Министерство просвещения Российской Федерации Федеральное государственное бюджетное образовательное учреждение высшего образования «Дагестанский государственный педагогический университет им. Р. Гамзатова»

Кафедра интеллектуальных систем и цифровой экономики

УТВЕРЖДАЮ
Начальник УМУ
_____ Гаджиев Р.Д.
«___»_____20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.06 Модуль общепрофессиональных компетенций

Б1.О.06.08 Основы кибербезопасности

Направление подготовки 09.03.03. Прикладная информатика
Профиль подготовки - «Прикладная информатика в здравоохранении»
Квалификация выпускника: Бакалавр
Формы обучения - очная; заочная
Год приема - 2026

Махачкала 2025

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Целью изучения дисциплины «Основы кибербезопасности» заключается в формировании у обучающихся необходимых теоретических знаний, практических навыков и компетенций, позволяющих эффективно обеспечивать защиту информационной инфраструктуры организаций и частных лиц от несанкционированного доступа, утечки конфиденциальных данных, вредоносных атак и иных угроз информационной безопасности.

Задачи дисциплины – формирование знаний, умений и навыков в области:

Освоение основ теории и практики защиты информации от несанкционированного доступа и киберугроз.

Развитие навыков анализа риска и выбора эффективных мер противодействия угрозам информационной безопасности.

Подготовка квалифицированных специалистов, способных проектировать и реализовывать надежные системы защиты цифровых активов организаций.

Код компетенции	Содержание компетенции	Индикаторы достижения компетенций
УК-1.	УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Демонстрирует владение методами системного анализа, способы обоснования решения (индукция, дедукция, по аналогии) поставленной задачи УК-1.2. Использует методы поиска, сбора и обработки, критического анализа и синтеза информации; навыки выбора методов критического анализа, адекватных поставленной задаче УК-1.3. Использует современные цифровые технологии для поиска, обработки, систематизации и анализа информации УК-1.4. Самостоятельно осуществляет поиск, анализ и синтез информации для решения задач из области профессиональной деятельности
ОПК-3.	ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Выявляет угрозы и уязвимости организаций с точки зрения информационной безопасности и предлагает меры по их устранению ОПК-3.2. Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры ОПК-3.3. Соблюдает требования информационной безопасности при осуществлении профессиональной деятельности

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.О.06.08 «Основы кибербезопасности» относится к **модулю общепрофессиональных компетенций** учебного плана (основной профессиональной

образовательной программы) подготовки бакалавров по направлению 09.03.03. Прикладная информатика профиль подготовки - «Прикладная информатика в здравоохранении»

Дисциплина Б1.О.06.08 «Основы кибербезопасности» базируется на компетенциях, знаниях и умениях, сформированных в ходе изучения школьного курса информатики.

Компетенции сформированные в процессе изучения дисциплины необходимы для освоения содержания дисциплин «Мультимедиа-технологии», «Трехмерное (3D) компьютерное проектирование», «Искусственный интеллект, экспертные системы и базы знаний» и «Компьютерное моделирование» выполнения заданий (учебной, производственной практик, научно-исследовательской работы и выпускной квалификационной работы).

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Дисциплина направлена на формирование следующих компетенций выпускника: УК-1, ОПК-3.

В результате изучения дисциплины, обучающиеся должны:

Код компетенции	Знает	Умеет	Владеет
УК-1	Знает принципы научного познания действительности; современную научную картину мира, место и роль человека в ней; основы естественнонаучных дисциплин в едином комплексе наук	Умеет выявлять, систематизировать и критически осмысливать научные и технические компоненты, включенные в различные области гуманитарного знания, культуру в целом и в историческом контексте	Владеет навыками работы с поисковыми сервисами и ресурсами сети Интернет
	Знает принципы и механизмы работы современных поисковых систем	Умеет осуществлять поиск информации с применением поисковых систем	Владеет современными методами поиска, обработки и использования информации, различными способами познания и освоения окружающего мира
	Знает функциональные возможности сервисов обработки, анализа и хранения информации	Умеет использовать современные цифровые средства для обработки, систематизации и анализа информации	Владеет навыками работы с прикладными компьютерными программами для поиска, обработки, систематизации и анализа информации
ОПК-3	Знает источники возникновения угроз для информационных ресурсов; модели и принципы защиты информации от несанкционированного доступа; методы антивирусной защиты информации; состав и методы организационно-правовой защиты	Умеет применять подходящие организационные, технические и программные средства для обеспечения информационной безопасности	Владеет навыками создания и настройки программных средств защиты информации для информационных ресурсов

	информации		
	Умеет оформлять документацию, связанную с профессиональной деятельностью, в соответствии со стандартами, нормами и правилами	Знает способы, средства и методы защиты информации, применяемые в организации (базе практики)	Владеет навыками самостоятельной работы с информационными и библиографическими источниками в области профессиональной деятельности

4.ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа). Дисциплина изучается в 6 семестре.

