

федеральное государственное бюджетное образовательное учреждение
высшего образования
"Красноярский государственный медицинский университет
имени профессора В.Ф. Войно-Ясенецкого"
Министерства здравоохранения Российской Федерации

Медико-психолого-фармацевтический факультет

Кафедра медицинской кибернетики и информатики

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

"Информационная безопасность"

уровень магистратуры

очная форма обучения

срок освоения ОПОП ВО - 2 года

2021 год

федеральное государственное бюджетное образовательное учреждение
высшего образования
"Красноярский государственный медицинский университет
имени профессора В.Ф. Войно-Ясенецкого"
Министерства здравоохранения Российской Федерации



УТВЕРЖДАЮ

Проректор по учебной работе

д.м.н., доцент

И.А. Соловьева

«20» октября 2021 г.

РАБОЧАЯ ПРОГРАММА

Дисциплины «Информационная безопасность»

Для ОПОП ВО по специальности 38.04.02 Менеджмент направленность (профиль)
«Управление в здравоохранении на основе интеллектуального анализа данных»

Уровень магистратуры

Очная форма обучения

Срок освоения ОПОП ВО - 2 года

Медико-психолого-фармацевтический факультет

Кафедра медицинской кибернетики и информатики

Курс - I

Семестр - I

Лекции - 8 час.

Практические занятия - 16 час.

Самостоятельная работа - 48 час.

Зачет - I семестр

Всего часов - 72

Трудоемкость дисциплины - 2 ЗЕ

2021 год

1. Вводная часть

1.1. Планируемые результаты освоения образовательной программы по дисциплине

Цель освоения дисциплины "Информационная безопасность" состоит в обучении студентов принципам и средствам обеспечения информационной безопасности в информационной системе.

1.2. Место дисциплины в структуре ОПОП ВО

1.2.1. Дисциплина «Информационная безопасность» относится к блоку Б1 - «Дисциплины (модули)».

Информатика, медицинская информатика

Знания: общих сведений об информационных технологиях и их использовании в профессиональной деятельности; основ современных технологий сбора, обработки и представления информации; классификацию современного программного обеспечения; основные составляющие части архитектуры компьютера, их функции

Умения: использовать современные информационно-коммуникационные технологии (включая пакеты прикладных программ, локальные и глобальные компьютерные сети) для сбора, обработки и анализа информации; использовать современные информационные технологии для получения доступа к источникам информации, хранения и обработки полученной информации

Навыки: применения в профессиональной деятельности базовых знаний в области естествознания, информатики и современных информационных технологий, подготовки документов различной сложности с использованием большинства возможностей текстового редактора; числовой обработки данных с использованием большинства возможностей электронных таблиц; подготовки иллюстративного графического материала с использованием возможностей программы для создания презентаций и графического редактора

1.3. Требования к результатам освоения дисциплины

1.3.1. Изучение данной дисциплины направлено на формирование у обучающихся следующих общекультурных (ОК), общепрофессиональных (ОПК) и профессиональных (ПК) компетенций:

В результате изучения дисциплины обучающиеся должны:

Общие сведения о компетенции УК-7.1	
Вид деятельности	-
Профессиональная задача	-
Код компетенции	УК-7.1
Содержание компетенции	Использует нормативно-правовую базу, правовые, этические правила, стандарты при решении задач искусственного интеллекта
Знать	
1	правовую базу информационного законодательства, правовые нормы и стандарты в области искусственного интеллекта и смежных областей.
2	содержание нормативно-правовых документов в сфере информационных технологий, искусственного интеллекта и информационной безопасности.
Уметь	
1	применять правовые нормы и стандарты в области искусственного интеллекта при создании систем искусственного интеллекта.
2	применять этические нормы и стандарты в области искусственного интеллекта при создании систем искусственного интеллекта.
3	использовать нормативно-правовые документы в сфере информационных технологий, искусственного интеллекта и информационной безопасности при разработке стандартов, норм и правил.
Владеть	
1	нормативно-правовой базой, правовыми, этическими правилами, стандартами при решении задач искусственного интеллекта.
Оценочные средства	
1	Вопросы к зачету
2	Вопросы по теме занятия
3	Практические навыки
4	Ситуационные задачи
5	Примерная тематика рефератов

Общие сведения о компетенции УК-7.2	
Вид деятельности	-
Профессиональная задача	-

Код компетенции	УК-7.2
Содержание компетенции	Разрабатывает стандарты, правила в сфере искусственного интеллекта и смежных областях и использует их в социальной и профессиональной деятельности
Знать	
1	содержание международных и российских стандартов и методологий разработки автоматизированных систем и программного обеспечения, стандартов в области информационной безопасности, подходов к управлению и основные принципы развития и использования технологий искусственного интеллекта.
Уметь	
1	использовать международные и российские стандарты и методологии разработки автоматизированных систем программного обеспечения, стандартов в области информационной безопасности, принципы развития и использования технологий искусственного интеллекта при разработке стандартов, норм и правил в сфере искусственного интеллекта.
Владеть	
1	навыками разработки стандартов, правил в сфере искусственного интеллекта и смежных областях.
Оценочные средства	
1	Вопросы к зачету
2	Вопросы по теме занятия
3	Практические навыки
4	Ситуационные задачи
5	Примерная тематика рефератов

Общие сведения о компетенции УК-7.6	
Вид деятельности	-
Профессиональная задача	-
Код компетенции	УК-7.6
Содержание компетенции	Осуществляет защиту прав результатов интеллектуальной деятельности и средств индивидуализации при создании инновационных продуктов в профессиональной деятельности
Знать	
1	принципы лицензирования и защиты авторских прав при создании инновационных продуктов в области профессиональной деятельности.
Уметь	
1	осуществлять лицензирование и защиту авторских прав при создании инновационных продуктов в области профессиональной деятельности.
Владеть	

1	методами лицензирования и защиты авторских прав при создании инновационных продуктов в области профессиональной деятельности.
Оценочные средства	
1	Вопросы к зачету
2	Вопросы по теме занятия
3	Практические навыки
4	Ситуационные задачи
5	Примерная тематика рефератов

