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

Кафедра информатики и информационно-коммуникационных технологий

УТВЕРЖДАЮ
И.о. начальника УМУ
_____
«2» июня 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.08 МОДУЛЬ "ИНФОРМАТИКА"
Б1.О.08.17 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки - 44.03.05 Педагогическое образование

Направленность (профили) – Математика и Информатика

Квалификация выпускника: Бакалавр

Форма обучения – очная, заочная

Год приема - 2025

Форма обучения	Семестр	Трудоемкость	Виды учебной работы					
			Лекции	Практ. занятия	Лабор. занятия	Промежуточный контроль	СРС	Форма аттестации
очная	10	72	12		20		40	зачет
заочная	10	72	2		6	3	61	зачет

Махачкала, 2025

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Целью освоения дисциплины «Информационная безопасность и защита информации» являются формирование знаний, умений, навыков и личностных качеств, характеризующих готовность бакалавра к планированию и достижению профессиональной карьеры.

Код компетенции	Содержание компетенции	Индикаторы достижения компетенций
ПК-1	Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач	ПК-1.1. Знает структуру, состав и дидактические единицы предметной области программирования. ПК-1.2. Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.О.08.17 «Информационная безопасность и защита информации» относится к **обязательной части** и **Модулю Б1.О.08 Информатика** учебного плана (основной профессиональной образовательной программы) подготовки бакалавров по направлению 44.03.05 Педагогическое образование.

Дисциплина Б1.О.08.17 «Информационная безопасность и защита информации» базируется на компетенциях, знаниях и умениях, сформированных в ходе изучения дисциплин «Вводный курс информатики», «Основы искусственного интеллекта», «Компьютерное моделирование», «Архитектура компьютера».

Компетенции сформированные в процессе изучения дисциплины необходимы для 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: ПК-1.

В результате изучения дисциплины обучающиеся должны:

Код компетенции	Знает	Умеет	Владеет
ПК-1	структуру, состав и	осуществлять отбор	навыками разработки

	дидактические единицы предметной области (преподаваемого предмета).	учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО.	различных форм учебных занятий, применения методов, приемов и технологий обучения, в том числе информационных.

4.ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины составляет 2 зачетные единицы (72час). Дисциплина изучается в 10 семестре.

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Вид учебной работы	**Трудоѐмкость**		
	час.	**В т.ч. по семестрам**	
		№1	**№2**
Общая трудоѐмкость дисциплины по учебному плану	**72**	**72**	
1. Контактная работа:			
лекции (общее кол-во часов, включая практическую подготовку)	12	12	
практические занятия, семинары и пр. (общее кол-во часов, включая практическую подготовку)			
лабораторные занятия (общее кол-во часов / включая практическую подготовку)	20	20	
курсовое проектирование			
групповые, индивидуальные консультации и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем			
2. Объем самостоятельной работы обучающихся (СРС)	**40**	**40**	
Вид промежуточного контроля:		зачет	

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Вид учебной работы	**Трудоѐмкость**		
	час.	**В т.ч. по семестрам**	
		№1	**№2**
Общая трудоѐмкость дисциплины по учебному плану	**72**	**72**	
1. Контактная работа:			
лекции (общее кол-во часов, включая практическую подготовку)	2	4	
практические занятия, семинары и пр. (общее кол-во часов, включая практическую подготовку)			
лабораторные занятия (общее кол-во часов / включая практическую подготовку)	6	6	
курсовое проектирование			
групповые, индивидуальные консультации и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем			
2. Объем самостоятельной работы обучающихся (СРС)	**61**	**61**	
Вид промежуточного контроля:	3	зачет	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
очная форма обучения

