № 126-ФЗ «О связи»	Промежуточная аттестация по модулям не предусмотрена	1. Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это… 1. комплексное обеспечение ИБ 2. безопасность АС 3. угроза ИБ 4. атака на АС 5. политика безопасности 2. Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются: 1. компаньон - вирусами 2. черви 3. паразитические 4. студенческие 5. призраки 6. стелс-вирусы 7. макровирусы 3. К видам системы обнаружения атак относятся: 1. системы, обнаружения атаки на ОС 2. системы, обнаружения атаки на конкретные приложения 3. системы, обнаружения атаки на удаленных БД 4. все варианты верны

Вопросы входного тестирования	Вопросы промежуточного тестирования	Вопросы итогового тестирования
Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» 4. Какой основной нормативный правовой акт определяет требования к размещению информации на официальных сайтах медицинских организациях: Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» Приказ Министерства здравоохранения Российской Федерации от 30.12.2014 N 956н «Требования к содержанию и форме информации о деятельности медицинских организаций, размещаемой на официальных сайтах Министерства здравоохранения Российской Федерации, органов государственной власти субъектов Российской Федерации, органов местного самоуправления и медицинских организаций в информационно-телекоммуникационной сети "Интернет"» 5. Согласно какому основному нормативному правовому акту разрешено проводить обработку персональных данных необходимых для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно: Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» 6. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем называется Информационной войной Информационным оружием Информационным превосходством		

Вопросы входного тестирования	Вопросы промежуточного тестирования	Вопросы итогового тестирования
7. Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним называется: Информационной войной Информационным оружием Информационным превосходством 8. Информация, позволяющая её обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг называется: Государственной тайной Коммерческой тайной Банковской тайной Конфиденциальной информацией 9. Информационной системой называется: Система, которая организует хранение и манипулирование информацией о предметной области Средство для обмена данными между компьютерными системами или между пользователем и компьютерными системами Совокупность программных и языковых средств, обеспечивающих управление базами данных Система, предназначенная для решения прикладных задач 10. Информационной безопасностью организации называется: Состояние защищенности интересов организации в условиях угроз в информационной сфере Процесс, используемый в информационной технологии для обработки защищаемой информации с требуемым уровнем ее защищенности Процесс обнаружения, распознавания и описания рисков Координированные действия по направлению и контролю над деятельностью организации в связи с рисками Система оценивания претендента для прохождения учебного курса дополнительной профессиональной программы - программы повышения квалификации «Планирование, создание и организация работы медицинских учреждений в условиях цифровизации» следующая. На каждый вопрос существует один единственный верный ответ. Правильный ответ на вопрос помечен жирным шрифтом. Каждый правильный ответ пополняет общий счёт правильных ответов у слушателя на 1 балл. Для прохождения курса целесообразно отбирать слушателей, получивших 6 и более баллов на этапе входного тестирования.		

8.2. Описание показателей и критериев оценивания, шкалы оценивания.

На входном этапе контроля сформированности компетенций по тестовым заданиям (вариант состоит из 9 заданий, решение каждого задания оценивается в 1 балл) применяется аналитическая шкала оценивания:

Балл	Критерии оценивания
1	тестовое задание решено верно
0	тестовое задание решено неверно

На входном этапе контроля сформированности компетенций по кейс-задачам применяется аналитическая шкала оценивания:

Балл	Критерии оценивания
5	Обучающийся демонстрирует полное понимание проблемы. Все требования, предъявляемые к заданию, выполнены. Обучающийся самостоятельно, используя полученные знания, решил представленную практическую задачу применительно к реальной или виртуальной организации.
4	Обучающийся демонстрирует значительное понимание проблемы. Все требования, предъявляемые к заданию, выполнены. При выполнении задания допущены незначительные неточности.
3	Демонстрирует частичное понимание проблемы. Большинство требований, предъявляемых к заданию, выполнены. При выполнении задания требовалась значительная помощь преподавателя.
2	Демонстрирует небольшое понимание проблемы, задание выполнено частично.
1	Демонстрирует непонимание проблемы. Попытки выполнения задания были неверными.
0	Нет ответа. Не было попытки решить поставленную практическую задачу.

