ФГБОУ ВО «Дагестанский государственный педагогический университет»
Факультет математики, физики и информатики
Кафедра информатики и вычислительной техники

УТВЕРЖДАЮ
И.о проректора по учебной работе и дополнительному образованию - начальник учебно-методического управления
_____ А.Д. Вечедова
«___» _____ 2018 г.

Рабочая программа дисциплины

Б1.В.ДВ.15.2 Защита информации

(шифр, название дисциплины)

Направление **44. 03.05. Педагогическое образование (с двумя профилями подготовки)**
(шифр, наименование направления)

Профили **«Математика» и «Информатика»**

Квалификация **Бакалавр**

Формы обучения _____очная; заочная_____

Сроки обучения – _____очно- 5 лет ; заочно- 5,5 года _____

Махачкала, 2018

Автор: Эсетов Ф.Э., доцент, к.п.н._____ _____
(ФИО, должность, ученое звание) (подпись)

Рецензент: Гаджиев Т.С., доцент кафедры информатики и информационных технологий, к.ф.-м.н.

Программа утверждена на заседаниях:

Кафедры информатики и вычислительной техники
(протокол № 7 от « 23 » марта 2018 г.)

Зав. кафедрой ___Эсетов Ф.Э., доцент_____ _____
(ФИО, ученое звание) (подпись)

Ученом совете факультета
(протокол № 8 от « 12 » апреля 2018 г.)

Председатель совета __Бакмаев Ш.А., профессор_____ _____
(ФИО, ученое звание) (подпись)

методическом совете ДГПУ
(протокол № 5 от « 25 » мая 2018 г.)

СОДЕРЖАНИЕ

1. Цели и задачи освоения дисциплины

1. Цели освоения дисциплины

Целями освоения дисциплины (модуля) Защита информации являются сформировать у будущего учителя информатики систему компетенций в области защиты информации в компьютерных системах для решения практических задач анализа и синтеза информационных процессов в педагогической и культурно-просветительской профессиональной деятельности.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 1. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)

Код компетенции	Наименование компетенции
(ОК-3)	способностью использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве
(ПСК -7)	- готов применять знания теоретической информатики, фундаментальной и прикладной математики для анализа и синтеза информационных систем и процессов

В результате освоения дисциплины обучающийся должен:

1) Знать: - терминологию и основные понятия теории защиты информации;

- содержание основных нормативных документов в области защиты компьютерной информации;
- виды угроз информационной безопасности;
- методы обеспечения информационной безопасности;
- требованиям к системам защиты информации;

2) Уметь: - выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в компьютерных системах;

3) Владеть - навыками работы с инструментальными средствами защиты информации.

3.Место дисциплины в структуре ОП бакалавриата

Учебная дисциплина «Защита информации» относится к дисциплинам по выбору вариативной части профессионального цикла.

Для изучения данной учебной дисциплины необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: *Информационные технологии, Теоретические основы информатики, компьютерные сети, интернет и мультимедиа технологии.*

4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины «Защита информации» составляет 72 часа. (2 зачетные единицы).

Объем контактной работы обучающихся с преподавателем по дисциплине (по видам учебных занятий) и на самостоятельную работу обучающихся очной формы отражен в таблице 2.

Таблица 2. Объем контактной работы обучающихся с преподавателем по дисциплине (по видам учебных занятий) и на самостоятельную работу обучающихся очной формы

Вид работы	Трудоемкость, часов		
	Семестр 10	Семестр	Итого
Общая трудоемкость, часов	**72**		**72**
Аудиторная работа:	**32**		**32**
Лекции (Л)	12		12
Практические занятия (ПЗ)			
Лабораторные работы (ЛР)	20		20
КСР			
Самостоятельная работа:	**40**		**40**
Вид итогового контроля (зачет, экзамен)	**зачет**		**зачет**

Объем дисциплины контактной работы обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся заочной формы отражен в таблице 3.