Общие сведения о компетенции ОПК-12.2	
Вид деятельности	-
Профессиональная задача	-
Код компетенции	ОПК-12.2
Содержание компетенции	Применяет инструментальные средства поддержки технологии проектирования и аудита информационных систем и сервисов; методы оценки экономической эффективности и качества, управления надежностью и информационной безопасностью
Знать	
1	особенности модернизации программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач.
Уметь	
1	модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач.
Владеть	
1	навыками модернизации программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач.
Оценочные средства	
1	Вопросы к зачету
2	Вопросы по теме занятия
3	Практические навыки
4	Тесты
5	Примерная тематика рефератов

Общие сведения о компетенции ПК-2.2	
Вид деятельности	-

Профессиональная задача	-
Код компетенции	ПК-2.2
Содержание компетенции	Участствует в проведении экспериментальной проверки работоспособности систем искусственного интеллекта
Знать	
1	методы постановки задач, проведения и анализа тестовых и экспериментальных испытаний работоспособности систем, основанных на знаниях.
Уметь	
1	ставить задачи и участвовать в проведении тестовых и экспериментальных испытаний работоспособности систем, основанных на знаниях, анализировать результаты и вносить изменения.
Владеть	
1	навыками проведения тестовых и экспериментальных испытаний работоспособности систем, основанных на знаниях, анализа результатов и внесения изменения.
Оценочные средства	
1	Вопросы к зачету
2	Вопросы по теме занятия
3	Практические навыки
4	Примерная тематика рефератов

2. ОСНОВНАЯ ЧАСТЬ

2.1. Объем дисциплины и виды учебной работы

		Семестр
Вид учебной работы	Всего часов	I
1	2	3
Аудиторные занятия (всего), в том числе	24	24
Лекции	8	8
Практические занятия	16	16
Из общего числа аудиторных часов - в интерактивной форме*	12 50%	12
Семинары		
Лабораторные работы		
КСР		
Самостоятельная работа студента (СРС), в том числе:	48	48
Подготовка презентаций, рефератов	9	9
Подготовка к занятиям	8	8
Подготовка к тестированию	3	3
Конспектирование источников и другой учебной литературы	4	4
Выполнение упражнений	6	6
Подготовка презентации научного проекта	10	10
Подготовка к промежуточной аттестации	8	8
Вид промежуточной аттестации		Зачет
Контактная работа	24	
Общая трудоемкость час.	72	72
ЗЕ	2	2

2.2. Разделы дисциплины и компетенции, которые должны быть сформированы при их изучении

№ раздела	Наименование раздела дисциплины	Темы разделов дисциплины	Код формируемой компетенции
1	2	3	4
1.	Правовые основы защиты информации в системе здравоохранения РФ.		
		Правовые основы защиты информации в системе здравоохранения РФ.	ПК-2.2, УК-7.1, УК-7.2, УК-7.6, ОПК-12.2
2.	Основные принципы и методы защиты информационной системы.		
		Принципы обеспечения информационной безопасности. Условия успешного функционирования информационной системы.	ПК-2.2, УК-7.1, УК-7.2, УК-7.6, ОПК-12.2
		Направления защиты информации в ИС. Основные виды угроз безопасности ИС и информации.	ПК-2.2, УК-7.1, УК-7.2, УК-7.6, ОПК-12.2
		Методы и технологии защиты информации, конфиденциальности информации в информационных системах. Технологии защиты целостности информации. Методы и технологии защиты доступности информации.	ПК-2.2, УК-7.1, УК-7.2, УК-7.6, ОПК-12.2

2.3. Разделы дисциплины и виды учебной деятельности

№ п/п	№ семестра	Наименование раздела дисциплины	Л	ЛР	ПЗ	Сем	СРС	КСР	Всего
1	2	3	4	5	6	7	8	9	10
1.	1	Правовые основы защиты информации в системе здравоохранения РФ.	2		4		10		16
2.	1	Основные принципы и методы защиты информационной системы.	6		12		38		56
		Всего	8		16		48		72

2.4. Тематический план лекций дисциплины

1 курс

1 семестр

№ раздела	№ темы	Наименование раздела дисциплины	Тема	Количество часов
1	2	3	4	5
1	1	Правовые основы защиты информации в системе здравоохранения РФ. [2.00]	Правовые основы защиты информации в системе здравоохранения РФ. ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2	2
2	2	Основные принципы и методы защиты информационной системы. [2.00]	Принципы обеспечения информационной безопасности. Условия успешного функционирования информационной системы. ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2	2
2	3	Основные принципы и методы защиты информационной системы. [2.00]	Направления защиты информации в ИС. Основные виды угроз безопасности ИС и информации. ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2	2
2	4	Основные принципы и методы защиты информационной системы. [2.00]	Методы и технологии защиты информации, конфиденциальности информации в информационных системах. Технологии защиты целостности информации. Методы и технологии защиты доступности информации. ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2	2
			Всего за семестр	8

			Всего часов	8
--	--	--	--------------------	----------

2.5. Тематический план практических/семинарских занятий

2.5.1. Тематический план практических занятий

1 курс

1 семестр

№ раздела	№ темы	Наименование раздела дисциплины	Тема	Количество часов
1	2	3	4	5
1	1	Правовые основы защиты информации в системе здравоохранения РФ. [4.00]	Правовые основы защиты информации в системе здравоохранения РФ. ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2	4
2	2	Основные принципы и методы защиты информационной системы. [4.00]	Принципы обеспечения информационной безопасности. Условия успешного функционирования информационной системы. (В интерактивной форме) ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2	4
2	3	Основные принципы и методы защиты информационной системы. [4.00]	Направления защиты информации в ИС. Основные виды угроз безопасности ИС и информации. (В интерактивной форме) ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2	4

2	4	Основные принципы и методы защиты информационной системы. [4.00]	Методы и технологии защиты информации, конфиденциальности информации в информационных системах. Технологии защиты целостности информации. Методы и технологии защиты доступности информации. (В интерактивной форме) ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2	4
			Всего за семестр	16
			Всего часов	16

