Приложение А

Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Дагестанский государственный технический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине « Методы и средства защиты информации**»**

Уровень образования: бакалавриат
(бакалавриат/магистратура/специалитет)

Направление подготовки бакалавриата/магистратуры/специальность: 01.03.02 - Прикладная математика и информатика
(код, наименование направления подготовки/специальности)

Профиль направления подготовки/специализация: Системное программирование и компьютерные технологии
(наименование)

Разработчик _____ Пиняскин В.В. к.х.н., доцент
подпись (ФИО уч. степень, уч. звание)

Фонд оценочных средств обсужден на заседании кафедры ПМиИ
«11» 9 2019 г., протокол №

Зав. кафедрой _____ Исабекова Т.И. к.ф-м.н., доцент
подпись (ФИО уч. степень, уч. звание)

г. Махачкала 2019

СОДЕРЖАНИЕ

Стр.

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины «Методы и средства защиты информации» и предназначен для контроля и оценки образовательных достижений, обучающихся (в т.ч. по самостоятельной работе студентов, далее – СРС), освоивших программу данной дисциплины.

Целью фонда оценочных средств является установление соответствия уровня подготовки обучающихся требованиям ФГОС ВО по направлению подготовки 01.03.02 – «Прикладная математика и информатика» дисциплины «Методы и средства защиты информации» предусмотрено формирование следующих компетенций:

1) ПК-7 Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения
2) ПК-8 Способен осуществлять конфигурирование операционных систем и сетевых устройств;
3) ПК-9. Способен осуществлять управление программно- аппаратными средствами информационных служб инфокоммуникационной системы организации

2. Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля)

Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля), и используемые оценочные средства приведены в таблице 1.

2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП

Таблица 1

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	Критерии оценивания	Наименование контролируемых разделов и тем[1]
ПК-7 Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения	ПК-7.1 Знает виды угроз информационных систем и методы обеспечения информационной безопасности	**Знать:** виды угроз информационных систем и методы обеспечения информационной безопасности **Владеть:** навыком защиты от угроз информационных систем и методами обеспечения информационной безопасности **Уметь:** управлять безопасностью от разного вида угроз информационных систем и обеспечение информационной безопасности	ТЕМА 1. Введение ТЕМА 2. Каналы утечки информации из компьютерных систем
	ПК-7.2 Умеет организовать комплексную защиту информационных систем	**Знать:** комплексную защиту информационных систем **Владеть:** комплексной защитой информационных систем **Уметь:** организовать комплексную защиту информационных систем	ТЕМА 3. Основы теории защиты информации в компьютерных системах
	ПК-7.3 Владеет правовыми, административными, программно-аппаратными средствами информационной защиты, навыками работы с инструментальными средствами	**Знать:** правовые, административные, программно- аппаратными средства информационной защиты, навыками работы с инструментальными средствами защиты получения, хранения, обработки и передачи информации.	ТЕМА 4. Основы криптографии

[1] *Наименования разделов и тем должен соответствовать рабочей программе дисциплины.*

	защиты	**Владеть:** правовыми, административными, программно-аппаратными средствами информационной защиты, навыками работы с инструментальными средствами защиты **Уметь:** использовать правовые, административные, программно-аппаратные средства информационной защиты, навыки работы с инструментальными средствами защиты	
ПК-8 Способен осуществлять конфигурирование операционных систем и сетевых устройств	ПК-8.1 Знает основные этапы и их содержание при установке и настройке операционных системи сетевых устройств	**Знать** основные этапы и их содержание при установке и настройке операционных системи сетевых устройств **Владеть** основными этапами и их содержание при установке и настройке операционных системи сетевых устройств **Уметь** осуществлять основные этапы и их содержание при установке и настройке операционных системи сетевых устройств	ТЕМА 5. Применение симметричных криптосистем для защиты компьютерной информации
	ПК-8.2 Умеет осуществлять установку и настройку операционных системи сетевых устройств	**Знать** установку и настройку операционных системи сетевых устройств **Владеть** установкой и настройкой операционных системи сетевых устройств **Уметь** установливать и настраивать операционные системы и сетевые устройства	ТЕМА 6. Инфраструктура открытых ключей