Таблица 3. Объем контактной работы обучающихся с преподавателем по дисциплине (по видам учебных занятий) и на самостоятельную работу обучающихся заочной формы

Вид работы	Трудоемкость, часов		
	Семестр 1	Семестр 2	Итого 1,2
Общая трудоемкость, часов	**72**		
Аудиторная работа:	**8**		
Лекции (Л)	4		
Практические занятия (ПЗ)			
Лабораторные работы (ЛР)	4		
КСР			
Самостоятельная работа:	**64**		
Вид итогового контроля (зачет, экзамен)	**зачет**		

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1. Содержание разделов учебной дисциплины (модуля)

Раздел 1. Понятия информационной безопасности, защиты информации. Основные задачи информационной безопасности. Предмет защиты информации, его свойства. Объект защиты информации
Раздел 2. Информация как правовая категория, ее особенности. Государственная политика информационной безопасности. Органы обеспечения информационной безопасности. Структура и состав информационного законнодательства в РФ. Стандарты информационной безопасности.

Раздел 3. Основные источники угроз безопасности информации. Классификация угроз информационной безопасности. Компьютерные вирусы как угроза информационной безопасности. Профилактика компьютерных вирусов.

Раздел 4. Уровни формирования режима информационной безопасности. Цели и задачи административного уровня обеспе-чения информационной безопасности. Группы сведений, содержащиеся в документации по политике безопасности организации. Программно-технический уровень обеспечения информационной безопасности.

Раздел 5. Пути достижения требуемой достоверности обработки информации. Организационные и инженерно-технические меры и мероприятия по обеспечению конфиденциальности информации в автоматизированных системах. Организационные и аппаратно-программные методы повышения сохранности информации.

Раздел 6. Особенности защиты информации в распределенных компьютерных системах. Защита информации в каналах связи. Межсетевое экранирование. Электронная цифровая подпись. Типовые удаленные атаки и их характеристика
Раздел 7. Классификация методов криптографического преобразования информации. Шифрование. Методы шифрования с симметричным ключом. Системы шифрования с открытым ключом

5.2. Структура учебной дисциплины (модуля)

Таблица 7. Структура учебной дисциплины (модуля) для очной формы обучения

Тема (раздел) дисциплины	**Итого**	**Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость (в часах)**				
		ЛК	**ПЗ**	**ЛР**	**КСР**	**Сам. Раб.**
10 семестр						
Раздел 1. Понятия информационной безопасности, защиты информации. Основные задачи информационной безопасности. Предмет защиты информации, его свойства. Объект защиты информации	10	1		2		7
Раздел 2. Информация как правовая категория, ее особенности. Государственная политика информационной безопасности. Органы обеспечения информационной безопасности. Структура и состав информационного законнодательства в РФ. Стандарты информационной безопасности	12	1		2		9

. Раздел 3. Основные источники угроз безопасности информации. Классификация угроз информационной безопасности. Компьютерные вирусы как угроза информационной безопасности. Профилактика компьютерных вирусов.	10	2		2		6
Раздел 4. Уровни формирования режима информационной безопасности. Цели и задачи административного уровня обеспе-чения информационной безопасности. Группы сведений, содержащиеся в документации по политике безопасности организации. Программно-технический уровень обеспечения информационной безопасности.	10	2		2		6
Раздел 5. Пути достижения требуемой достоверности обработки информации. Организационные и инженерно-технические меры и мероприятия по обеспечению конфиденциальности информации в автоматизированных системах. Организационные и аппаратно-программные методы повышения сохранности информации.	10	2		2		6
Раздел 6. Особенности защиты информации в распределенных компьютерных системах. Защита информации в каналах связи. Межсетевое экранирование. Электронная цифровая подпись. Типовые удаленные атаки и их характеристика	10	2		2		6
Раздел 7. Классификация методов криптографического преобразования информации. Шифрование. Методы шифрования с симметричным ключом. Системы шифрования с открытым ключом	10	**2**		**2**		6
Всего за семестр	**72**	**12**		**20**		**40**

Целью Лабораторных и практических занятий является контроль усвоения студентами теоретического материала по дисциплине, а также привитие навыков и умений применения полученных знаний при решении экономических задач.