№ п/п	Наименование темы (раздела) дисциплины (модуля)	Общая трудоѐмкость в акад.часах	Трудоѐмкость по видам учебных занятий (в акад.часах)			
			Лек/ пр.подг.	Лаб / пр.подг.	Пр/ пр.подг.	СР
1	**Основные понятия «информационной безопасности».** Персональные данные как вид защищаемой информации. Определение и эволюция понятия «информационная безопасность». Цели, задачи, направления информационной безопасности. Базовые принципы обеспечения информационной безопасности.	15	2	4		9
2	**Правовые основы информационной безопасности и защиты персональных данных.** Законодательство о безопасности и защите информации, его структура и содержание. Авторское право. Интеллектуальная собственность.	15	2	4		9
3	**Программные средства защиты информации.** Компьютерные вирусы и антивирусная защита. Парольная защита. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство защиты от несанкционированного доступа. Средства родительского контроля.	15	2	4		9
4	**Технические средства защиты и комплексное обеспечение информационной безопасности.** Средства контроля доступа в информационных системах. Технические средства защиты информации. Механические системы защиты информации. Электронные ключи и замки. Биометрические системы идентификации. Основные этапы обеспечения защиты информации: определение политики и составляющих информационной безопасности, управление рисками, аудит информационной безопасности. Меры и методы по защите информации в образовательных	15	4	4		7

	организациях. Анализ и оценивание угроз информационной безопасности личности в цифровой образовательной среде. Интернет-зависимость. Влияние социальных сетей на адаптацию молодежи.					
5	**Элементы криптографии.** Понятие шифра. Симметричное и ассиметричное шифрование. Односторонние функции. Метод RSA. Электронная подпись.	12	2	4		6
	Итого:	72	12	20		40

заочная форма обучения

№ п/п	Наименование темы (раздела) дисциплины (модуля)	Общая трудоѐмкость в акад.часах	Трудоѐмкость по видам учебных занятий (в акад.часах)			
			Лек/ пр.подг.	Лаб / пр.подг.	Пр/ пр.подг.	СР
1	**Основные понятия «информационной безопасности».** Персональные данные как вид защищаемой информации. Определение и эволюция понятия «информационная безопасность». Цели, задачи, направления информационной безопасности. Базовые принципы обеспечения информационной безопасности.	12				12
2	**Правовые основы информационной безопасности и защиты персональных данных.** Законодательство о безопасности и защите информации, его структура и содержание. Авторское право. Интеллектуальная собственность.	14	2			12
3	**Программные средства защиты информации.** Компьютерные вирусы и антивирусная защита. Парольная защита. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство защиты от несанкционированного доступа. Средства родительского контроля.	14		2		12
4	**Технические средства защиты и комплексное обеспечение информационной безопасности.** Средства контроля доступа в информационных системах. Технические средства защиты	14		2		12

	информации. Механические системы защиты информации. Электронные ключи и замки. Биометрические системы идентификации. Основные этапы обеспечения защиты информации: определение политики и составляющих информационной безопасности, управление рисками, аудит информационной безопасности. Меры и методы по защите информации в образовательных организациях. Анализ и оценивание угроз информационной безопасности личности в цифровой образовательной среде. Интернет-зависимость. Влияние социальных сетей на адаптацию молодежи.					
5	**Элементы криптографии.** Понятие шифра. Симметричное и ассиметричное шифрование. Односторонние функции. Метод RSA. Электронная подпись.	15		2		13
	контроль	3				
	Итого:	72	2	6		61

5.1. Содержание разделов дисциплины (модуля)

Тема 1. Основные понятия «информационной безопасности».
Персональные данные как вид защищаемой информации. Определение и эволюция понятия «информационная безопасность». Цели, задачи, направления информационной безопасности. Базовые принципы обеспечения информационной безопасности.

Тема 2. Правовые основы информационной безопасности и защиты персональных данных.
Законодательство о безопасности и защите информации, его структура и содержание. Авторское право. Интеллектуальная собственность.

Тема 3. Программные средства защиты информации.
Компьютерные вирусы и антивирусная защита.
Парольная защита. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство защиты от несанкционированного доступа. Средства родительского контроля.

Тема 4. Технические средства защиты и комплексное обеспечение информационной безопасности.
Средства контроля доступа в информационных системах. Технические средства защиты информации. Механические системы защиты информации. Электронные ключи и замки. Биометрические системы идентификации. Основные этапы обеспечения защиты информации: определение политики и составляющих информационной безопасности, управление рисками, аудит информационной безопасности. Меры и методы по защите

информации в образовательных организациях. Анализ и оценивание угроз информационной безопасности личности в цифровой образовательной среде. Интернет-зависимость. Влияние социальных сетей на адаптацию молодежи.