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Вид учебной работы	**Трудоёмкость**	
	час.	**В т.ч. по семестрам**
		№1
Общая трудоёмкость дисциплины по учебному плану	**144**	
1. Контактная работа:		
лекции (общее кол-во часов, включая практическую подготовку)	18	
практические занятия, семинары и пр. (общее кол-во часов, включая практическую подготовку)		
практические занятия (общее кол-во часов / включая практическую подготовку)	36	
курсовое проектирование		
групповые, индивидуальные консультации и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем		
2. Объем самостоятельной работы обучающихся (СРС)	**81**	
в том числе часов, выделенных на подготовку к экзамену (зачету)	**9**	
Вид промежуточного контроля:		экзамен

Вид учебной работы	**Трудоёмкость**	
	час.	**В т.ч. по семестрам**
		№1
Общая трудоёмкость дисциплины по учебному плану	**144**	
1. Контактная работа:		
лекции (общее кол-во часов, включая практическую подготовку)	4	
практические занятия, семинары и пр. (общее кол-во часов, включая практическую подготовку)		
лабораторные занятия (общее кол-во часов / включая практическую подготовку)	8	
курсовое проектирование		
групповые, индивидуальные консультации и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем		
2. Объем самостоятельной работы обучающихся (СРС)	**126**	
в том числе часов, выделенных на подготовку к экзамену	**6**	
Вид промежуточного контроля:		экзамен

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

№ п/п	Наименование темы (раздела) дисциплины (модуля)	Общая трудоёмкость в акад.часах	Трудоёмкость по видам учебных занятий (в акад.часах)			
			Лек/ пр.подг.	Лаб / пр.подг.	Пр/ пр.подг.	СР
1	**Основные понятия и виды угроз информационной безопасности** Определение информационной безопасности и её основные цели. Классификация видов угроз: внутренние и внешние угрозы, случайные и преднамеренные атаки. Понятие уязвимости и вектора атак. Анализ распространённых типов угроз: вирусы, фишинг, DDoS-атаки, инсайдеры. Особенности защиты медицинских информационных систем.	34	4		10	20
2	**Методы и инструменты защиты информации.** Модели информационной безопасности: целостность, доступность, конфиденциальность («триада ЦДК»). Организационные меры защиты: политика информационной безопасности, контроль доступа, управление рисками. Технические средства защиты: антивирусы, межсетевые экраны, VPN-технологии, шифрование данных. Специфичные требования безопасности в области здравоохранения: защита персональных данных пациентов, HIPAA и аналогичные стандарты.	38	4		10	24
3	**Правовые основы и этические аспекты информационной безопасности.** Законодательство Российской Федерации в сфере информационной безопасности (ФЗ-152, ФЗ-187). Международные нормы и соглашения в области защиты данных (GDPR, ISO/IEC 27001). Этические проблемы в обеспечении информационной безопасности: ответственность специалиста, правила поведения в сети, добросовестность использования служебной информации. Специальные аспекты защиты медицинской информации в российском законодательстве.	38	4		10	24
4	**Инцидент-менеджмент и реагирование на нарушения информационной безопасности.** Этапы управления инцидентами информационной безопасности:	25	6		6	13

	обнаружение, идентификация, локализация, устранение последствий. Способы выявления и расследования инцидентов, проведение пост-анализа. Создание планов действий на случай чрезвычайных ситуаций в области информационной безопасности. Практическое применение процедур восстановления работоспособности систем после инцидента в условиях здравоохранения.					
	Подготовка к экзамену (зачету)	9				
	Итого:	144	18		36	81

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

№ п/п	Наименование темы (раздела) дисциплины (модуля)	Общая трудоёмкость в акад.часах	Трудоёмкость по видам учебных занятий (в акад.часах)			
			Лек/ пр.подг.	Лаб / пр.подг.	Пр/ пр.подг.	СР
1	**Основные понятия и виды угроз информационной безопасности** Определение информационной безопасности и её основные цели. Классификация видов угроз: внутренние и внешние угрозы, случайные и преднамеренные атаки. Понятие уязвимости и вектора атак. Анализ распространённых типов угроз: вирусы, фишинг, DDoS-атаки, инсайдеры. Особенности защиты медицинских информационных систем.	35	1		2	32
2	**Методы и инструменты защиты информации.** Модели информационной безопасности: целостность, доступность, конфиденциальность («триада ЦДК»). Организационные меры защиты: политика информационной безопасности, контроль доступа, управление рисками. Технические средства защиты: антивирусы, межсетевые экраны, VPN-технологии, шифрование данных. Специфичные требования безопасности в области здравоохранения: защита персональных данных пациентов, HIPAA и аналогичные стандарты.	37	1		2	34
3	**Правовые основы и этические аспекты информационной безопасности.** Законодательство Российской Федерации в сфере информационной безопасности (ФЗ-	37	1		2	34

	152, ФЗ-187). Международные нормы и соглашения в области защиты данных (GDPR, ISO/IEC 27001). Этические проблемы в обеспечении информационной безопасности: ответственность специалиста, правила поведения в сети, добросовестность использования служебной информации. Специальные аспекты защиты медицинской информации в российском законодательстве.					
4	**Инцидент-менеджмент и реагирование на нарушения информационной безопасности.** Этапы управления инцидентами информационной безопасности: обнаружение, идентификация, локализация, устранение последствий. Способы выявления и расследования инцидентов, проведение пост-анализа. Создание планов действий на случай чрезвычайных ситуаций в области информационной безопасности. Практическое применение процедур восстановления работоспособности систем после инцидента в условиях здравоохранения.	29	1		2	26
	Подготовка к экзамену (зачету)	**6**				
	Итого:	144	4		8	126

5.1. Содержание разделов дисциплины (модуля)

Тема 1. Основные понятия и виды угроз информационной безопасности

Определение информационной безопасности и её основные цели. Классификация видов угроз: внутренние и внешние угрозы, случайные и преднамеренные атаки. Понятие уязвимости и вектора атак. Анализ распространённых типов угроз: вирусы, фишинг, DDoS-атаки, инсайдеры. Особенности защиты медицинских информационных систем.