На этапе итоговой аттестации применяется измерительная шкала оценивания сформированности компетенций.

Критерий оценки	Показатели оценки					
	0	1	2	3	4	5
% правильных ответов	0-19	≥20	≥40	≥60	≥70	≥85

8.3. Примеры контрольных заданий по модулям или всей образовательной программе.

Тестирование по итогам каждого модуля отсутствуют

Пример вопросов из итогового тестирования:

Банк тестовых вопросов:

1. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это….

1. информационная война
2. информационное оружие
3. информационное превосходство

2. Информация, не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.

1. служебная информация
2. коммерческая тайна
3. банковская тайна
4. конфиденциальная информация

3. Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена

1. конфиденциальность
2. целостность
3. доступность
4. аутентичность
5. аппелеруемость

4. Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как

запланировано
1. надежность
2. точность
3. контролируемость
4. устойчивость

8.4. Тесты и обучающие задачи (кейсы), иные практикоориентированные формы заданий.

Модуль 1.

Пример тестового задания:

В каких случаях право субъекта на доступ к его персональным данным может быть ограничено?

1. обработка осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
2. обработка осуществляется в соответствии с законодательством о ПОД/ФТ.
3. обработка осуществляется в случаях, предусмотренных законодательством о транспортной безопасности
4. обработка осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими ему обвинение по уголовному делу или применившими к нему меру пресечения до предъявления обвинения (за исключением случаев, когда допускается ознакомление подозреваемого или обвиняемого с такими персональными данными)

Пример кейс-задачи:

Руководитель медицинской организации разбирает обращение гражданина по вопросу сбора персональных данных гражданина медицинским персоналом. Пациент возражает против сбора персональных данных и требует получения лечения. Регистратор без сбора определённых данных направление на приём врача не выдаёт. Необходимо разъяснить целесообразность и законность сбора персональных данных клиента медицинского учреждения. На какой закон следует сослаться для разрешения упомянутого вопроса.

Модуль 2.

Пример тестового задания:

Возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности:

1. Комплексное обеспечение информационной безопасности
2. Безопасность АС
3. Угрозы информационной безопасности
4. Атака на автоматизированную систему
5. Политика безопасности

Пример кейс-задачи:

Руководитель медицинской организации получил информацию о скорой проверки сайта учреждения. Во избежание наложения штрафа следует проверить и, при необходимости, внести исправления в текущую версию сайта медорганизации. В соответствии с каким нормативным правовым актом необходимо сверить информацию, размещённую на сайте?

Модуль 3.

Пример тестового задания:

Возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности:

К вирусам, не изменяющим среду обитания относятся:

1. черви
2. студенческие
3. полиморфные
4. спутники

Пример кейс-задачи:

Руководитель медицинской организации получил информацию о необходимости организации отдела информационной безопасности в учреждении. Для организации работы

отдела необходимо подготовить положение о деятельности отдела информационной безопасности. Подготовьте упомянутый локальный нормативный акт.

8.5. Описание процедуры оценивания результатов обучения.

Процедура оценивания результатов обучения зависит от типа оценочных материалов. Для тестов с множественным выбором предусмотрено автоматическое оценивание результатов. Для кейс-заданий, тестовых заданий в форме короткого ответа и эссе, аналитических заданий применяется метод ручного оценивания. Разрешено 2 попытки прохождения задания. В качестве результата засчитывается высшая из двух полученных оценок.

Входное и итоговое аттестационные испытания включают тестовые задания с вопросами только закрытого типа.

9. Организационно-педагогические условия реализации программы

9.1. Кадровое обеспечение программы

№ п/п	Фамилия, имя, отчество (при наличии)	Место основной работы и должность, ученая степень и ученое звание (при наличии)	Ссылки на веб-страницы с портфолио (при наличии)	Фото в формате jpeg	Отметка о полученном согласии на обработку персональных данных
1	Кравченко Олег Юрьевич	доцент кафедры Информационных технологий и защиты информации РГЭУ (РИНХ), кандидат физико-математических наук	отсутствует		Согласен на обработку персональных данных