	ПК-8.3 Имеет практический опыт установки и настройки операционных системи сетевых устройств	**Знать** установку и настройки операционных систем и сетевых устройств **Владеть** опытом установки и настройки операционных систем и сетевых устройств **Уметь** устанавливать и настраивать операционные системы и сетевые устройства	ТЕМА 7. Методы идентификации и аутентификации пользователей компьютерных систем
ПК-9. Способен осуществлять управление программно- аппаратными средствами информационных служб инфокоммуникационной системы организации	ПК-9.1.1 Знает методы управления доступом к программно-аппаратным средствам информационных служб инфокоммуникационной системы Выявлен	Знать методы управления доступом к программно-аппаратным средствам информационных служб инфокоммуникационной системы Владеть управлением доступом к программно-аппаратным средствам информационных служб инфокоммуникационной системы Уметь управлять доступом к программно-аппаратным средствам информационных служб инфокоммуникационной системы	ТЕМА 8. Защита компьютерных систем от удаленных атак через сеть Internet.
	ПК-9.1.2 Знает методы восстановления работоспособности программно-аппаратных средств инфокоммуникационной системы и/или ее составляющих после сбоев	Знать методы восстановления работоспособности программно-аппаратных средств инфокоммуникационной системы и/или ее составляющих после сбоев Владеть методами восстановления работоспособности программно-аппаратных средств инфокоммуникационной системы и/или ее составляющих после сбоев Уметь восстановать работоспособность программно-аппаратных средств инфокоммуникационной системы и/или ее составляющих после сбоев	ТЕМА 9. Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)

	ПК-9.1.3 Знает методы обслуживания периферийного оборудования	**Знать** методы обслуживания периферийного оборудования **Владеть** владеет методы обслуживания периферийного оборудования **Уметь** обслуживать периферийного оборудования	ТЕМА 9. Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине «Методы и средства защиты информации» определяется на следующих этапах:

1. **Этап текущих аттестаций**
2. **Этап промежуточных аттестаций**

Таблица 2

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	**Этапы формирования компетенции**					
		Этап текущих аттестаций					**Этап промежуточной аттестации**
		1-5 неделя	**6-10 неделя**	**11-15 неделя**	**1-17 неделя**		**18-20 неделя**
		Текущая аттестация №1	Текущая аттестация №2	Текущая аттестация №3	СРС	КР/КП	Промежуточная аттестация
1		**2**	**3**	**4**	**5**	**6**	**7**
ПК-7 Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения	ПК-7.1 Знает виды угроз информационных систем и методы обеспечения информационной безопасности	Контрольная работа	Контрольная работа	Контрольная работа	Реферат, Устный опрос		*Экзамен по дисциплине*
	ПК-7.2 Умеет организовать комплексную защиту информационных систем	Контрольная работа	Контрольная работа	Контрольная работа	Реферат, Устный опрос		*Экзамен по дисциплине*
	ПК-7.3 Владеет правовыми, административными, программно- аппаратными средствами информационной защиты, навыками работы с инструментальными средствами защиты	Контрольная работа	Контрольная работа	Контрольная работа	Реферат, Устный опрос		*Экзамен по дисциплине*
ПК-8 Способен осуществлять	ПК-8.1 Знает основные этапы и их содержание при установке и настройке операционных системи	Контрольная работа	Контрольная работа	Контрольная работа	Реферат, Устный опрос		*Экзамен по дисциплине*

конфигурирование операционных систем и сетевых устройств	сетевых устройств						
	ПК-8.2 Умеет осуществлятьустановку и настройку операционных системи сетевых устройств	Контрольная работа	Контрольная работа	Контрольная работа	Реферат, Устный опрос		*Экзамен по дисциплине*
	ПК-8.3 Имеет практический опыт установки и настройки операционных системи сетевых устройств	Контрольная работа	Контрольная работа	Контрольная работа	Реферат, Устный опрос		*Экзамен по дисциплине*
ПК-9. Способен осуществлять управление программно-аппаратными средствами информационных служб инфокоммуникационной системы организации	ПК-9.1.1 Знает методы управления доступом к программно-аппаратным средствам информационных служб инфокоммуникационной системы	Контрольная работа	Контрольная работа	Контрольная работа	Реферат, Устный опрос		*Экзамен по дисциплине*
	ПК-9.1.2 Знает методы восстановления работоспособности программно-аппаратных средств инфокоммуникационной системы и/или ее составляющих после сбоев	Контрольная работа	Контрольная работа	Контрольная работа	Реферат, Устный опрос		*Экзамен по дисциплине*
	ПК-9.1.3 Знает методы обслуживания периферийного оборудования	Контрольная работа	Контрольная работа	Контрольная работа	Реферат, Устный опрос		*Экзамен по дисциплине*

СРС – самостоятельная работа студентов;
КР – курсовая работа;
КП – курсовой проект.

2.2. Показатели уровней сформированности компетенций на этапах их формирования, описание шкал оценивания

2.2.1. Показатели уровней сформированности компетенций на этапах их формирования

Результатом освоения дисциплины «Методы и средства защиты информации» является установление одного из уровней сформированности компетенций: высокий, повышенный, базовый, низкий.