Тема 2. Методы и инструменты защиты информации. Модели информационной безопасности: целостность, доступность, конфиденциальность («триада ЦДК»). Организационные меры защиты: политика информационной безопасности, контроль доступа, управление рисками. Технические средства защиты: антивирусы, межсетевые экраны, VPN-технологии, шифрование данных. Специфичные требования безопасности в области здравоохранения: защита персональных данных пациентов, HIPAA и аналогичные стандарты.

Тема 3. Правовые основы и этические аспекты информационной безопасности. Законодательство Российской Федерации в сфере информационной безопасности (ФЗ-152, ФЗ-187). Международные нормы и соглашения в области защиты данных (GDPR, ISO/IEC 27001). Этические проблемы в обеспечении информационной безопасности: ответственность специалиста, правила поведения в сети, добросовестность использования служебной информации. Специальные аспекты защиты медицинской информации в российском законодательстве. Принципы построения ЭВМ. Простейшие типы архитектур ЭВМ. Совершенствование внутренней

структуры ЭВМ. Обобщенная структура ПЭВМ. Внутримашинный интерфейс. Системная магистраль. Системная плата: основные модули, их характеристики, разъемы.

Тема 4. Инцидент-менеджмент и реагирование на нарушения информационной безопасности.

Этапы управления инцидентами информационной безопасности: обнаружение, идентификация, локализация, устранение последствий. Способы выявления и расследования инцидентов, проведение пост-анализа.

Создание планов действий на случай чрезвычайных ситуаций в области информационной безопасности. Практическое применение процедур восстановления работоспособности систем после инцидента в условиях здравоохранения.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

№ п/п	Наименование раздела дисциплины	Вид самостоятельной работы обучающихся
1	**Основные понятия и виды угроз информационной безопасности.**	подготовка к практические занятиям; подготовка к лекциям; выполнение аудиторной контрольной работы.
2	**Методы и инструменты защиты информации.**	подготовка к практические занятиям; подготовка к лекциям; выполнение аудиторной контрольной работы.
3	**Правовые основы и этические аспекты информационной безопасности.**	подготовка к практические занятиям; подготовка к лекциям; выполнение аудиторной контрольной работы.
4	**Инцидент-менеджмент и реагирование на нарушения информационной безопасности.**	подготовка к практические занятиям; подготовка к лекциям; выполнение аудиторной контрольной работы.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

7.1. Оценочные материалы для проведения текущего контроля успеваемости

.

№ п/п	Наименование темы (раздела) дисциплины (модуля)	Средства текущего контроля успеваемости	Перечень компетенций
1	**Основные понятия и виды угроз информационной безопасности.**	Контрольная работа, тест.	ОПК-3
2	**Методы и инструменты защиты информации.**	Контрольная работа, тест.	УК-1
3	**Правовые основы и этические аспекты информационной безопасности.**	Контрольная работа, тест.	ОПК-3
4	**Инцидент-менеджмент и реагирование на нарушения информационной безопасности.**	Контрольная работа, тест.	УК-1

В университете применяется при реализации всех дисциплин (в том числе при оценивании курсовых работ (проектов)) и практик, установленных учебными планами ОП ВО.

Оценка обучающегося по дисциплине в БРС формируется из:

- баллов, полученных при проведении текущего контроля успеваемости;
- баллов, полученных на промежуточной аттестации.

Баллы, полученные обучающимся при проведении текущего контроля успеваемости, представляют собой сумму баллов, полученных по контрольным точкам, а также дополнительных и премиальных баллов.

Результаты текущего контроля успеваемости фиксируются в единых для всего университета контрольных срезах, устанавливаемые после определенного периода обучения. Для очной формы обучения устанавливаются 2 контрольных среза в каждом семестре. Для заочной – по результатам итогового контроля освоения дисциплины.

По каждому контрольному срезу обучающемуся начисляются баллы за:

- посещаемость в оцениваемый период (20%);
- результаты обучения по (80%):

а) освоенным за оцениваемый период разделам и (или) темам (очная форма обучения);

б) дисциплине (очно-заочная и заочная форма обучения).

По дисциплине обучающемуся могут быть начислены:

- дополнительные баллы;
- премиальные баллы.

Перевод оценок из пятибалльной системы оценивания в 100-балльную по дисциплинам и практикам, а также оценок обучающихся, переведенных в университет из других организаций, осуществляющих образовательную деятельность, в которых БРС не применялась, и в других подобных случаях осуществляется следующим образом:

- «отлично» - 85-100 баллов;

- «хорошо» - 70-84 баллов;

- «удовлетворительно» - 51-69 баллов;

- «зачтено» - 51 балл.

Максимальное количество баллов обучающегося по одной дисциплине (включая баллы, полученные при проведении текущего контроля успеваемости, и баллы, полученные на промежуточной аттестации) составляет 100 баллов.

Если средний рейтинговый балл студента по дисциплине гарантирует ему положительную оценку, в соответствии со шкалой оценок, то преподаватель обязан при желании студента выставить соответствующую оценку без итогового контроля, проставив полученный им средний рейтинговый балл.

Студент может повысить свой рейтинговый балл, проходя итоговый контроль, но при этом весомость набранного в ходе текущего контроля среднего рейтингового балла составляет: 0,5 (50%).