Применяемые технологии при проведении практического занятия:

- ознакомление студентов с целью и задачами занятия;
- фронтальный опрос;
- решение практических задач;
- тестирование по теме;
- выполнение контрольных работ;
- подготовка и защита рефератов по отдельным темам;
- подведение итогов и оценка знаний студентов.

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся осуществляется методами самообучения и самоконтроля в двух направлениях:

- для закрепления и углубления знаний и навыков, полученных на лекционных и практических занятиях;
- для самостоятельного изучения отдельных тем и вопросов дисциплины.

Самостоятельная работа осуществляется в виде:

- конспектирования учебной, научной и периодической литературы;
- проработки учебного материала (по конспектам лекций учебной и научной литературы);
- подготовки сообщений и докладов к семинарам и практическим занятиям, к участию в тематических дискуссиях, работе научного кружка и конференциях;
- работы с нормативными документами и законодательной базой, с первичными документами и отчетностью предприятий;
- поиска и обзора научных публикаций и электронных источников информации, подготовки заключения по обзору информации;
- выполнения лабораторных, контрольных работ, творческих (проектных) заданий, курсовых работ (проектов);
- решения практических и ситуационных задач;
- составления аналитических таблиц, графического оформления материала;
- написания рефератов, докладов;
- работы с тестами и контрольными вопросами для самопроверки;
- анализа отчетной информации организаций различных организационно-правовых форм и видов деятельности;
- моделирования и анализа конкретных проблемных ситуаций;
- написания выводов и предложений на основе проведенного анализа.

Результаты самостоятельной работы контролируются и учитываются при текущем и промежуточном контроле успеваемости обучающегося. При этом проводятся тестирование, экспресс-опрос и фронтальный опрос на семинарских и практических занятиях, заслушивание докладов и сообщений по дополнительному материалу к лекциям, проверка домашних контрольных работ и т.д.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№	Контролируемые разделы (темы) дисциплины (результаты по разделам)	Код контролируемой компетенции (или её части) и ее формулировка – по желанию	наименование оценочного средства
1.	Раздел 1. Понятия информационной безопасности, защиты информации. Основные задачи информационной	ОК-3, ПСК-7	Контрольная работа, тест.

	безопасности. Предмет защиты информации, его свойства. Объект защиты информации		
2.	Раздел 2. Информация как правовая категория, ее особенности. Государственная политика информационной безопасности. Органы обеспечения информационной безопасности. Структура и состав информационного законнодательства в РФ. Стандарты информационной безопасности.	ОК-3, ПСК-7	Контрольная работа, тест.
3.	Раздел 3. Основные источники угроз безопасности информации. Классификация угроз информационной безопасности. Компьютерные вирусы как угроза информационной безопасности. Профилактика компьютерных вирусов.	ОК-3, ПСК-7	Контрольная работа, тест.
4.	Раздел 4. Уровни формирования режима информационной безопасности. Цели и задачи административного уровня обеспе-чения информационной безопасности. Группы сведений, содержащиеся в документации по политике безопасности организации. Программно-технический уровень обеспечения информационной безопасности.	ОК-3, ПСК-7	Контрольная работа, тест.
5.	Раздел 5. Пути достижения требуемой достоверности обработки информации. Организационные и инженерно-технические меры и мероприятия по обеспечению конфиденциальности информации в автоматизированных системах. Организационные и аппаратно-программные методы повышения сохранности информации.	ОК-3, ПСК-7	Контрольная работа, тест.
6.	Раздел 6. Особенности защиты информации в распределенных компьютерных системах. Защита информации в каналах связи. Межсетевое экранирование. Электронная цифровая подпись. Типовые удаленные атаки и их характеристика	ОК-3, ПСК-7	Контрольная работа, тест.
7.	Раздел 7. Классификация методов криптографического преобразования	ОК-3, ПСК-7	Контрольная работа, тест.