2.5.2. Тематический план семинарских занятий

Данный вид работы учебным планом не предусмотрен

2.6. Тематический план лабораторных работ

Данный вид работы учебным планом не предусмотрен

2.7. Контроль самостоятельной работы

Данный вид работы учебным планом не предусмотрен

2.8. Самостоятельная работа
2.8.1. Виды самостоятельной работы

1 курс
1 семестр

№ раздела	№ темы	Наименование раздела дисциплины	Тема	Вид самост. работы	Количество часов
1	2	3	4	5	6
1	1	Правовые основы защиты информации в системе здравоохранения РФ. [10.00]	Правовые основы защиты информации в системе здравоохранения РФ. ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2	Конспектирование источников и другой учебной литературы [4.00], Подготовка к занятиям [2.00], Подготовка к тестированию [1.00], Подготовка презентаций, рефератов [3.00]	10
2	2	Основные принципы и методы защиты информационной системы. [10.00]	Принципы обеспечения информационной безопасности. Условия успешного функционирования информационной системы. ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2	Выполнение упражнений [3.00], Подготовка к занятиям [3.00], Подготовка к тестированию [1.00], Подготовка презентаций, рефератов [3.00]	10
2	3	Основные принципы и методы защиты информационной системы. [10.00]	Направления защиты информации в ИС. Основные виды угроз безопасности ИС и информации. ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2	Выполнение упражнений [3.00], Подготовка к занятиям [3.00], Подготовка к тестированию [1.00], Подготовка презентаций, рефератов [3.00]	10

2	4	Основные принципы и методы защиты информационной системы. [10.00]	Методы и технологии защиты информации, конфиденциальности информации в информационных системах. Технологии защиты целостности информации. Методы и технологии защиты доступности информации. ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2	Подготовка презентации научного проекта [10.00]	10
2	5	Основные принципы и методы защиты информационной системы. [8.00]	Систематизация изученного материала. ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2	Подготовка к промежуточной аттестации [8.00]	8
			Всего за семестр		48
			Всего часов		48

2.9. Оценочные средства, в том числе для проведения промежуточной аттестации обучающихся по дисциплине

2.9.1. Виды контроля и аттестации, формы оценочных средств

1 семестр					
			Оценочные средства		
№ п/п	Виды контроля	Наименование раздела дисциплины	Форма	Кол-во вопросов в задании	Кол-во независимых вариантов
1	2	3	4	5	6
1	Для входного контроля				
			Тесты	15	20
2	Для текущего контроля				
		Правовые основы защиты информации в системе здравоохранения РФ.			
			Вопросы по теме занятия	3	5
			Ситуационные задачи	2	5
			Тесты	15	20
		Основные принципы и методы защиты информационной системы.			
			Вопросы по теме занятия	3	5
			Ситуационные задачи	2	5
			Тесты	15	20
3	Для промежуточного контроля				
			Вопросы к зачету	2	10
			Практические навыки	1	10
			Тесты	25	10

2.9.2. Примеры оценочных средств

Входной контроль

Тесты

1. НАИБОЛЕЕ РИСКОВАННОЙ ДЛЯ МЕДИЦИНСКОГО УЧРЕЖДЕНИЯ С ТОЧКИ ЗРЕНИЯ ВЕРОЯТНОГО МОШЕННИЧЕСТВА И НАРУШЕНИЯ БЕЗОПАСНОСТИ ЯВЛЯЕТСЯ КАТЕГОРИЯ

1) сотрудники

2) хакеры

3) атакующие

4) контрагенты (лица, работающие по договору)

5) руководство компании

Правильный ответ: 1

ОПК-12.2

2. ПРИ КЛАССИФИКАЦИИ ДАННЫХ РУКОВОДСТВО ДОЛЖНО

1) продумать типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

2) продумать необходимый уровень доступности, целостности и конфиденциальности

3) оценить уровень риска и отменить контрмеры

4) продумать управление доступом, которое должно защищать данные

5) снизить уровень классификации информации, чтобы она была всем доступна

Правильный ответ: 2

ОПК-12.2

3. В КОНЕЧНОМ СЧЕТЕ НЕСЕТ ОТВЕТСТВЕННОСТЬ ЗА ГАРАНТИИ ТОГО, ЧТО ДАННЫЕ КЛАССИФИЦИРОВАНЫ И ЗАЩИЩЕНЫ

1) владелец данных

2) пользователь

3) администратор

4) руководство

5) сотрудник

Правильный ответ: 4

ОПК-12.2

Текущий контроль

Вопросы по теме занятия

1. Что такое «информационный шум»?

ПК-2.2 , УК-7.1 , УК-7.2 , УК-7.6 , ОПК-12.2

2. Каковы предпосылки начала информационной войны?

ПК-2.2 , УК-7.1 , УК-7.2 , УК-7.6 , ОПК-12.2

3. Что такое открытый ключ электронной подписи?

1) Открытый ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и его сертификатом, подтверждающим принадлежность ключа проверки электронной подписи его владельцу.

ПК-2.2 , УК-7.1 , УК-7.2 , УК-7.6 , ОПК-12.2

Ситуационные задачи

1. Ситуационная задача №1: Вы – руководитель отдела информационной безопасности организации. Вы подозреваете, что один из пользователей корпоративной информационной системы создает и распространяет вредоносные программы внутри сети.

1) Какая статья уголовного кодекса была нарушена?

2) Какое наказание должен понести нарушитель?

Ответ 1: Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

Ответ 2: Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

УК-7.2 , УК-7.1

2. Ситуационная задача №2: Вы готовите доклад по методам и концепции информационных войн.

1) Перечислите способы поражения и разрушения сознания информационными войнами.

2) Какова концепция информационной войны?

Ответ 1: Можно выделить пять основных способов поражения и разрушения сознания: 1) Поражение нейромозгового субстрата, снижающее уровень функционирования сознания, может происходить на основе действия химических веществ, длительного отравления воздуха, пищи, направленных радиационных воздействий. 2) Понижение уровня организации

информационно—коммуникативной среды на основе ее дезинтеграции и примитивизации, в которой функционирует и живет сознание. 3) Окультизм: воздействие на организацию сознания на основе направленной передачи мыслеформ субъекту поражения. 4) Специальная организация и распространение по каналам коммуникации образов и текстов, которые разрушают работу сознания (условно может быть обозначено как психотропное оружие). 5) Разрушение способов и форм идентификации личности по отношению к фиксированным общностям, приводящее к смене форм самоопределения и к деперсонализации.

Ответ 2: Концепция информационной войны: 1) подавление элементов инфраструктуры государственного, военного управления; 2) радиоэлектронная борьба (электронно-магнитное воздействие); 3) радиоэлектронная разведка; 4) хакерная война; 5) формирование и массовое распространение по информационным каналам противника или глобальным сетям дезинформации.

УК-7.2 , УК-7.6

3. Ситуационная задача №3: Вы владеете сертификатом ключа подписи.