По дисциплине с итоговым контролем – «зачет» студент допускается к сдаче зачета только в том случае, если его средний рейтинговый балл по итогам срезов составляет 30 и выше. В противном случае он автоматически получает – «незачтено». Если его средний рейтинговый балл по итогам срезов составляет 51 и выше, он автоматически получает – «зачтено».

В случаях, когда студент желает повысить свой рейтинговый балл и принимает решение участвовать в промежуточной аттестации, то весомость среднего рейтинговых баллов, полученных при проведении **текущего контроля** успеваемости и полученных на промежуточной аттестации составляет: 0,5 (50%) и 0,5 (50%).

При проведении текущего контроля успеваемости преподаватель может учесть дополнительные баллы в качестве премиальных баллов, начисляемых обучающемуся:

- определения дополнительных баллов по научно-исследовательской деятельности

Показатель	Баллы
Публикация статьи в журнале, сборнике трудов российской, региональной, вузовской конференции	От 5 до 10
Публикация тезисов статьи в сборнике трудов российской, региональной, вузовской конференции, депонирование статьи	От 5 до 10
Доклады на конференциях: внутривузовских, межвузовских, всероссийских и международных	От 5 до 10
Участие в конкурсах грантов: внутривузовский, региональный, всероссийский и международный	От 10 до 15
Участие в конкурсах НИРС: внутривузовский, региональный, всероссийский и международный	От 5 до 10
Участие в изготовлении демонстрационных материалов, наглядных и учебно-методических пособий и т.д.	От 5 до 10
Получение патента, свидетельства на охрану интеллектуальной собственности	От 10 до 15
Участие в вузовской, межвузовской, всероссийской олимпиадах	От 5 до 10
Внедрение результатов исследований в учебный, производственный процесс	От 5 до 10

- определения дополнительных баллов по общественной деятельности

Показатель	Баллы
Участие в организационной структуре факультета: староста группы, курса, профорг студентов факультета и т.д.	От 10 до 15
Организация разовых общественных акций на факультете, в университете и т.д.	От 10 до 15
Участие в культурно-массовых мероприятиях на факультете, в университете и т.д.	От 10 до 15
Участие в вузовских спортивных, организационно-воспитательных мероприятиях	От 10 до 15
Участие в городских, областных спортивных, организационно-воспитательных мероприятиях	От 10 до 15
Участие в российских, международных спортивных, организационно-воспитательных мероприятиях	От 10 до 20

Весомость среднего рейтингового балла и баллов, полученных на пересдаче, составляет соответственно: 0,3 (30%) и 0,7 (70%).

Если студент после пересдачи не получил положительной оценки, то он в установленные вузом сроки идет на комиссионную пересдачу дисциплины.

Весомость среднего балла, полученного при комиссионной сдаче, составляет, соответственно 0 (0%) и 1 (100%), а баллы, полученные при повторной сдаче – аннулируются.

Студент, пропустивший текущий контроль по уважительной причине (болезнь или иные причины, подтвержденные документально), должен его пройти до сдачи следующего промежуточного контроля по дисциплине. Для этого с разрешения декана факультета, директора института формируется индивидуальная балльно-рейтинговая

ведомость.

Итоговая оценка по результатам освоения дисциплины выставляется по 5-балльной шкале или в зачетном формате (в соответствии с формой промежуточной аттестации по дисциплине, установленной учебным планом).

Итоговая оценка заносится в экзаменационную (зачетную) ведомость и зачетную книжку студента.

Итоговый государственный экзамен по специальности оценивается по 100 – балльной шкале.

Правила перевода оценок из 100-балльной системы в пятибалльную систему приведены в таблице 1.

Форма промежуточной аттестации по дисциплине, практике	**Отрицательная оценка**	**Положительные оценки**		
Зачет	**Не зачтено** (менее 50 баллов)	**Зачтено** (более 50 баллов)		
Курсовая работа Зачет с оценкой Экзамен	**Неудовлетворительно** (менее 50 баллов)	**Удовлетвори тельно** (51-69 баллов)	**Хорошо** (70-84 баллов)	**Отлично** (85-100 баллов)

7.2. Оценочные материалы для проведения промежуточной аттестации

1. Семестр – 6; форма аттестации – экзамен.

2. Примерный перечень вопросов к экзамену.

1. Информационная безопасность: сущность, основные компоненты и цели.
2. Типология угроз информационной безопасности в медицинских организациях.
3. Современные классификации компьютерного вредоносного программного обеспечения.
4. Активные и пассивные методы сетевого сканирования: сравнительный анализ.
5. Основные разновидности атак на медицинскую информационную систему.
6. Внутренняя угроза vs внешняя угроза в контексте медицинских учреждений.
7. Политика информационной безопасности: роль и назначение.
8. Принципы защиты персональной медицинской информации.
9. Корпоративная культура информационной безопасности: элементы и рекомендации.
10. Регулирование обработки персональных данных в медицинских учреждениях.
11. Криптографические методы защиты данных: применение в здравоохранении.
12. Аутентификация пользователей в медицинских информационных системах.
13. Биометрия: возможности и ограничения использования в медицинских целях.
14. Резервное копирование: стратегия и необходимость в здравоохранении.
15. Межсетевые экраны: механизм работы и целесообразность применения.
16. Виртуальные частные сети (VPN): преимущества и область применения.
17. Управление доступом к медицинским данным: основные подходы.
18. Целостность данных vs Доступность данных: специфика медицинской сферы.
19. Шифрование данных в электронных медицинских картах: причины и практика.
20. Проверка подлинности SSL-сертификатов в медицинских приложениях.
21. Этапность процесса управления рисками информационной безопасности.
22. Порядок планирования повышения уровня информационной безопасности.
23. Значение аудита информационной безопасности для медицинских учреждений.
24. Методика устранения недостатков в управлении ИБ.
25. Обязанности сотрудников службы информационной безопасности.
26. Частые ошибки сотрудников медицинских учреждений при обработке персональных данных.
27. Непрерывность бизнеса при нарушениях информационной безопасности.
28. Критерии оценки эффективности мероприятий по ИБ.