	информации. Шифрование. Методы шифрования с симметричным ключом. Системы шифрования с открытым ключом		

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1. Схема оценки уровня формирования компетенции ОК-3

Показатели (что обучающийся должен продемонстрировать)	**Оценочная шкала**		
	Удовлетворительно	**Хорошо**	**Отлично**
Знать - методы обеспечения информационной безопасности; - требованиям к системам защиты информации; Уметь: обосновывать организационно-технические мероприятия по защите информации в компьютерных системах; Владеть - навыками работы с инструментальными средствами защиты информации.	Знает основной материал, но допускает неточности, При решении примеров, задач допускает ошибки.	Знает учебный материал. Умеет правильно применить теорию при выполнении практических заданий, владеет необходимыми приемами выполнения практических заданий, но затрудняется с применением знаний, связанных с новыми нестандартными задачами. показывает должный уровень сформированности компетенций.	Знает глубоко и прочно учебный материал, свободно отвечает на вопросы, свободно решает задачи, не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических заданий, показывает должный уровень сформированности компетенций.

2. Схема оценки уровня формирования компетенции ПСК-7

Показатели (что обучающийся должен продемонстрировать)	**Оценочная шкала**		
	Удовлетворительно	**Хорошо**	**Отлично**
Знать: - терминологию и основные понятия теории защиты информации; - содержание основных нормативных документов в области защиты компьютерной информации; - виды угроз	Знает основной материал, но допускает неточности, При выполнении практических заданий допускает ошибки.	Знает учебный материал. Умеет правильно применить теорию при выполнении практических заданий, владеет необходимыми приемами выполнения практических	Знает глубоко и прочно учебный материал, свободно отвечает на вопросы, свободно решает задачи, не затрудняется с ответом при видоизменении заданий, правильно

информационной безопасности; Уметь: - выявлять угрозы информационной безопасности Владеть - навыками работы с инструментальными средствами защиты информации.		заданий, но затрудняется с применением знаний, связанных с новыми нестандартными задачами. показывает должный уровень сформированности компетенций.	обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических заданий, показывает должный уровень сформированности компетенций.

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Вопросы для контроля и самостоятельной работы:

1. Свойства информации как объекта защиты
2. Виды защищаемой информации
3. Информационные угрозы
4. Информационные атаки
5. Технические каналы утечки информации
6. Электромагнитные каналы утечки информации
7. Акустические каналы утечки информации
8. Физические поля, создающие каналы утечки информации
9. Кодирование для защиты информации от искажения помехами в системах передачи
10. Обратная связь для адаптации к помеховой обстановке
11. Искажения кодированных сообщений помехами
12. Шифрация для защиты от несанкционированного доступа к информации
13. Стандарты симметричных криптосистем
14. Двухключевые криптосистемы (криптосистемы с открытым ключом)
15. Стойкость к имитирующим и дезинформирующим помехам (обеспечение подлинности сообщений)
16. Сети связи
17. Основные угрозы безопасности информации и методы защиты информации в кабельных телефонных сетях
18. Методы и средства защиты информации в мобильных системах
19. Защита информации в цифровых системах мобильной связи с кодовым разделением каналов
20. Методы представления речевого сигнала
21. Компрессия аналогового речевого сигнала
22. Дискретные методы передачи и обработки речевого сигнала
23. Критерии оценки систем закрытия речи
24. Функциональная схема системы закрытой связи
25. Угрозы информационным ресурсам и информационные атаки на вычислительные системы
26. Общие сведения о компьютерных вирусах
27. Принципы функционирования основных разновидностей вирусов
28. Использование СТЕЛС технологии в вирусных программах
29. Программные средства борьбы с вирусами

30. Программные закладки
31. Действие вирусов и программных закладок в сетях ЭВМ
32. Организационно-технические меры защиты от угроз безопасности сети
33. Создание изолированной программной среды
34. Комплексный характер проблемы защиты информации в сетях ЭВМ

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Результаты формирования компетенций по дисциплине оцениваются по балльно-рейтинговой системе.