Тема 5. Элементы криптографии.
Понятие шифра. Симметричное и ассиметричное шифрование. Односторонние функции. Метод RSA. Электронная подпись.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

№ п/п	Наименование раздела дисциплины	Вид самостоятельной работы обучающихся
1	**Основные понятия «информационной безопасности».**	подготовка к лабораторным занятиям; подготовка к лекциям; выполнение аудиторной контрольной работы.
2	**Правовые основы информационной безопасности и защиты персональных данных.**	подготовка к лабораторным занятиям; подготовка к лекциям; выполнение аудиторной контрольной работы.
3	**Программные средства защиты информации.**	подготовка к лабораторным занятиям; подготовка к лекциям; выполнение аудиторной контрольной работы.
4	**Технические средства защиты и комплексное обеспечение информационной безопасности.**	подготовка к лабораторным занятиям; подготовка к лекциям; выполнение аудиторной контрольной работы.
5	**Элементы криптографии.**	подготовка к лабораторным занятиям; подготовка к лекциям; выполнение аудиторной контрольной работы.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Оценочные материалы для проведения текущего контроля успеваемости

.

№ п/п	Наименование темы (раздела) дисциплины (модуля)	Средства текущего контроля успеваемости	Перечень компетенций
1	**Основные понятия «информационной безопасности».**	Контрольная работа, тест.	ПК-1
2	**Правовые основы информационной безопасности и защиты персональных данных.**	Контрольная работа, тест.	ПК-1
3	**Программные средства защиты информации.**	Контрольная работа, тест.	ПК-1
4	**Технические средства защиты и комплексное обеспечение**	Контрольная работа, тест.	ПК-1

	информационной безопасности.		
5	**Элементы криптографии.**	Контрольная работа, тест.	ПК-1

В университете БРС 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)	**Удовлетворительно** (51-69 баллов)	**Хорошо** (70-84 баллов)	**Отлично** (85-100 баллов)

Оценочные материалы для проведения промежуточной аттестации

1. **Семестр – 10; форма аттестации – зачет.**

2. **Примерный перечень вопросов к зачету.**

1. Роль информации в современном мире. Понятие о защищаемой информации.
2. Теория информационной безопасности. Основные направления.
3. Обеспечение ИБ и направления защиты.
4. Требования к системе и политике ИБ.
5. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
6. Доктрина информационной безопасности РФ.
7. Защита государственной тайны в РФ.
8. Защита коммерческой тайны в РФ.
9. Защита персональных данных в РФ.
10. Защита служебной и профессиональной тайны в РФ.
11. Процедуры сертификации и аттестации в РФ.
12. Понятие о защищаемой информации. Свойства информации.
13. Угрозы информации. Классификация угроз.
14. Угрозы нарушения конфиденциальности информации. Особенности и примеры реализации угроз.
15. Угрозы нарушения целостности информации. Особенности и примеры реализации угроз.
16. Угроза нарушения доступности информации. Особенности и примеры реализации угрозы.
17. Источники угроз. Классификация источников угроз.
18. Идентификация и аутентификация. Использование парольной защиты. Недостатки парольной защиты.
19. Понятие электронной подписи.
20. Организационные меры обеспечения информационной безопасности. Служба безопасности предприятия.
21. Организация внутри объектового режима предприятия. Организация охраны.
22. Криптографические меры обеспечения информационной безопасности.

Классификация криптографических алгоритмов.

23. Программно-аппаратные защиты информации. Межсетевые экраны, их функции и назначения.
24. Программно-аппаратные защиты информации. Антивирусные средства, их функции и назначения.
25. Особенности защиты беспроводных и мобильных подключений.
26. Симметричное и ассиметричное шифрование.
27. Принципы симметричного шифрования.
28. Односторонние функции и их применение.
29. Простейшие методы ассиметричного шифрования.
30. Метод RSA.
31. Электронная подпись и ее применение.

Примерная тематика заданий для индивидуальных работ:

Изучение ФЗ №152-ФЗ «О персональных данных» и ФЗ «О защите детей от информации, причиняющей вред их развитию»

Составление каталога интернет-ресурсов, полезных для воспитания, образования и развития детей.

Сравнение функций родительского контроля в составе антивирусных программ

Планирование мероприятий по защите персональных данных в образовательной организации.

Разработка политики информационной безопасности в образовательной организации.

Примерная тематика индивидуальных проектных заданий.