29. Модель зрелости информационной безопасности CMMI в здравоохранении.
30. Мероприятия по обучению сотрудников требованиям информационной безопасности.
31. Закон РФ «Об информации, информационных технологиях и о защите информации»: основные положения.
32. Конфиденциальность, целостность и доступность данных: суть каждого компонента.
33. Правовое регулирование защиты информации в электронной медицине.
34. Международные законы и регламенты обработки персональных данных в медицине.
35. Ответственность за нарушение требований информационной безопасности.
36. Передача личной информации пациента третьими лицами: законные основания.
37. Анонимизация данных: достаточно ли для обеспечения безопасности?
38. Деонтологические аспекты врачебной профессии в контексте информационной безопасности.
39. Последствия незаконного распространения персональных данных пациентов.
40. Обработка персональных данных россиянами зарубежными компаниями: правовая сторона вопроса.

7.3. Перечень компетенций и индикаторов их достижения, описание критериев оценивания компетенций представляются в таблице

Код компетенции, индикаторы достижения компетенции (ИДК)	Уровни освоения компетенций			
	Продвинутый	Базовый	Пороговый	Не освоены компетенции
	«отлично»	«хорошо»	«удовлетворительно»	«неудовлетворительно»
	«зачтено»			«не зачтено»
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач				
УК-1.1. Демонстрирует владение методами системного анализа, способы обоснования решения (индукция, дедукция, по аналогии) поставленной задачи	*Критерий* 1 Обладает твердым и полным знанием материала, владеет дополнительной информацией. Дает полный, развернутый ответ	*Критерий* 1 Знает материал в запланированном объёме. Ответ достаточно полный, но не отражает некоторые аспекты.	*Критерий* 1 Допускает неточности в формулировках. Знает только основной материал.	*Критерий* 1 Не знает значительной части материала. Отвечает на вопрос частично. Не отвечает на поставленные вопросы.
	Критерий 2 Раскрывает структуру и состав изучаемых разделов информатики, демонстрирует сформированные системные знания. Успешно	*Критерий 2* Раскрывает структуру и состав некоторых изучаемых разделов информатики. При решении предметных задач допускает	*Критерий 2* Фрагментарно описывает структуру и состав изучаемых разделов информатики. Допускает множественные ошибки при решении предметных задач	*Критерий 2* Не знает структуру и содержание изучаемых разделов информатики. Не справляется с решением предложенных предметных задач

	справляется с решением всех поставленных математических задач	единичные ошибки		
УК-1.2. Использует методы поиска, сбора и обработки, критического анализа и синтеза информации; навыки выбора методов критического анализа, адекватных поставленной задаче	*Критерий 1* Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости. Обладает диапазоном практических умений, требуемых для решения определенных проблем в нестандартной ситуации.	*Критерий 1* Знает основные понятия и ключевые факты в пределах изучаемой области. Обладает диапазоном практических умений, требуемых для решения определенных проблем в пределах изучаемой области. .	*Критерий 1* Обладает базовыми общими знаниями и основными умениями, требуемыми для выполнения простых задач.	*Критерий 1* Неспособен самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.
	Критерий 2 Обладает твердым и полным знанием материала, владеет дополнительной информацией. Дает полный, развернутый ответ	*Критерий* 2 Знает материал в запланированном объёме. Ответ достаточно полный, но не отражает некоторые аспекты.	*Критерий* 2 Допускает неточности в формулировках. Знает только основной материал.	*Критерий* 2 Не знает значительной части материала. Отвечает на вопрос частично. Не отвечает на поставленные вопросы.
УК-1.3. Использует современные цифровые технологии для поиска, обработки, систематизации и анализа информации	*Критерий 1* Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости. Обладает диапазоном практических умений, требуемых для решения определенных проблем в нестандартной	*Критерий 1* Знает основные понятия и ключевые факты в пределах изучаемой области. Обладает диапазоном практических умений, требуемых для решения определенных проблем в пределах изучаемой области.	*Критерий 1* Обладает базовыми общими знаниями и основными умениями, требуемыми для выполнения простых задач.	*Критерий 1* Неспособен самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.