9.2. Учебно-методическое обеспечение и информационное сопровождение

Учебно-методические материалы	
Методы, формы и технологии	**Методические разработки, материалы курса, учебная литература**
- лекции в форме вебинаров - тест	Карпов О.Э., Клейменова Е.Б., Назаренко Г.И., Силаева Н.А. Автоматизированное проектирование медицинских технологических процессов / Под ред. Г.И. Назаренко. – М.: Деловой экспресс, 2016. – 200 с. Обмачевская С.Н. Медицинская информатика. Курс лекций. / Учебное пособие. // М. Изд-во: «Лань». 2019. 184 с. Костюк А.В., Бобонец С.А., Флегонтов А.В., Черных А.К. Информационные технологии: базовый курс. / Учебное пособие. // М. Изд-во: «Лань». 2 издание. 2019. 604 с. Г. И. Назаренко, Я. И. Гулиев, Д. Е. Ермаков. Медицинские информационные системы: теория и практика. / Под редакцией Г. И. Назаренко, Г. С. Осипова. // Москва: «ФИЗМАТЛИТ». 2005. - 320 с. Коваленко В.В. Проектирование информационных систем. Учебное пособие. / Учебное пособие. // М. Изд-во: «Форум». Серия: «Высшее образование». 2018. - 320 с. Григорьева И.И., Григорьев М.В. Проектирование информационных систем. Учебное пособие. / Учебное пособие. // М. Изд-во: «Форум». Серия: «Профессиональное образование». 2019. -319 с. Сабанов А.Г., Зыков В.Д., Мещеряков Р.В., Рылов С.П., Шелупанов А.А. Защита персональных данных в организациях здравоохранения. / М. Научное издание. 2012. -206 с. Масалков А.С. Особенности киберпреступлений. Инструменты нападения и защита информации / Москва. ДМК Пресс. 2018. - 226 с.

Учебно-методические материалы	
Методы, формы и технологии	**Методические разработки, материалы курса, учебная литература**
	Автоматизация процессов, цифровые и информационные технологии в управлении и клинической практике лечебного учреждения: научные труды / Под ред. О.Э. Карпова. – М.: Деловой экспресс, 2016. – 388 с. Андреева Н.М., Василюк Н.Н., Пак Н.И., Хеннер Е.К. Практикум по информатике. / Учебное пособие. // М. Изд-во: «Лань». 2 издание. 2019. 248 с. Мацкевич Д. Руководство «Требования и рекомендации на серверное помещение и системы». 2009. 62 с. Всероссийское добровольное пожарное общество. Система стандартов пожарной безопасности: Автоматические установки газового пожаротушения. Проектирование, монтаж и эксплуатации. – URL: http://kovdpo.ru/pdf/3_04_08.pdf. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации. / Учебное пособие // Москва, Берлин. Изд-ВО: «Директ-Медиа» 2015. - 253 с. Аверченков В. И. Аудит информационной безопасности: учебное пособие. / Под общей редакцией А. П. Курило // М. Изд-во: «Флинта». 2016. – 270 с.

Информационное сопровождение	
Электронные образовательные ресурсы	Электронные информационные ресурсы
Электронный учебно-методический комплекс образовательной программы размещен на портале электронного обучения РГЭУ (РИНХ)– Режим доступа: https://do.rsue.ru	Банк данных угроз безопасности информации – URL: http://bdu.fstec.ru. Официальный сайт государственной системы правовой информации. // Официальный интернет-портал правовой информации – URL: http://pravo.gov.ru/. Официальный сайт Министерства здравоохранения Российской Федерации – URL: https://www.rosminzdrav.ru/. Официальный сайт Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий – URL: https://www.mchs.gov.ru/. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации – URL: https://digital.gov.ru/ru/. Официальный сайт Правительства Российской Федерации – URL: http://government.ru/. Официальный сайт Прокуратуры Российской Федерации – URL: http://www.genproc.gov.ru/. Официальный сайт Уполномоченного органа по защите прав субъектов персональных данных – URL: http://pd.rkn.gov.ru. Официальный сайт Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека – URL: https://www.rospotrebnadzor.ru/. Официальный сайт Федеральной службы по надзору в сфере здравоохранения – URL: https://www.roszdravnadzor.ru/. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций – URL: https://rkn.gov.ru/. Официальный сайт Федеральной службы по техническому и экспортному контролю – URL: https://fstec.ru/.