- Биометрические системы идентификации
- Безопасность и конфиденциальность в Интернете
- Понятие о персональных данных
- Информация, составляющая коммерческую тайну
- Объекты информационной безопасности в предметной области
- Информационная среда иллюзии или реальности
- Случайные и целенаправленные угрозы нарушения сохранности информации
- Понятие дезинформации
- Риски информационной безопасности
- Информационное оружие
- Информационные войны
- Технические средства промышленного шпионажа
- Классы безопасности
- Аудит информационной безопасности
- История хакерства
- Хакерство в России
- Правовые механизмы защиты информации на разных уровнях
- Понятие и применение электронной цифровой подписи
- Манипуляции сознанием
- Программы родительского контроля
- Средства антивирусной защиты мобильных устройств

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

Код компетенции, индикаторы	Уровни освоения компетенций			
	Продвинутый	Базовый	Пороговый	Не освоены компетенции

достижения компетенции (ИДК)	«отлично»	«хорошо»	«удовлетворительно»	«неудовлетворительно»
	«зачтено»			«не зачтено»
ПК-1. Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач				
ИДК 1.1 ПК-1.1. Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета).	*Критерий* 1 Обладает твердым и полным знанием материала, владеет дополнительной информацией. Дает полный, развернутый ответ	*Критерий* 1 Знает материал в запланированном объѐме. 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 справляется с решением всех поставленных математических задач	*Критерий 2* Раскрывает структуру и состав некоторых изучаемых разделов информатики. При решении предметных задач допускает единичные ошибки	*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
	Критерий 3 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 3* Знает основные понятия и ключевые факты в пределах изучаемой области. Обладает диапазоном практических умений, требуемых для решения определенных проблем в пределах изучаемой области. .	*Критерий 3* Обладает базовыми общими знаниями и основными умениями, требуемыми для выполнения простых задач .	*Критерий 3* Неспособен самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.

ИДК 1.2. ПК-1.2. Умеет осуществлять отбор учебного содержания для	*Критерий* 1 Обладает твердым и полным знанием материала,	*Критерий* 1 Знает материал в запланированном объѐме. Ответ	*Критерий* 1 Допускает неточности в формулировках. Знает только основной материал.	*Критерий* 1 Не знает значительной части материала. Отвечает на вопрос частично. Не отвечает на
его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО.	владеет дополнительной информацией. Дает полный, развернутый ответ	достаточно полный, но не отражает некоторые аспекты.		поставленные вопросы.
	Критерий 2 Самостоятельно анализирует теоретический материал, умеет применять теоретическую базу при выполнении практических заданий, предлагает собственный метод решения.	*Критерий* 2 Правильно применяет теоретическую базу при выполнении практических заданий.	*Критерий* 2 Способен решать задачи по заданному алгоритму. Испытывает затруднения при анализе теоретического материала и его применении на практике.	*Критерий* 2 Не может установить связь теории с практикой. Не может проанализировать теоретический материал и обосновать его использование на практике.
	Критерий 3 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 3 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 3 Испытывает затруднения в отборе материала, связанные с логикой изложения и с применением учебного материала в различных формах обучения в соответствии с требованиями ФГОС ОО	Не умеет соотносить содержание изучаемых дисциплин с содержанием школьного курса информатики

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

Перечень основной учебной литературы

1. Белов Е.Б. Основы информационной безопасности: Учебн. пособие/
2. Запечников С.В. Информационная безопасность открытых систем. Часть 1: Учебник для вузов / Запечников С.В., Милославская Н.Г., Толстой А.И.,
3. Малюк А.А. Введение в защиту информации в автоматизированных системах: Учебн. пособие для вузов / Малюк А.А., Пазизин С.В., Погожий Н.С. - М.: Горячая линия - Телеком, 2004. - 147 с.
4. Снытников А.А. Лицензирование и сертификация в области защиты информации. - М.: Гелиос АРВ, 2003. - 192 с.
5. Хорев А.А. Защита информации от утечки по техническим каналам: Учебн. пособие. - М.: МО РФ, 2006.

6. Будников С.А., Паршин Н.В. Информационная безопасность автоматизированных систем: Учебное пособие, издание второе, дополненное - Издательство им. Е.А. Болховитинова, Воронеж, 2011.