	ситуации.			
	Критерий 2 Обладает твердым и полным знанием материала, владеет дополнительной информацией. Дает полный, развернутый ответ	*Критерий* 2 Знает материал в запланированном объёме. Ответ достаточно полный, но не отражает некоторые аспекты.	*Критерий* 2 Допускает неточности в формулировках. Знает только основной материал.	*Критерий* 2 Не знает значительной части материала. Отвечает на вопрос частично. Не отвечает на поставленные вопросы.
УК-1.4. Самостоятельно осуществляет поиск, анализ и синтез информации для решения задач из области профессиональной деятельности	*Критерий 1* Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости. Обладает диапазоном практических умений, требуемых для решения определенных проблем в нестандартной ситуации.	*Критерий 1* Знает основные понятия и ключевые факты в пределах изучаемой области. Обладает диапазоном практических умений, требуемых для решения определенных проблем в пределах изучаемой области.	*Критерий 1* Обладает базовыми общими знаниями и основными умениями, требуемыми для выполнения простых задач.	*Критерий 1* Неспособен самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.
	Критерий 2 Обладает твердым и полным знанием материала, владеет дополнительной информацией. Дает полный, развернутый ответ	*Критерий* 2 Знает материал в запланированном объёме. Ответ достаточно полный, но не отражает некоторые аспекты.	*Критерий* 2 Допускает неточности в формулировках. Знает только основной материал.	*Критерий* 2 Не знает значительной части материала. Отвечает на вопрос частично. Не отвечает на поставленные вопросы.
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности				
ОПК-3.1. Выявляет угрозы и уязвимости организаций с точки зрения информационной безопасности и предлагает меры по их устранению	*Критерий* 1 Самостоятельно анализирует теоретический материал, умеет применять теоретическую базу при	*Критерий* 1 Правильно применяет теоретическую базу при выполнении практических заданий.	*Критерий* 1 Способен решать задачи по заданному алгоритму. Испытывает затруднения при анализе теоретического	*Критерий* 1 Не может установить связь теории с практикой. Не может проанализировать теоретический материал и обосновать его использование на

	выполнении практических заданий, предлагает собственный метод решения.		материала и его применении на практике.	практике.
	Критерий 2 Умеет отбирать материал в зависимости от уровня сложности и логики изложения; умеет применять учебный материал в различных формах обучения в соответствии с требованиями ФГОС ОО	*Критерий 2* Способен отбирать материал в зависимости от уровня сложности, но допускает неточности в в применении учебного материала в различных формах обучения в соответствии с требованиями ФГОС ОО	*Критерий 2* Испытывает затруднения в отборе материала, связанные с логикой изложения и с применением учебного материала в различных формах обучения в соответствии с требованиями ФГОС ОО	*Критерий 2* Не умеет соотносить содержание изучаемых дисциплин с содержанием школьного курса информатики
ОПК-3.2. Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры	*Критерий* 1 Самостоятельно анализирует теоретический материал, умеет применять теоретическую базу при выполнении практических заданий, предлагает собственный метод решения.	*Критерий* 1 Правильно применяет теоретическую базу при выполнении практических заданий.	*Критерий* 1 Способен решать задачи по заданному алгоритму. Испытывает затруднения при анализе теоретического материала и его применении на практике.	*Критерий* 1 Не может установить связь теории с практикой. Не может проанализировать теоретический материал и обосновать его использование на практике.
	Критерий 2 Умеет отбирать материал в зависимости от уровня сложности и логики изложения; умеет применять учебный материал в различных формах обучения в соответствии с требованиями ФГОС ОО	*Критерий 2* Способен отбирать материал в зависимости от уровня сложности, но допускает неточности в в применении учебного материала в различных формах обучения в соответствии с требованиями ФГОС ОО	*Критерий 2* Испытывает затруднения в отборе материала, связанные с логикой изложения и с применением учебного материала в различных формах обучения в соответствии с требованиями ФГОС ОО	*Критерий 2* Не умеет соотносить содержание изучаемых дисциплин с содержанием школьного курса информатики
ОПК-3.3. Соблюдает требования информационной	*Критерий* 1 Самостоятельно анализирует	*Критерий* 1 Правильно применяет	*Критерий* 1 Способен решать задачи по заданному	*Критерий* 1 Не может установить связь теории с

безопасности при осуществлении профессиональной деятельности	теоретический материал, умеет применять теоретическую базу при выполнении практических заданий, предлагает собственный метод решения.	теоретическую базу при выполнении практических заданий.	алгоритму. Испытывает затруднения при анализе теоретического материала и его применении на практике.	практикой. Не может проанализировать теоретический материал и обосновать его использование на практике.
	Критерий 2 Умеет отбирать материал в зависимости от уровня сложности и логики изложения; умеет применять учебный материал в различных формах обучения в соответствии с требованиями ФГОС ОО	*Критерий 2* Способен отбирать материал в зависимости от уровня сложности, но допускает неточности в в применении учебного материала в различных формах обучения в соответствии с требованиями ФГОС ОО	*Критерий 2* Испытывает затруднения в отборе материала, связанные с логикой изложения и с применением учебного материала в различных формах обучения в соответствии с требованиями ФГОС ОО	*Критерий 2* Не умеет соотносить содержание изучаемых дисциплин с содержанием школьного курса информатики

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. Перечень основной учебной литературы

1. Жданов А.А., Чиркин А.Н. Информационная безопасность и защита информации. Учебник и практикум для вузов. — Москва: Издательство Юрайт, 2022 г.
2. Лапонина О.Р. Политика информационной безопасности и стандартизация в области информационной безопасности. Учебное пособие. — Москва: Форум, Инфра-М, 2021 г.
3. Попов А.М., Сидоров Н.И. Компьютерные сети и информационная безопасность. Учебник для бакалавриата и магистратуры. — Москва: Юрайт, 2022 г.
4. Краснов А.В., Гавриков М.К. Практикум по информационной безопасности. Учебное пособие. — СПб.: Питер, 2021 г.
5. Зубарев Р.Ю., Логинова Е.Б. Методология построения систем информационной безопасности. Учебное пособие. — Екатеринбург: УрФУ, 2020 г.
6. Куликов С.С., Леонтьев В.П. Безопасность автоматизированных информационных систем в медицине. Учебное пособие. — Ростов-на-Дону: Феникс, 2021 г.