- 1) Каковы обязательства владельца сертификата ключа подписи?
- 2) Как происходит приостановление действия сертификата ключа подписи?

Ответ 1: Владелец сертификата ключа подписи обязан: не использовать для электронной цифровой подписи открытые и закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются или использовались ранее; хранить в тайне закрытый ключ электронной цифровой подписи; немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа электронной цифровой подписи нарушена.

Ответ 2: 1. Действие сертификата ключа подписи может быть приостановлено удостоверяющим центром на основании указания лиц или органов, имеющих такое право в силу закона или договора, а в корпоративной информационной системе также в силу установленных для нее правил пользования. 2. Период от поступления в удостоверяющий центр указания о приостановлении действия сертификата ключа подписи до внесения соответствующей информации в реестр сертификатов ключей подписей должен устанавливаться в соответствии с общим для всех владельцев сертификатов ключей подписей правилом. По договоренности между удостоверяющим центром и владельцем сертификата ключа подписи этот период может быть сокращен. 3. Действие сертификата ключа подписи по указанию полномочного лица (органа) приостанавливается на исчисляемый в днях срок, если иное не установлено нормативными правовыми актами или договором. Удостоверяющий центр возобновляет действие сертификата ключа подписи по указанию полномочного лица (органа). В случае, если по истечении указанного срока не поступает указание о возобновлении действия сертификата ключа подписи, он подлежит аннулированию. 4. В соответствии с указанием полномочного лица (органа) о приостановлении действия сертификата ключа подписи удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты, времени и срока приостановления действия сертификата ключа подписи, а также извещает об этом владельца сертификата ключа подписи и полномочное лицо (орган), от которого получено указание о приостановлении действия сертификата ключа подписи.

УК-7.1 , УК-7.2

Тесты

1. СОТРУДНИК УЧРЕЖДЕНИЯ МОЖЕТ БЫТЬ ПРИВЛЕЧЕН К ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЛУЧАЕ

- 1) выхода в интернет без разрешения администратора
- 2) при установке компьютерных игр
- 3) установки нелицензионного ПО
- 4) не выхода из информационной системы

5) в любом случае неправомерного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности

Правильный ответ: 5

ОПК-12.2

2. БОМБАРДИРОВКА АТС - ЭТО

- 1) средство информационной войны**
- 2) метод информационной войны
- 3) операция информационной войны
- 4) оружие информационной войны
- 5) информационная война

Правильный ответ: 1

ОПК-12.2

3. АНТИВИРУС, КОТОРЫЙ ЗАПОМИНАЕТ ИСХОДНОЕ СОСТОЯНИЕ ПРОГРАММ, КАТАЛОГОВ И СИСТЕМНЫХ ОБЛАСТЕЙ ДИСКА КОГДА КОМПЬЮТЕР НЕ ЗАРАЖЕН ВИРУСОМ, А ЗАТЕМ ПЕРИОДИЧЕСКИ ИЛИ ПО КОМАНДЕ ПОЛЬЗОВАТЕЛЯ СРАВНИВАЕТ ТЕКУЩЕЕ СОСТОЯНИЕ С ИСХОДНЫМ, НАЗЫВАЕТСЯ

- 1) детектор
- 2) доктор
- 3) сканер
- 4) ревизор**
- 5) сторож

Правильный ответ: 4

ОПК-12.2

Промежуточный контроль

Вопросы к зачету

1. Классификация компьютерных преступлений

1) Несмотря на многообразие компьютерных преступлений, их можно классифицировать по отдельным общим группам. В начале 90-х гг. XX века рабочая группа в рамках Интерпола разработала специальный классификатор. В соответствии с ним все компьютерные преступления классифицированы следующим образом. 1. QA — несанкционированный доступ и перехват: QAH — компьютерный абордаж (несанкционированный доступ); QAI — перехват с помощью специальных технических средств; QAT — кража времени (уклонение от платы за пользование); QAZ — иные виды несанкционированного доступа и перехвата. 2. QD — изменение компьютерных данных: QDL — логическая бомба; GDT — троянский конь; QDV — компьютерный вирус; QDW — компьютерный червь; QDZ — прочие виды данных. 3. QF — компьютерное мошенничество: QFC — мошенничество с банкоматами; QFF — компьютерная подделка; QFG — мошенничество с игровыми автоматами; QFM — манипуляции с программами ввода-вывода; QFP — мошенничество с платежными средствами; QFT — телефонное мошенничество; QFZ — прочие компьютерные мошенничества. В соответствии с УК РФ выделяют следующие преступления в сфере компьютерной информации: Неправомерный доступ к компьютерной информации; Создание, использование и распространение вредоносных компьютерных программ; Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

ПК-2.2 , УК-7.1 , УК-7.2 , УК-7.6 , ОПК-12.2

2. Симметричные методы криптографии

1) Криптография сегодня по праву считается одним из разделов математики, который занимается разработкой методов и алгоритмов шифрования данных. Преобразование текста из открытого сообщения в шифротекст называется зашифровыванием (шифрацией). Обратное преобразование шифротекста в исходное сообщение назовем расшифровыванием (дешифрацией). Зашифровывание и расшифровывание должно производиться по определенному методу, называемому алгоритмом зашифровывания. Любой конкретный алгоритм содержит некоторый набор параметров, позволяющих всякий раз использовать его для шифрации. Таким образом, для понятий метода и ключа шифрования введем следующие определения. Метод шифрования - это формальный алгоритм, описывающий порядок преобразования исходного сообщения в шифрованное. Ключ шифрования - это набор параметров (данных), необходимых для применения метода. Если при зашифровывании и расшифровывании применялся один и тот же ключ, то такой метод называется симметричным. Существует достаточно много методов симметричного шифрования. Как известно, Юлий Цезарь для связи со своими военачальниками использовал метод подстановки с ключом, равным 3. В исходном сообщении каждый символ заменялся другим символом, отстоящим от него в алфавите на 3 позиции вправо.