Перечень дополнительной учебной литературы

1. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. - М.: Горячая линия - Телеком.
2. Бузов Г.А. Защита от утечки информации по техническим каналам: Учебн. пособие / Бузов Г.А., Калинин С.В., Кондратьев А.В.- М.: Горячая линия - Телеком, 2005. - 416 с.
3. Ушаков Д.В. - М.: Горячая линия - Телеком, 2006. - 686 с.
4. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. - Минск, 2005.-304 с.
5. Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных сетях. - Ростов-на-Дону: Издательство СКНЦ ВШ, 2006.
6. Язов Ю.К. Основы технологий проектирования систем защиты
7. информации в информационно-телекоммуникационных системах:
8. Монография /Аграновский А.В., Мамай В.И., Назаров И.Г., Язов Ю.К. - Издательство СКНЦ ВШ, 2006.
9. Петраков А.В. Основы практической защиты информации. Учебное пособие. -М., 2005.- 281 с.
10. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. - С.-П., 2004.- 384 с.

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

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

Перечень информационных технологий и программного обеспечения

Для осуществления образовательного процесса по дисциплине необходимо использование следующего лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

1. Microsoft Office 2010

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. №44).

Для проведения лабораторных занятий используются компьютерные класс кафедры информатики и вычислительной техники (ауд. № 43, 47)), оборудованные современными персональными компьютерами с соответствующим программным обеспечением:

- ауд. № 43 - компьютерный зал:

ПЭВМ в сборе: CPUAMD Athlon (tm)4840 Quad Core Processor-3,10 GHz/DDR 4 Gb/HDD 500 Gb. Монитор: MY19HJJCQ959494B **– 12 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 своѐ 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):
Доцент, к.ф.-м..н. Рагимханова Г.С.

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ):
«Информационная безопасность и защита информации»

1. **Цель освоения дисциплины (модуля): изучение разделов: основные понятия**

«информационной безопасности», правовые основы информационной безопасности и защиты персональных данных, программные средства защиты информации, технические средства защиты и комплексное обеспечение информационной безопасности, элементы криптографии.

2. **Место дисциплины в структуре образовательной программы**
   Дисциплина ***«Информационная безопасность и защита информации»*** относится к обязательной части образовательной программы бакалавриата по направлению 44.03.05 Педагогическое образование.
3. **Требования к результатам освоения дисциплины(модуля):**

Код компетенции	Содержание компетенции	Индикаторы достижения компетенций
ПК-1	Способен осваивать и использовать теоретические знания и практические умениями навыки в предметной области при решении профессиональных задач	ПК-1.1. Знает структуру, состав и дидактические единицы предметной области архитектуры компьютера. ПК-1.2. Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО.

4. **Общая трудоемкость дисциплины (модуля) составляет 3 зачетные единицы (108 часов).**
5. **Семестр: 10**
6. **Основные разделы дисциплины (модуля):**
   Тема 1. Основные понятия «информационной безопасности».
   Персональные данные как вид защищаемой информации. Определение и эволюция понятия «информационная безопасность». Цели, задачи, направления информационной безопасности. Базовые принципы обеспечения информационной безопасности.

   Тема 2. Правовые основы информационной безопасности и защиты персональных данных.
   Законодательство о безопасности и защите информации, его структура и содержание. Авторское право. Интеллектуальная собственность.

   Тема 3. Программные средства защиты информации.
   Компьютерные вирусы и антивирусная защита.
   Парольная защита. Идентификация и аутентификация. Разграничение доступа.
   Межсетевые экраны как средство защиты от несанкционированного доступа.
   Средства родительского контроля.

Тема 4. Технические средства защиты и комплексное обеспечение информационной безопасности.
Средства контроля доступа в информационных системах. Технические средства защиты информации. Механические системы защиты информации. Электронные ключи и замки. Биометрические системы идентификации. Основные этапы обеспечения защиты информации: определение политики и составляющих информационной безопасности, управление рисками, аудит информационной безопасности. Меры и методы по защите информации в образовательных организациях. Анализ и оценивание угроз информационной безопасности личности в цифровой образовательной среде. Интернет-зависимость. Влияние социальных сетей на адаптацию молодежи.

Тема 5. Элементы криптографии.
Понятие шифра. Симметричное и ассиметричное шифрование. Односторонние функции. Метод RSA. Электронная подпись.

7. **Формы текущего контроля успеваемости и промежуточной аттестации: зачет.**

Автор: *Рагимханова Г. С., доцент кафедры информатики и ВТ*