8.2. Перечень дополнительной учебной литературы

1. Балдин К.В., Белотелов Н.А., Брюховецкий А.С. Управление информационной безопасностью. Учебник. — Москва: Дашков и Ко, 2020 г.
2. Левин В.К. Технические средства защиты информации. Учебное пособие. — Санкт-Петербург: Лань, 2020 г.

3. Масленников Ф.Ф., Яшанов С.Г. Организационно-техническое обеспечение информационной безопасности предприятий и организаций. Учебное пособие. — Тюмень: Тюменский государственный университет, 2020 г.
4. Алексеенко В.Н., Колотов С.В. Организация комплексной защиты объектов информатизации. Учебное пособие. — Пенза: Пензенский гос. ун-т, 2021 г.
5. Голицына О.Л., Максимов Н.В., Попов И.И. Современные методы защиты информации. Учебное пособие. — Москва: Академия, 2022 г.
6. Андреев Ю.Н., Щербаков А.Ю. Проектирование и реализа

8.3. Перечень Интернет-ресурсов, необходимых для освоения дисциплины (модуля)

1. 1. Научная электронная библиотека - elibrary.ru
2. Открытая электронная библиотека. – URL: http://orel.rsl.ru
3. Электронно-библиотечная система – ЭБС - iprbookshop.ru
4. Фундаментальная библиотека ДГПУ - http://lib.dspu.ru
5. Единое окно доступа к образовательным ресурсам – www.window.edu.ru
6. Российское образование федеральный портал – www.edu.ru
7. Национальная электронная библиотека (НЭБ)
8. Университетские библиотеки – www.biblioclub.ru

8.4. Перечень информационных технологий и программного обеспечения

Для осуществления образовательного процесса по дисциплине необходимо использование следующего лицензионного и свободно распространяемого программного обеспечения:
1. Microsoft Office 2016

При проведении обучения используются следующие информационные системы и программы:

1. Электронная библиотека курса, конспекты лекций, программное обеспечение, задания для лабораторных и практических занятий и самостоятельной работы, варианты тестовых заданий для проверки текущих и остаточных знаний студентов, варианты заданий для текущего и промежуточного контроля знаний обучающихся
2. Компьютерное и мультимедийное оборудование.
3. Система компьютерного тестирования (MyTestX).
4. ИС “Рейтинг студентов” – учет учебной деятельности студентов с использованием балльно-рейтингового метода оценивания.
5. При проведении обучения по дисциплине используются активные и интерактивные формы обучения, включая: лекции-визуализации, лекции-беседы, лекции с разбором конкретных ситуаций.

Лекции-визуализации используются на этапе введения студентов в новую тему. Они основаны на использовании в качестве наглядного материала мультимедийной презентации, содержащей такие формы наглядности, как схемы, рисунки, диаграммы и т.д. После освоения студентам базовых знаний по изучаемой теме проводятся лекции беседы, когда студентам адресуются вопросы для обсуждения в начале лекции и по ее ходу. Для пояснения материала изучаемой темы на практическом примере используются лекции с разбором конкретных ситуаций.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для осуществления образовательного процесса по дисциплине необходима следующая материально-техническая база:

- библиотечный фонд (учебная, учебно-методическая, справочная литература);
- компьютеризированные рабочие места для обучаемых с доступом в сеть Интернет;
- аудитории, оборудованные проекционной техникой.

Для проведения лекционных занятий используется лекционный зал ИМФиИТО, оборудованный проектором и интерактивной доской (ауд. №38, 38а, 19).

Для проведения лабораторных занятий используются компьютерные класс кафедры информатики и вычислительной техники (ауд. № 34а, 18а)), оборудованные современными персональными компьютерами с соответствующим программным обеспечением:

- ауд. № 34а - компьютерный зал:

ПЭВМ в сборе: CPUAMD Athlon (tm)4840 Quad Core Processor-3,10 GHz/DDR 4 Gb/HDD 500 Gb. Монитор: MY19HJJCQ959494B **– 16 шт;**

Все персональные компьютеры подключены к сети университета и имеют выход в глобальную сеть Интернет.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Приступая к изучению дисциплины, обучающимся целесообразно ознакомиться с ее рабочей программой, учебной, научной и методической литературой, имеющейся в библиотеке университета, а также с предлагаемым перечнем заданий.

Рекомендации по подготовке к аудиторным занятиям

Лекционные занятия

Умение сосредоточенно слушать лекции, активно воспринимать излагаемые сведения – это важнейшее условие освоения данной дисциплины. Каждая из лекций сопровождается компьютерной презентацией. Кроме того, в конце каждой лекции с целью создания условий для осмысления содержания лекционного материала обучающимся предлагается ответить на вопрос для размышления. Краткие записи лекций, их конспектирование помогает усвоить материал. Поэтому в ходе лекционных занятий необходимо вести конспектирование учебного материала, обращая внимание на самое важное и существенное в нем. Имеет смысл оставить в рабочих конспектах поля, на которых делать пометки, замечания, дополнения. Целесообразно разработать собственную "маркографию" (значки, символы), сокращения слов.