ПК-2.2 , УК-7.1 , УК-7.2 , УК-7.6 , ОПК-12.2

3. Персональные данные

1) Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» определяет 6 категорий конфиденциальных сведений. Это: Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях. Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской

Федерации и федеральными законами (служебная тайна). Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее). Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна). Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них. Иными словами, конфиденциальная информация – это информация с ограниченным доступом, не содержащая государственную тайну. Абсолютное большинство информационных ресурсов медицинских учреждений содержат те или иные сведения конфиденциального характера (служебная, коммерческая, врачебная тайна) и в соответствии с частью 4 ст. 9 Закона «Об информации, информационных технологиях и о защите информации» доступ к ней должен быть ограничен. При этом наибольшее внимание современное законодательство уделяет защите персональных данных. Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных» устанавливает, что «персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)». Под обработкой персональных данных следует понимать «любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных». Важно, что под обработкой понимаются любые действия, как с использованием средств автоматизации (т.е. средств вычислительной техники), так и без этих средств. Иными словами, если персональные данные собираются, накапливаются и хранятся (т.е. обрабатываются) на бумажных носителях, в виде, например, традиционной бумажной медицинской документации, то на любые действия с этой документацией распространяется действие данного Федерального закона. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств. Таким образом, если в медицинской информационной системе обрабатываются персональные данные (а именно это и происходит в абсолютном большинстве медицинских информационных систем), то эта система является информационной системой персональных данных. Первейшим условием обработки персональных данных является согласие субъекта персональных данных на обработку этих данных. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Согласие должно включать в себя, в частности: 1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе; 2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных); 3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных; 4) цель обработки персональных данных; 5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных; 6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу; 7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных; 8) срок, в течение которого

действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом; 9) подпись субъекта персональных данных. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных только при наличии оснований, перечисленных в Законе.

ПК-2.2 , УК-7.1 , УК-7.2 , УК-7.6 , ОПК-12.2

Практические навыки

1. Создать sfx-архив файла с помощью программы 7-zip

1) Запустить программу «Пуск – Программы – «7-Zip»; указать путь к папке, где находится файл; выделить указателем мыши файл, подлежащий архивации и нажать кнопку Добавить; в открывшемся окне необходимо уточнить, если нужно, имя архивного файла и поставить галочку "Создать SFX-архив"; нажать кнопку "ОК".

ПК-2.2 , УК-7.1 , УК-7.2 , УК-7.6 , ОПК-12.2

2. Создать электронную подпись заданного текстового фрагмента с помощью программы PGP

1) Выделить фрагмент текста; скопировать его в буфер обмена; щелкнуть правой кнопкой мыши на значке PGP на панели задач; выбрать пункт "ClipboardSign"; выбрать владельца электронной подписи; вставить из буфера обмена сформированную электронную подпись после исходного текстового фрагмента.

ПК-2.2 , УК-7.6 , УК-7.1 , УК-7.2 , ОПК-12.2

3. Определить IP-адрес компьютера

1) Нажать сочетание клавиш "Win R"; в появившемся окне "Выполнить" написать "cmd"; нажать кнопку "ОК"; в появившейся командой строке написать "ipconfig /all".

ПК-2.2 , УК-7.1 , УК-7.2 , УК-7.6 , ОПК-12.2

Тесты

1. ИНФОРМАЦИЯ В ЭЛЕКТРОННОЙ ФОРМЕ, КОТОРАЯ ПРИСОЕДИНЕНА К ДРУГОЙ ИНФОРМАЦИИ В ЭЛЕКТРОННОЙ ФОРМЕ (ПОДПИСЫВАЕМОЙ ИНФОРМАЦИИ) И КОТОРАЯ ИСПОЛЬЗУЕТСЯ ДЛЯ ОПРЕДЕЛЕНИЯ ЛИЦА, ПОДПИСЫВАЮЩЕГО ИНФОРМАЦИЮ - ЭТО

- 1) электронная подпись**
- 2) ключ электронной подписи
- 3) открытый ключ проверки электронной подписи
- 4) сертификат открытого ключа электронной подписи
- 5) закрытый ключ электронной подписи

Правильный ответ: 1

ОПК-12.2

2. НЕКАЯ УНИКАЛЬНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ СИМВОЛОВ, ЗАПИСАННАЯ НА ЭЛЕКТРОННЫЙ НОСИТЕЛЬ (ФЛЭШ-КАРТУ ИЛИ СМАРТ-КАРТУ) - ЭТО

1) ключ электронной подписи

2) электронная подпись

3) сертификат открытого ключа электронной подписи

4) открытый ключ проверки электронной подписи

5) закрытый ключ электронной подписи

Правильный ответ: 1

ОПК-12.2

3. ИНФОРМАЦИОННАЯ ВОЙНА - ЭТО

1) атака против информационной функции, зависящая от применяемых средств

2) атака против информационной функции, независимо от применяемых средств

3) любая атака против информационной функции

4) любая атака против информационной функции, независимо от применяемых средств

5) любая атака против информационной функции, зависящая от применяемых средств

Правильный ответ: 4

ОПК-12.2

2.10. Примерная тематика курсовых работ (проектов)
Данный вид работы учебным планом не предусмотрен

2.11. Перечень практических умений/навыков

1 курс

1 семестр

№ п/п	Практические умения
1	2
1	Применять правовые нормы и стандарты в области искусственного интеллекта при создании систем искусственного интеллекта. Уровень: Уметь УК-7.1
2	Применять этические нормы и стандарты в области искусственного интеллекта при создании систем искусственного интеллекта. Уровень: Уметь УК-7.1
3	Использовать нормативно-правовые документы в сфере информационных технологий, искусственного интеллекта и информационной безопасности при разработке стандартов, норм и правил. Уровень: Уметь УК-7.1
4	Нормативно-правовой базой, правовыми, этическими правилами, стандартами при решении задач искусственного интеллекта. Уровень: Владеть УК-7.1
5	Использовать международные и российские стандарты и методологии разработки автоматизированных систем программного обеспечения, стандартов в области информационной безопасности, принципы развития и использования технологий искусственного интеллекта при разработке стандартов, норм и правил в сфере искусственного интеллекта. Уровень: Уметь УК-7.2
6	Навыками разработки стандартов, правил в сфере искусственного интеллекта и смежных областях. Уровень: Владеть УК-7.2
7	Осуществлять лицензирование и защиту авторских прав при создании инновационных продуктов в области профессиональной деятельности. Уровень: Уметь УК-7.6
8	Методами лицензирования и защиты авторских прав при создании инновационных продуктов в области профессиональной деятельности. Уровень: Владеть УК-7.6
9	Модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач. Уровень: Уметь ОПК-12.2