Всего по дисциплине студент может набрать 100 баллов (или более с учетом бонусных баллов), из которых 20 баллов составляют баллы за посещаемость, 50 – за активность и 30 студент получает на зачете или на экзамене.

Всего по дисциплине предусмотрено два модуля. Для расчета баллов, полученных студентом за модуль и итогового рейтинга с учетом трудоемкости дисциплины, включенной в учебный план, показатели (по посещению, активности, рубежного контроля) перемножаются на соответствующие коэффициенты. Данные коэффициенты определяются отдельно для каждого модуля следующим образом:

Коэффициент посещения - $К_{посещ.}=10/ N_{зан.}$

Коэффициент активности - $К_{актив.}=25/ N_{актив.}$

Где:

$N_{зан.}$ – количество занятий (пар) по дисциплине в данном модуле;

$N_{актив.}$ – максимальное количество баллов, которое может набрать студент на занятиях (практических, семинарских, лабораторных) в данном модуле + баллы, полученные на рубежном контроле.

Баллы, полученные студентами, заносятся в журнал БРС сразу после окончания занятия, во время которого эти баллы были получены.

Оценка на промежуточном контроле (зачет, экзамен) выставляется по результатам баллов, полученным студентом в сумме обоих модулей по следующей таблице

Набранные студентом баллы	Оценка на промежуточном контроле, если дисциплина завершается экзаменом (зачетом с оценкой)	Оценка на промежуточном контроле, если дисциплина завершается зачетом
от 0 до 50	неудовлетворительно	не зачтено
от 51 до 64	удовлетворительно	зачтено
от 65 до 74	хорошо	
от 75 до 100	отлично	

Для процедура оценивания используются тесты, контрольные работы.

Наиболее способным студентам преподаватель рекомендует специальную научную разработку отдельных тем и проблем курса в рамках работы кафедрального кружка студенческого научного общества с последующими выступлениями на ежегодных научных конференциях университета.

Тестирование: на практических занятиях реализуется **тестирование** студентов с целью контроля результатов их самостоятельной работы по усвоению основных понятий и тем курса.

Оценка работы с тестовыми заданиями:

0- 20 % правильных ответов оценивается как «неудовлетворительно»; 30-50% - «удовлетворительно»; 60-80% - «хорошо»; 80-100% – «отлично».

Система оценки ответа студента на зачете:

Оценка "незачтено" выставляется при незнании основных вопросов материала или при наличии грубых ошибок в ответах на них, неумении на основе теоретических знаний решать практические задачи.

Оценка "зачтено" выставляется при достаточно полном знании материала учебной программы, отсутствии существенных неточностей при его изложении и в ответах на вопросы, умении решать практические задачи.

Система оценки ответа студента на экзамене:

Оценка за каждый вопрос и итоговая оценка выставляется в 4-х бальной системе: "отлично", "хорошо", "удовлетворительно", "неудовлетворительно". При этом:

Оценка "отлично" выставляется при глубоком и всестороннем знании материала учебной программы, грамотном и логически стройном его изложении, умении на основе теоретических знаний решать практические задачи.

Оценка "хорошо" выставляется при твердом и достаточно полном знании материала учебной программы, отсутствии существенных неточностей при его изложении и в ответах на вопросы, умении решать практические задачи.

Оценка "удовлетворительно" выставляется при наличие неточностей в знании основного материала, при допущении ошибок при выполнении практических заданий.