9.3. Материально-технические условия реализации программы

Вид занятий	Наименование оборудования, программного обеспечения
Лекция	ПЭВМ под управлением операционной системы Microsoft Windows, Linux либо MacOS с установленным веб-браузером (Google Chrome/Mozilla Firefox/Safari/Opera/Яндекс.Браузер/Atom), программа для видеоконференций Zoom..
Практическое занятие	
Самостоятельная работа	

II. **Паспорт компетенций** (Приложение 2)

Приложение 2

ФГБОУ ВО «Ростовский государственный экономический университет (РИНХ)»

ПАСПОРТ КОМПЕТЕНЦИИ

Дополнительная профессиональная программа – программа повышения квалификации «Планирование, создание и организация работы медицинских учреждений в условиях цифровизации»

1.	Наименование компетенции	**понимать законодательство Российской Федерации в сферах проектирования и организации информационных систем в медицинских организациях, защиты персональных данных сотрудников и клиентов (пациентов) медицинских организаций, защиты информационных систем медицинских организаций от вредоносных воздействий**	
2.	Указание типа компетенции	профессиональная	
3.	Определение, содержание и основные сущностные характеристики компетенции	знание, понимание, применение законодательства Российской Федерации в сферах проектирования и организации информационных систем в медицинских организациях, защиты персональных данных сотрудников и клиентов (пациентов) медицинских организаций, защиты информационных систем медицинских организаций от вредоносных воздействий	
4.	Дескриптор знаний, умений и навыков по уровням	**Уровни сформированности компетенции обучающегося**	**Индикаторы**
		Начальный уровень	**Знает**: актуальной нормативно-правовой базы в сфере защиты информационных систем медицинских организаций от вредоносных воздействий; основные методы обеспечения защиты персональных данных
		Базовый уровень	**Знает**: актуальной нормативно-правовой базы в сфере защиты информационных систем медицинских организаций от вредоносных воздействий;
		Продвинутый	**Знает**: актуальной нормативно-правовой базы в сфере проектирования и организации информационных систем в медицинских организациях, защиты персональных данных сотрудников и клиентов (пациентов) медицинских организаций, защиты информационных систем медицинских организаций от вредоносных воздействий
		Профессиональный	**Знает**: актуальной нормативно-правовой базы в сфере проектирования и организации информационных систем в медицинских организациях, защиты персональных данных сотрудников и клиентов (пациентов) медицинских организаций, защиты

			информационных систем медицинских организаций от вредоносных воздействий.
5.	Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции	Владение данной компетенцией является необходимым условием для овладения следующими компетенциями: - организовывать деятельность медицинской организации с применением информационных технологий (в том числе и организовывать дистанционную работу, включая телемедицинские услуги), актуальных современной цифровой экономики; - распознавать возможные угрозы безопасности информационной системы медицинской организации; - организовывать защиту персональных данных сотрудников и клиентов (пациентов) медицинской организации; - организовывать работу по защите информационной системы медицинской организации от возможных несанкционированных доступов и сторонних вредных воздействий.	
6.	Средства и технологии оценки	Тесты, кейс-задачи.	

ПАСПОРТ КОМПЕТЕНЦИИ

Дополнительная профессиональная программа – программа повышения квалификации «Планирование, создание и организация работы медицинских учреждений в условиях цифровизации»

1	Наименование компетенции	**организовывать деятельность медицинской организации с применением информационных технологий (в том числе и организовывать дистанционную работу, включая телемедицинские услуги), актуальных современной цифровой экономики**	
2	Указание типа компетенции	профессиональная	
3	Определение, содержание и основные сущностные характеристики компетенции	знание и умение и применение навыков по организации деятельности медицинской организации с применением информационных технологий (в том числе и организовывать дистанционную работу, включая телемедицинские услуги), актуальных современной цифровой экономики	
4	Дескриптор знаний, умений и навыков по уровням	**Уровни сформированности компетенции обучающегося**	**Индикаторы**
		Начальный уровень	**Владеет умением**: аппаратной части информационных систем
		Базовый уровень	**Обладает умением**: аппаратной части информационных систем; построения архитектуры информационной системы
		Продвинутый	**Обладает навыком**: выявления основных угроз безопасности информационных систем и охраны персональных данных
		Профессиональный	**Владеет умением**: аппаратной части информационных систем **Обладает навыком**: выявления основных угроз безопасности информационных систем и охраны персональных данных; подготовки общего перечня информации, содержащейся на сайте медицинской организации.