10	Навыками модернизации программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач. Уровень: Владеть ОПК-12.2
11	Ставить задачи и участвовать в проведении тестовых и экспериментальных испытаний работоспособности систем, основанных на знаниях, анализировать результаты и вносить изменения. Уровень: Уметь ПК-2.2
12	Навыками проведения тестовых и экспериментальных испытаний работоспособности систем, основанных на знаниях, анализа результатов и внесения изменения. Уровень: Владеть ПК-2.2

2.12. Примерная тематика рефератов (эссе)

1 курс

1 семестр

№ п/п	Темы рефератов
1	2
1	Искусственный интеллект в информационной безопасности. ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2
2	Искусственный интеллект: возможности и угрозы. ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2
3	Как технологии искусственного интеллекта могут противостоять кибератакам? ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2
4	Искусственный интеллект и анализ данных. ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2
5	Искусственный интеллект - прорывная технология в информационной безопасности. ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2
6	Почему искусственный интеллект все чаще принимают на кибервооружение? ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2
7	Нужна ли защита для искусственного интеллекта? ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2
8	Робот-хакер. ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2
9	Стоит ли бояться искусственного интеллекта? ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2
10	Медицина и искусственный интеллект: возможно ли это? ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2

2.13. Учебно-методическое и информационное обеспечение дисциплины

2.13.1. Перечень основной литературы, необходимой для освоения дисциплины

				Кол-во экземпляров	
№ п/п	Наименование, вид издания	Автор(-ы), составитель(-и), редактор(-ы)	Место издания, издательство, год	В библиотеке	На кафедре
1	2	3	4	5	6
1	Информационная безопасность и защита информации : учебное пособие. - Текст : электронный. - URL: https://ibooks.ru/reading.php?productid=361272	Е. К. Баранова, А. В. Бабаш	М. : РИОР : ИНФРА-М, 2019.	ЭБС iBooks	-/-

2.13.2. Перечень дополнительной литературы, необходимой для освоения дисциплины

				Кол-во экземпляров	
№ п/п	Наименование, вид издания	Автор(-ы), составитель(-и), редактор(-ы)	Место издания, издательство, год	В библиотеке	На кафедре
1	2	3	4	5	6
1	Информатика и информационные технологии : учебник для вузов. - Текст : электронный. - URL: https://urait.ru/viewer/informatika-i-informacionnye-tehnologii-468473#page/1	М. В. Гаврилов, В. А. Климов	Москва : Юрайт, 2021.	ЭБС Юрайт	-/-
2	Информационные технологии : учебник для вузов. - Текст : электронный. - URL: https://urait.ru/viewer/informacionnye-tehnologii-468634#page/1	Б. Я. Советов, В. В. Цехановский	М. : Юрайт , 2021.	ЭБС Юрайт	-/-
3	Медицинская информатика : учебник. - Текст : электронный. - URL: http://www.studmedlib.ru/ru/book/ISBN9785970436455.html	В. П. Омельченко, А. А. Демидова	Москва : ГЭОТАР-Медиа, 2016.	ЭБС Консультант студента (ВУЗ)	-/-

4	Медицинская информатика : учебник. - Текст : электронный. - URL: https://www.studentlibrary.ru/book/ISBN9785970445730.html	ред. Т. В. Зарубина, Б. А. Кобринский	Москва : ГЭОТАР-Медиа, 2018.	ЭБС Консультант студента (ВУЗ)	-/-
5	Медицинская информатика. Курс лекций : учебное пособие для вузов. - Текст : электронный. - URL: https://reader.lanbook.com/book/154391#1	С. Н. Обмачевская	Санкт-Петербург : Лань, 2021.	ЭБС Лань	-/-

2.13.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Порядковый номер	1
Наименование	Лекции по информационной безопасности
Вид	Интернет-ресурс
Форма доступа	http%3A%2F%2Fcourse.secsem.ru%2Flections
Рекомендуемое использование	Для подготовки к занятиям

Порядковый номер	2
Наименование	Информатика для начинающих. Видеолекции
Вид	Интернет-ресурс
Форма доступа	https%3A%2F%2Fwww.youtube.com%2Fplaylist%3Flist%3DPLho0jPY15RAEDNZnWd-xFfnIDvLJQ7FES
Рекомендуемое использование	Для самостоятельного изучения, подготовки к занятиям

Порядковый номер	3
Наименование	Кибер-безопасность и десять сфер ее применения. Дистанционный курс
Вид	Интернет-ресурс
Форма доступа	https%3A%2F%2Fwww.coursera.org%2Flearn%2Fcyber-security-domain
Рекомендуемое использование	Для подготовки к занятиям, самостоятельного изучения

Порядковый номер	4
Наименование	Единый портал электронной подписи
Вид	Интернет-ресурс
Форма доступа	www.iecp.ru
Рекомендуемое использование	Для самостоятельного изучения, подготовки к занятиям

2.13.4. Карта перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем по специальности 38.04.02 Менеджмент направленность (профиль) «Управление в здравоохранении на основе интеллектуального анализа данных» для очной формы обучения

№ п/п	Вид	Наименование	Режим доступа	Доступ	Рекомендуемое использование
1	2	3	4	5	6
1.	Видеоуроки практических навыков	-/-	-/-	-/-	-/-
2.	Видеолекции	-/-	-/-	-/-	-/-
3.	Учебно-методический комплекс для дистанционного обучения	-/-	-/-	-/-	-/-
4.	Программное обеспечение	-/-	-/-	-/-	-/-
5.	Информационно-справочные системы и базы данных	ЭБС КрасГМУ «Colibris» ЭБС Консультант студента ВУЗ ЭБС Консультант студента Колледж ЭБС Айбукс ЭБС Букап ЭБС Лань ЭБС Юрайт ЭБС MedLib.ru НЭБ eLibrary БД Web of Science БД Scopus ЭМБ Консультант врача Wiley Online Library Springer Nature ScienceDirect (Elsevier) СПС КонсультантПлюс	https://krasgmu.ru http://www.studmedlib.ru/ http://www.medcollegelib.ru/ https://ibooks.ru/ https://www.books-up.ru/ https://e.lanbook.com/ https://www.biblio-online.ru/ https://www.medlib.ru https://elibrary.ru/ http://webofscience.com/ https://www.scopus.com/ http://www.rosmedlib.ru/ http://search.ebscohost.com/ http://onlinelibrary.wiley.com/ http://journals.cambridge.org/ https://rd.springer.com/ https://www.sciencedirect.com/ http://www.consultant.ru/	По логину/паролю По логину/паролю По логину/паролю По логину/паролю По логину/паролю По логину/паролю По логину/паролю По логину/паролю По логину/паролю, по IP-адресу По логину/паролю, по IP-адресу По IP-адресу По логину/паролю По IP-адресу По IP-адресу По IP-адресу По IP-адресу По IP-адресу По IP-адресу По IP-адресу По IP-адресу	Для самостоятельной работы, при подготовке к занятиям