Практические занятия

В ходе подготовки к практическим занятиям необходимо изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д. При этом важно учитывать рекомендации преподавателя и требования учебной программы. Важно также опираться на конспекты лекций. В ходе занятия важно внимательно слушать выступления своих однокурсников. При необходимости задавать им уточняющие вопросы, активно участвовать в обсуждении изучаемых вопросов. В ходе своего выступления целесообразно использовать как технические средства обучения, так и традиционные, то есть доску и мел (при необходимости).

Организация внеаудиторной деятельности обучающихся

Внеаудиторная деятельность обучающегося по данной дисциплине предполагает самостоятельный поиск информации, необходимой, во-первых, для выполнения заданий самостоятельной работы (инвариантной и вариативной частей) и, во-вторых, подготовку к текущей и промежуточной аттестации. Успешная организация времени по усвоению данной дисциплины во многом зависит от наличия у обучающегося умения самоорганизовать себя и своё время для выполнения предложенных домашних заданий.

Подготовка к зачету (экзамену)

В процессе подготовки к зачету обучающемуся рекомендуется так организовать свою учебу, чтобы все виды работ и заданий, предусмотренные рабочей программой, были выполнены в срок. Основное в подготовке к зачету - это повторение всего материала учебной дисциплины. В дни подготовки к зачету необходимо избегать чрезмерной перегрузки умственной работой, чередуя труд и отдых. При подготовке к сдаче зачета старайтесь весь объем работы распределять равномерно по дням, отведенным для подготовки к зачету, контролировать каждый день выполнения работы. Лучше, если можно перевыполнить план. Тогда всегда будет резерв времени. При подготовке к зачету целесообразно повторять пройденный материал в строгом соответствии с учебной программой, примерным перечнем учебных вопросов, заданий, которые выносятся на зачет и содержащихся в данной программе.

11. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Под специальными условиями для получения образования обучающихся с ограниченными возможностями здоровья понимаются условия обучения, воспитания и развития таких студентов, включающие в себя использование при необходимости адаптированных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего необходимую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания вуза и другие условия, без которых невозможно или затруднено освоение образовательных программ обучающихся с ограниченными возможностями здоровья.

Обучение в рамках учебной дисциплины обучающихся с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Обучение по учебной дисциплине обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах.

В целях доступности обучения по дисциплине обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- наличие альтернативной версии официального сайта института в сети «Интернет» для слабовидящих;
- весь необходимый для изучения материал, согласно учебному плану (в том числе, для обучающихся по индивидуальным учебным планам) предоставляется в электроном виде на диске.
- индивидуальное равномерное освещение не менее 300 люкс;
- присутствие ассистента, оказывающего обучающемуся необходимую помощь;
- обеспечение возможности выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

- обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию института.

2) для лиц с ограниченными возможностями здоровья по слуху:

- наличие микрофонов и звукоусиливающей аппаратуры коллективного пользования (аудиоколонки);

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и других приспособлений).

Перед началом обучения могут проводиться консультативные занятия, позволяющие студентам с ограниченными возможностями адаптироваться к учебному процессу.

В процессе ведения учебной дисциплины профессорско-преподавательскому составу рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи обучающимся с ограниченными возможностями здоровья в установлении полноценных межличностных отношений с другими обучающихся, создании комфортного психологического климата в учебной группе.

Особенности проведения текущей и промежуточной аттестации по дисциплине для обучающихся с ограниченными возможностями здоровья устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и другое). При необходимости предоставляется дополнительное время для подготовки ответа на зачете или экзамене.

Автор(ы) рабочей программы дисциплины (модуля):

Зияудинова О. М.

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ):

«Основы кибербезопасности»

Цель освоения дисциплины (модуля): «Основы кибербезопасности» по профилю «Прикладная информатика в здравоохранении» состоит в приобретении студентами глубоких знаний и профессиональных компетенций, направленных на эффективное обеспечение информационной безопасности медицинских информационных систем и сохранение конфиденциальности персональных данных пациентов.

1. **Место дисциплины в структуре образовательной программы**

Дисциплина ***«Основы кибербезопасности»*** относится к вариативной части образовательной программы бакалавриата по направлению Б1.О.06.13 Прикладная информатика

2. **Требования к результатам освоения дисциплины(модуля):**

Код компетенции	Содержание компетенции	Индикаторы достижения компетенций
УК-1.	УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Демонстрирует владение методами системного анализа, способы обоснования решения (индукция, дедукция, по аналогии) поставленной задачи УК-1.2. Использует методы поиска, сбора и обработки, критического анализа и синтеза информации; навыки выбора методов критического анализа, адекватных поставленной задаче УК-1.3. Использует современные цифровые технологии для поиска, обработки, систематизации и анализа информации УК-1.4. Самостоятельно осуществляет поиск, анализ и синтез информации для решения задач из области профессиональной деятельности
ОПК-3.	ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Выявляет угрозы и уязвимости организаций с точки зрения информационной безопасности и предлагает меры по их устранению ОПК-3.2. Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры ОПК-3.3. Соблюдает требования информационной безопасности при осуществлении профессиональной деятельности

3. **Общая трудоемкость дисциплины (модуля) составляет 4 зачетные единицы (144 часа).**
4. **Семестр: 6**
5. **Основные разделы дисциплины (модуля):**

1. Основные понятия и виды угроз информационной безопасности

2. Методы и инструменты защиты информации.

3. Правовые основы и этические аспекты информационной безопасности.

4. Инцидент-менеджмент и реагирование на нарушения информационной безопасности.

6. **Формы текущего контроля успеваемости и промежуточной аттестации: экзамен.**

Автор: *Зияудинова О. М.*