Оценка "неудовлетворительно" выставляется при незнании основных вопросов экзаменационного билета или наличии грубых ошибок в ответах на них, неумении на основе теоретических знаний решать практические задачи.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

основная литература:

1. Куприянов А. И. и др. Основы защиты информации. Гриф УМО МО,- Академия, 2008.
2. Запечников С. В. Информационная безопасность открытых систем. Средства защиты в сетях. Том 2. Гриф МО РФ, Горячая линия-Телеком, 2008.
3. Под ред. С.А. Клейменова Информационная безопасность и защита информации. Учебное пособие для студентов ВУЗов, - Академия, 2009.
4. Расторгуев С.П. Основы информационной безопасности / С.П. Расторгуев. -2-е изд., стер.- М.: Академия, 2009.- 192 с.

б) дополнительная литература:

1. Запечников С. В. Информационная безопасность открытых систем. Том 1. Угрозы, уязвимости, атаки и подходы к защите, Гриф МО РФ, Горячая линия-Телеком, 2008.
2. Расторгуев С.П. Информационная война. Проблемы и модели. Экзистенциальная математика,- Гелиос АРВ, 2008.
3. Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов,- Горячая линия-Телеком, 2009.
4. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Гриф МО РФ, Книжный мир,2009.
5. Панасенко С. Алгоритмы шифрования. Специальный справочник, - БХВ-Петербург, 2009.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Образовательный портал http://www.edu.ru
2. Федеральное государственное учреждение: "Государственный научно-исследовательский институт информационных технологий и телекоммуникаций" http://www.informika.ru/projects/infotech/.
3. Федеральный образовательный портал: http://www.ict.edu.ru
4. Электронные образовательные ресурсы: http://www.ou.tsu.ru
5. Электронные учебники http://bookwebmaster.narod.ru
6. Электронная библиотека издательства "Лань". URL: http://e.lanbook.com
7. www.parallel.ru
8. www.computer-museum.ru
9. www.ixbt.com
10. www.mpi.org
11. www.omp.org

10. Методические указания для обучающихся по освоению дисциплины (модуля)

Для изучения курса студентам необходимо использовать лекционный материал, учебники и учебные пособия из списка литературы, статьи из периодических изданий, ресурсы информационно-телекоммуникационной сети «Интернет»

Кроме того, целесообразно использовать следующие методические материалы:

1. Варианты контрольных работ и тестов.
2. Задачи для практических занятий самостоятельной работы
3. Раздаточный материал для практических занятий.
4. Задания для промежуточного и текущего контроля знаний студентов.
5. Электронную базу данных по дисциплине.
6. Учебно-методический комплекс дисциплины.

Для теоретического и практического усвоения дисциплины большое значение имеет самостоятельная работа студентов, которая может осуществляться студентами индивидуально и под руководством преподавателя.

Самостоятельная работа студентов, предусмотренная учебным планом в объеме не менее 50-70% общего количества часов, направлена на более глубокое усвоение изучаемого курса, формирование навыков исследовательской работы и ориентирование студентов на умение применять теоретические знания на практике.

Показателем освоения материала служит успешное решение задач предлагаемых домашних контрольных работ и выполнение аудиторных самостоятельных и контрольных работ.

В качестве оценочных средств программой дисциплины предусматривается:

- текущий контроль (аудиторные контрольные работы, домашние задания).
- промежуточный контроль (экзамен).

Формы текущего, промежуточного и итогового контроля.

Текущий контроль:

- Самостоятельные работы
- Индивидуальные задания
- Опрос студентов

Промежуточный контроль:

- Контрольная работа по курсу

Итоговый контроль:

- экзамен

Критерии оценок

В основе оценки знаний по предмету лежат следующие основные требования:

- освоение всех разделов теоретического курса программы;
- умение применять полученные знания к решению конкретных задач.