2.13.5. Материально-техническая база дисциплины, необходимая для осуществления образовательного процесса по дисциплине "Информационная безопасность" по специальности 38.04.02 Менеджмент направленность (профиль) «Управление в здравоохранении на основе интеллектуального анализа данных» (Очное, Высшее образование, 2,00) для очной формы обучения

№ п/п	Наименование	Кол-во	Форма использования
1	2	3	4
	Аудитория №1		аудитория для проведения занятий лекционного типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 17E0-180524-112536-910-593
1	Проектор	1	
2	Микрофон	1	
3	Доска	1	
4	Компьютер	1	
5	Колонки	1	
6	Проекционный экран	1	
7	Трибуна	1	
8	Столы	60	
9	Посадочные места	360	
10	Индукционная система Исток С1и	1	
11	Акустический усилитель и колонки	1	

	Аудитория №2		аудитория для проведения занятий лекционного типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 17E0-180524-112536-910-593
1	Проектор	1	
2	Микрофон	1	
3	Доска	1	
4	Компьютер	1	
5	Колонки	1	
6	Проекционный экран	1	
7	Трибуна	1	
8	Стол	60	
9	Посадочные места	360	
	Аудитория №3		аудитория для проведения занятий лекционного типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 17E0-180524-112536-910-593
1	Проектор	1	
2	Микрофон	1	
3	Доска	1	
4	Компьютер	1	
5	Колонки	1	

6	Проекционный экран	1	
7	Трибуна	1	
8	Столы	32	
9	Посадочные места	256	
	Лекционный зал лабораторного корпуса		аудитория для проведения занятий лекционного типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 17E0-180524-112536-910-593
1	Проектор	1	
2	Микрофон	1	
3	Доска	1	
4	Компьютер	1	
5	Колонки	1	
6	Проекционный экран	1	
7	Трибуна	1	
8	Столы	60	
9	Посадочные места	300	
10	Индукционная система Исток С1и	1	
	Лекционный зал морфологического корпуса		аудитория для проведения занятий лекционного типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 17E0-180524-112536-910-593

1	Проектор	1	
2	Микрофон	1	
3	Доска	1	
4	Компьютер	1	
5	Колонки	1	
6	Проекционный экран	1	
7	Трибуна	1	
8	Стол	100	
9	Посадочные места	350	
10	Индукционная система Исток С1и	1	
11	Акустический усилитель и колонки	1	
	Актовый зал		аудитория для проведения занятий лекционного типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 17E0-180524-112536-910-593
1	Проектор	1	
2	Микрофон	2	
3	Доска	3	
4	Компьютер	1	
5	Колонки	1	
6	Проекционный экран	1	
7	Трибуна	1	
8	Стол	40	

9	Посадочные места	200	
10	Индукционная система Исток С1и	1	
11	Акустический усилитель и колонки	1	
	Компьютерный класс №1 (3-03)		учебная аудитория для проведения занятий семинарского типа, аудитория для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 17E0-180524-112536-910-593 Свободно распространяемое ПО: Google Chrome, Mozilla Firefox, Adobe Reader, VLC Media Player, 7-zip, Daemon Tools Lite, Firebird, Gimp, PSPP, R, GNU Octave, STADIA, Bloodshed Dev-C++, Open Office, AnyLogic Personal Learning Edition
1	Видеопроектор	1	
2	Комплект учебной мебели, посадочных мест	13	
3	Сетевой сервер	1	
4	Экран	1	
5	Аудиоколонки	1	
6	Доска магнитно-маркерная	1	
7	Персональные компьютеры	12	
	Компьютерный класс №2 (2-103а)		учебная аудитория для проведения занятий семинарского типа, аудитория для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 17E0-180524-112536-910-593 Свободно распространяемое ПО: Google Chrome, Mozilla Firefox, Adobe Reader, VLC Media Player, 7-zip, Daemon Tools Lite, Firebird, Gimp, PSPP, R, GNU Octave, STADIA, Bloodshed Dev-C++, Open Office, AnyLogic Personal Learning Edition

1	Комплект учебной мебели, посадочных мест	17	
2	Видеопроектор	1	
3	Клавиатура со шрифтом Брайля	1	
4	Локальный сетевой сервер	1	
5	Клавиатура программируемая крупная адаптивная	1	
6	Экран	1	
7	Ресивер для подключения устройств	1	
8	Аудиоколонки	2	
9	Индукционная система Исток С1и	1	
10	Доска магнитно-маркерная	1	
11	Джойстик компьютерный	1	
12	Персональные компьютеры	16	
13	Специализированное ПО: экранный доступ JAWS	1	
	Компьютерный класс №3 (3-46)		учебная аудитория для проведения занятий семинарского типа, аудитория для проведения занятий лекционного типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 17E0-180524-112536-910-593 qMS: Лиц. Серт б/н Свободно распространяемое ПО: Google Chrome, Mozilla Firefox, Adobe Reader, VLC Media Player, 7-zip, Daemon Tools Lite, Firebird, Gimp, PSPP, R, GNU Octave, STADIA, Bloodshed Dev-C++, Open Office, AnyLogic Personal Learning Edition
1	Комплект учебной мебели, посадочных мест	21	
2	Видеопроектор	1	
3	Локальный сетевой сервер	1	

4	Экран	1	
5	Аудиоколонки	2	
6	Доска магнитно-маркерная	1	
7	Персональные компьютеры	20	
	Компьютерный класс №5 (3-90)		учебная аудитория для проведения занятий семинарского типа, аудитория для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 17E0-180524-112536-910-593 Свободно распространяемое ПО: Google Chrome, Mozilla Firefox, Adobe Reader, VLC Media Player, 7-zip, Daemon Tools Lite, Firebird, Gimp, PSPP, R, GNU Octave, STADIA, Bloodshed Dev-C++, Open Office, AnyLogic Personal Learning Edition
1	Комплект учебной мебели, посадочных мест	15	
2	Видеопроектор	1	
3	Локальный сетевой сервер	1	
4	Экран	1	
5	Аудиоколонки	1	
6	Персональные компьютеры	14	
	Читальный зал УБИЦ		аудитория для самостоятельной работы Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 17E0-180524-112536-910-593
1	Проектор	1	
2	Клавиатура со шрифтом Брайля	13	
3	Экран	1	