5	Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции	Для овладения данной компетенции необходимо владеть следующей компетенцией: - понимать законодательство Российской Федерации в сферах проектирования и организации информационных систем в медицинских организациях, защиты персональных данных сотрудников и клиентов (пациентов) медицинских организаций, защиты информационных систем медицинских организаций от вредоносных воздействий. Владение данной компетенцией является необходимым условием для овладения следующими компетенциями: - распознавать возможные угрозы безопасности информационной системы медицинской организации; - организовывать защиту персональных данных сотрудников и клиентов (пациентов) медицинской организации; - организовывать работу по защите информационной системы медицинской организации от возможных несанкционированных доступов и сторонних вредных воздействий.
6	Средства и технологии оценки	Тесты, кейс-задачи.

ПАСПОРТ КОМПЕТЕНЦИИ

Дополнительная профессиональная программа – программа повышения квалификации «Планирование, создание и организация работы медицинских учреждений в условиях цифровизации»

1	Наименование компетенции	**распознавать возможные угрозы безопасности информационной системы медицинской организации**	
2	Указание типа компетенции	профессиональная	
3	Определение, содержание и основные сущностные характеристики компетенции	знание, умение и применение навыков по распознаванию возможных угроз безопасности информационной системы медицинской организации	
4	Дескриптор знаний, умений и навыков по уровням	**Уровни сформированности компетенции обучающегося**	**Индикаторы**
		Начальный уровень	**Владеет умением**: основных методов и средств обеспечения безопасности информационных систем
		Базовый уровень	**Владеет умением**: основных методов и средств обеспечения безопасности информационных систем; поиска составляющих информационной системы
		Продвинутый	**Обладает навыком**: использования основных методов обеспечения защиты информационных систем и охраны персональных данных
		Профессиональный	**Обладает навыком**: использования основных методов обеспечения защиты информационных систем и охраны персональных данных
	Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции	Для овладения данной компетенции необходимо владеть следующей компетенцией: - понимать законодательство Российской Федерации в сферах проектирования и организации информационных систем в медицинских организациях, защиты персональных данных сотрудников и клиентов (пациентов) медицинских организаций, защиты информационных систем медицинских организаций от вредоносных воздействий;	

		- организовывать деятельность медицинской организации с применением информационных технологий (в том числе и организовывать дистанционную работу, включая телемедицинские услуги), актуальных современной цифровой экономики. Владение данной компетенцией является необходимым условием для овладения следующими компетенциями: - организовывать защиту персональных данных сотрудников и клиентов (пациентов) медицинской организации; - организовывать работу по защите информационной системы медицинской организации от возможных несанкционированных доступов и сторонних вредных воздействий.
	Средства и технологии оценки	практические задания

ПАСПОРТ КОМПЕТЕНЦИИ

Дополнительная профессиональная программа – программа повышения квалификации «Планирование, создание и организация работы медицинских учреждений в условиях цифровизации»

1	Наименование компетенции	**организовывать защиту персональных данных сотрудников и клиентов (пациентов) медицинской организации**	
2	Указание типа компетенции	профессиональная	
3	Определение, содержание и основные сущностные характеристики компетенции	знание и умение и применение навыков по организации защиты персональных данных сотрудников и клиентов (пациентов) медицинской организации	
4	Дескриптор знаний, умений и навыков по уровням	**Уровни сформированности компетенции обучающегося**	**Индикаторы**
		Начальный уровень	**Владеет умением**: использования основных методов обеспечения защиты информационных систем и охраны персональных данных
		Базовый уровень	**Владеет умением**: использования основных методов обеспечения защиты информационных систем и охраны персональных данных
		Продвинутый	**Обладает навыком**: подбора и использования антивирусного программного обеспечения
		Профессиональный	**Обладает навыком**: использования основных методов обеспечения защиты информационных систем и охраны персональных данных
5	Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции	Для овладения данной компетенции необходимо владеть следующей компетенцией: - понимать законодательство Российской Федерации в сферах проектирования и организации информационных систем в медицинских организациях, защиты персональных данных сотрудников и клиентов (пациентов) медицинских организаций, защиты информационных систем медицинских организаций от вредоносных воздействий; - организовывать деятельность медицинской организации с применением информационных технологий (в том числе и организовывать дистанционную работу, включая телемедицинские услуги), актуальных современной цифровой экономики; - распознавать возможные угрозы безопасности информационной системы медицинской организации. Владение данной компетенцией является необходимым условием для овладения следующими компетенцией:	