Ответ заслуживает ***отличной оценки***, если экзаменуемый показывает знания, в полной степени, отвечающие предъявляемым к ответу требованиям: это требование основных понятий и приемов решения задач. Отличная оценка характеризует свободную ориентацию экзаменуемого в предмете. Ответы на вопросы, в том числе и дополнительные, должны обнаруживать уверенное владение терминологией, основными умениями и навыками.

Хорошая оценка характеризует тот ответ, который не в полной степени удовлетворяет вышеперечисленным критериям, однако, экзаменуемый обнаруживает прочные знания в объеме курса. Ответ должен быть достаточно аргументирован, вопросы глубоко и осмысленно изложены.

Оценка «***удовлетворительно***» выставляется за то, что ответ экзаменуемого соотносится с основными требованиями, т.е. имеются в виду твердые знания в объеме учебной программы и умение владеть терминологией. Удовлетворительная оценка выставляется за знание в целом, однако, отдельные детали могут быть упущены.

Неудовлетворительная оценка выставляется, если ответ не удовлетворяет хотя бы одному из требований или отсутствуют знания основных понятий и методов решения задач.

11.Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем

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 ФМФиИ.
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.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

1. *Лекционные занятия:*
    a. аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук).
    b. УМК дисциплины, электронные образовательные ресурсы
2. *Лабораторные занятия:*
    a. компьютерный класс,
    b. программное обеспечение, презентации.
    c. Программные модели

АННОТАЦИЯ
рабочей программы дисциплины
«Защита информации»

Дисциплина **Защита информации** входит в вариативную по выбору часть образовательной программы бакалавриата по направлению 44.03.05 Педагогическое образование.

Дисциплина реализуется на факультете математики, физики и информатики кафедрой информатики и вычислительной техники.

Содержание дисциплины охватывает круг вопросов, связанных с изучением разделов:

Раздел 1. Понятия информационной безопасности, защиты информации. Основные задачи информационной безопасности. Предмет защиты информации, его свойства. Объект защиты информации.

Раздел 2. Информация как правовая категория, ее особенности. Государственная политика информационной безопасности. Органы обеспечения информационной безопасности. Структура и состав информационного законнодательства в РФ. Стандарты информационной безопасности.

Раздел 3. Основные источники угроз безопасности информации. Классификация угроз информационной безопасности. Компьютерные вирусы как угроза информационной безопасности. Профилактика компьютерных вирусов.

Раздел 4. Уровни формирования режима информационной безопасности. Цели и задачи административного уровня обеспе-чения информационной безопасности. Группы сведений, содержащиеся в документации по политике безопасности организации. Программно-технический уровень обеспечения информационной безопасности.

Раздел 5. Пути достижения требуемой достоверности обработки информации. Организационные и инженерно-технические меры и мероприятия по обеспечению конфиденциальности информации в автоматизированных системах. Организационные и аппаратно-программные методы повышения сохранности информации.

Раздел 6. Особенности защиты информации в распределенных компьютерных системах. Защита информации в каналах связи. Межсетевое экранирование. Электронная цифровая подпись. Типовые удаленные атаки и их характеристика Раздел 7. Классификация методов криптографического преобразования информации. Шифрование. Методы шифрования с симметричным ключом. Системы шифрования с открытым ключом.

Дисциплина нацелена на формирование следующих компетенций выпускника: общекультурных – ОК-3, профессионально – специализированных– ПСК-7.

В рабочей программе дисциплины предусмотрено проведение:

−учебных занятий в виде лабораторных, практических работ, самостоятельной работы,

−контроль успеваемости в форме зачета

Объем дисциплины зачетных единиц 2, в академических часах 72

Трудоемкость видов учебной работы приведена в таблице.

Виды учебной работы и их трудоемкость

Форма обучения	Семестр	Трудо емкость	Лекции (час)	Лабора торные занятия (час)	Промежуто чный контроль (час)	Самостоятельная работа (час)	Итоговая аттестация
Очная	10	72	12	20		40	зачет
Заочная	10	72	4	4		64	зачет