4	Ноутбук	1	
5	Персональный компьютер	18	
6	Сканирующая и читающая машина CARA CE	1	
7	Стол	30	
8	Посадочные места	43	
9	Индукционная система Исток С1и	1	
10	Головная компьютерная мышь	1	
11	Клавиатура программируемая крупная адаптивная	1	
12	Джойстик компьютерный	1	
13	Принтер Брайля (рельефно-точечный)	1	
14	Специализированное ПО: экранный доступ JAWS	1	
15	Ресивер для подключения устройств	1	

2.14. Образовательные технологии

Используемые образовательные технологии при изучении данной дисциплины: интерактивные технологии, информационно-коммуникационные технологии. 50 % интерактивных часов от объема аудиторных часов. В рамках изучения дисциплины «Информационная безопасность» обучение студентов производится на лекциях, аудиторных (практических) занятиях, а также в результате самостоятельного изучения отдельных тем. Занятия проводятся с использованием следующих методов обучения: объяснительно-иллюстративный, метод проблемного изложения, эвристический. В рамках изучения дисциплины проводятся следующие разновидности лекций: академическая лекция, лекция-беседа, лекция с разбором конкретных ситуаций. Проводятся следующие разновидности аудиторных (практических) занятий: традиционный, с использованием докладов по вопросам темы занятия, конференция, работа в малых группах, защита презентаций, упражнение, просмотр и обсуждение видеофрагментов. Внеаудиторная (самостоятельная) работа обучающихся включает следующие виды учебной деятельности: конспектирование источников и другой учебной литературы, подготовку презентаций и рефератов, выполнение упражнений, подготовку к тестированию, подготовку к занятиям, подготовку презентации научного проекта.

2.15. Разделы дисциплины и междисциплинарные связи с последующими дисциплинами

		Разделы дисциплины, необходимые для изучения последующих дисциплин	
№ п/п	Наименование последующих дисциплин	1	2
1	Информационные медицинские системы	+	+

2.16. Методические указания для обучающихся по освоению дисциплины

Обучение складывается из аудиторных занятий (24 час.), включающих лекционный курс и практические занятия, и самостоятельной работы (48 час.) Основное учебное время выделяется на работу с нормативными актами, регулирующими правоотношения в области информации, обеспечению мер безопасности в интернете, обществе и учреждении. При изучении дисциплины необходимо освоить практические умения по обеспечению безопасности в интернете, обществе и учреждении. Практические занятия проводятся в виде демонстрации слайдов, решения ситуационных задач, ответов на тестовые задания, отработки практических навыков по работе на ПК. В учебном процессе широко используются активные и интерактивные формы проведения занятий: работа в малых группах, выполнение упражнений. Самостоятельная работа обучающихся подразумевает конспектирование источников и другой учебной литературы, подготовку презентаций и рефератов, выполнение упражнений, подготовку к тестированию, подготовку к занятиям, подготовку презентации научного проекта. Каждый обучающийся обеспечен доступом к библиотечным фондам университета и кафедры. По каждому разделу учебной дисциплины разработаны методические указания для обучающихся и методические рекомендации для преподавателей. Во время освоения учебной дисциплины обучающиеся самостоятельно проводят изучение теоретического материала и выполнение учебных заданий. Исходный уровень знаний обучающихся определяется тестированием, текущий контроль усвоения предмета определяется тестированием, решением ситуационных задач, устным опросом по вопросам к занятиям. В конце изучения учебной дисциплины проводится трехэтапный зачет, включающий тестовый контроль, собеседование и оценку практических навыков.

2.17. Особенности организации обучения по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья

1. Обучение инвалидов и лиц с ограниченными возможностями здоровья

по заявлению обучающегося кафедрой разрабатывается адаптированная рабочая программа с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья обучающегося.

2. В целях освоения учебной программы дисциплины инвалидами и лицами с ограниченными возможностями здоровья кафедра обеспечивает:

1) для инвалидов и лиц с ограниченными возможностями здоровья по зрению:

- размещение в доступных местах и в адаптированной форме справочной информации о расписании учебных занятий для обучающихся, являющихся слепыми или слабовидящими;
- присутствие преподавателя, оказывающего обучающемуся необходимую помощь;
- выпуск альтернативных форматов методических материалов (крупный шрифт или аудиофайлы);

2) для инвалидов и лиц с ограниченными возможностями здоровья по слуху:

- надлежащими звуковыми средствами воспроизведения информации;

3) для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата:

- возможность беспрепятственного доступа обучающихся в учебные помещения, туалетные комнаты и другие помещения кафедры. В случае невозможности беспрепятственного доступа на кафедру организовывать учебный процесс в специально оборудованном помещении (ул. Партизана Железняка, 1, Университетский библиотечно-информационный центр: электронный читальный зал (ауд. 1-20), читальный зал (ауд. 1-21).

3. Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах.

4. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Категории студентов	Оборудование	Формы
С нарушением слуха	1. Индукционная система Исток с1и	- в печатной форме; - в форме электронного документа;

С нарушением зрения	1. Сканирующая и читающая машина SARA CE; 2. Специализированное ПО: экранный доступ JAWS; 3. Наклейка на клавиатуру со шрифтом Брайля; 4. Принтер Брайля (рельефно-точечный);	- в печатной форме (по договору на информационно-библиотечное обслуживание по межбиблиотечному абонементу с КГБУК «Красноярская краевая специальная библиотека – центр социокультурной реабилитации инвалидов по зрению» №2018/2 от 09.01.2018 (срок действия до 31.12.2022)) - в форме электронного документа; - в форме аудиофайла;
С нарушением опорно-двигательного аппарата	1. Специализированный стол; 2. Специализированное компьютерное оборудование (клавиатура программируемая крупная адаптивная, головная компьютерная мышь, джойстик компьютерный);	- в печатной форме; - в форме электронного документа; - в форме аудиофайла;
1. Ресивер для подключения устройств.		