		- организовывать работу по защите информационной системы медицинской организации от возможных несанкционированных доступов и сторонних вредных воздействий.
6	Средства и технологии оценки	Практические задания

ПАСПОРТ КОМПЕТЕНЦИИ
Дополнительная профессиональная программа – программа повышения квалификации «Планирование, создание и организация работы медицинских учреждений в условиях цифровизации»

<table>
<tr><td>1</td><td>Наименование компетенции</td><td colspan="2">организовывать работу по защите информационной системы медицинской организации от возможных несанкционированных доступов и сторонних вредных воздействий</td></tr>
<tr><td>2</td><td>Указание типа компетенции</td><td colspan="2">профессиональная</td></tr>
<tr><td>3</td><td>Определение, содержание и основные сущностные характеристики компетенции</td><td colspan="2">знание и умение и применение навыков по организации деятельности по защите информационной системы медицинской организации от возможных несанкционированных доступов и сторонних вредных воздействий</td></tr>
<tr><td rowspan="5">4</td><td rowspan="5">Дескриптор знаний, умений и навыков по уровням</td><td>Уровни сформированности компетенции обучающегося</td><td>Индикаторы</td></tr>
<tr><td>Начальный уровень</td><td>Знает:
основных методов обеспечения защиты персональных данных</td></tr>
<tr><td>Базовый уровень</td><td>Обладает умением:
подбора антивирусного программного обеспечения
подготовки локальных нормативных правовых актов</td></tr>
<tr><td>Продвинутый</td><td>Обладает навыком:
подбора составляющих аппаратной части к информационной системы медицинской организации;</td></tr>
<tr><td>Профессиональный</td><td>Обладает навыком:
подготовки локальных нормативных правовых актов в соответствии с актуальным профильным нормативным правовым актам Российской Федерации</td></tr>
<tr><td>5</td><td>Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции</td><td colspan="2">Для овладения данной компетенции необходимо владеть следующей компетенцией:
- понимать законодательство Российской Федерации в сферах проектирования и организации информационных систем в медицинских организациях, защиты персональных данных сотрудников и клиентов (пациентов) медицинских организаций, защиты информационных систем медицинских организаций от вредоносных воздействий;
- организовывать деятельность медицинской организации с применением информационных технологий (в том числе и организовывать дистанционную работу, включая телемедицинские услуги), актуальных современной цифровой экономики;
- распознавать возможные угрозы безопасности информационной системы медицинской организации;
- организовывать защиту персональных данных сотрудников и клиентов (пациентов) медицинской организации.</td></tr>
<tr><td>6</td><td>Средства и технологии оценки</td><td colspan="2">Практические задания</td></tr>
</table>

VI. Иная информация о качестве и востребованности образовательной программы

программа реализуется впервые.

V. Рекомендаций к программе от работодателей: Имеются 2 письма-рекомендации от ООО «Женское Время»; Медицинский центр «Гиппократ».

VI. Указание на возможные сценарии профессиональной траектории граждан по итогам освоения образовательной программы

Текущий статус	Цель
освоение смежных профессиональных областей	повышение уровня дохода, расширение профессиональной деятельности
работающий по найму в организации, на предприятии	развитие профессиональных качеств
	повышение заработной платы
	смена работы без изменения сферы профессиональной деятельности

VII. Дополнительная информация - отсутствует

VIII. Приложенные Скан-копии - Утвержденная образовательная программа

СОГЛАСОВАНО:

Проректор
по развитию образовательных программ Т.В. Торопова

Директор Бизнес-школы О.Н. Степаненко