Таблица 3

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
Высокий (оценка «отлично», «зачтено»)	Сформированы четкие системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные и верные. Даны развернутые ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции	Обучающимся усвоена взаимосвязь основных понятий дисциплины, в том числе для решения профессиональных задач. Ответы на вопросы оценочных средств самостоятельны, исчерпывающие, содержание вопроса/задания оценочного средства раскрыто полно, профессионально, грамотно. Даны ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции
Повышенный (оценка «хорошо», «зачтено»)	Знания и представления по дисциплине сформированы на повышенном уровне. В ответах на вопросы/задания оценочных средств изложено понимание вопроса, дано достаточно подробное описание ответа, приведены и раскрыты в тезисной форме основные понятия. Ответ отражает полное знание материала, а также наличие, с незначительными пробелами, умений и навыков по изучаемой дисциплине. Допустимы единичные негрубые ошибки. Обучающимся продемонстрирован повышенный уровень освоения компетенции	Сформированы в целом системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные, грамотные. Продемонстрирован повышенный уровень владения практическими умениями и навыками. Допустимы единичные негрубые ошибки по ходу ответа, в применении умений и навыков
Базовый (оценка «удовлетворительно», «зачтено»)	Ответ отражает теоретические знания основного материала дисциплины в объеме, необходимом для дальнейшего освоения ОПОП. Обучающийся допускает неточности в ответе, но обладает необходимыми знаниями для их	Обучающийся владеет знаниями основного материал на базовом уровне. Ответы на вопросы оценочных средств неполные, допущены существенные ошибки. Продемонстрирован базовый уровень владения

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
	устранения. Обучающимся продемонстрирован базовый уровень освоения компетенции	практическими умениями и навыками, соответствующий минимально необходимому уровню для решения профессиональных задач
Низкий (оценка «неудовлетворительно», «не зачтено»)	Демонстрирует полное отсутствие теоретических знаний материала дисциплины, отсутствие практических умений и навыков	

2.2.2. Описание шкал оценивания

В ФГБОУ ВО «ДГТУ» внедрена модульно-рейтинговая система оценки учебной деятельности студентов. В соответствии с этой системой применяются пятибальная, двадцатибальная и стобальная шкалы знаний, умений, навыков.

Шкалы оценивания			Критерии оценивания
пятибальная	двадцатибальная	стобальная	
«Отлично» - 5 баллов	«Отлично» - 18-20 баллов	«Отлично» - 85 – 100 баллов	Показывает высокий уровень сформированности компетенций, т.е.: – продемонстрирует глубокое и прочное усвоение материала; – исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал; – правильно формирует определения; – демонстрирует умения самостоятельной работы с нормативно-правовой литературой; – умеет делать выводы по излагаемому материалу.
«Хорошо» - 4 баллов	«Хорошо» - 15 - 17 баллов	«Хорошо» - 70 - 84 баллов	Показывает достаточный уровень сформированности компетенций, т.е.: – демонстрирует достаточно полное знание материала, основных теоретических положений; – достаточно последовательно, грамотно логически стройно излагает материал; – демонстрирует умения ориентироваться в нормальной литературе; – умеет делать достаточно обоснованные выводы по излагаемому материалу.
«Удовлетворительно» - 3 баллов	«Удовлетворительно» - 12 - 14 баллов	«Удовлетворительно» - 56 – 69 баллов	Показывает пороговый уровень сформированности компетенций, т.е.: – демонстрирует общее знание изучаемого материала; – испытывает серьезные затруднения при ответах на дополнительные вопросы; – знает основную рекомендуемую литературу; – умеет строить ответ в соответствии со структурой излагаемого материала.
«Неудовлетворительно» - 2 баллов	«Неудовлетворительно» - 1-11 баллов	«Неудовлетворительно» - 1-55 баллов	Ставится в случае: – незнания значительной части программного материала; – не владения понятийным аппаратом дисциплины; – допущения существенных ошибок при изложении учебного материала; – неумение строить ответ в соответствии со структурой излагаемого вопроса; – неумение делать выводы по излагаемому материалу.

3. Типовые контрольные задания, иные материалы и методические рекомендации, необходимые для оценки сформированности компетенций в процессе освоения ОПОП

3.1.Задания и вопросы для входного контроля

1. Принципы построения и архитектуру вычислительных систем;
2. Виды контента информационных ресурсов предприятия и интернет-ресурсов;
3. Основы безопасности жизнедеятельности в области профессиональной деятельности;
4. Методы и средства обеспечения информационной безопасности компьютерных систем;
5. Базовые понятия и определения, используемые в сфере информационной безопасности;
6. Основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам

3.2. Оценочные средства и критерии сформированности компетенций

Аттестационная контрольная работа №1

Комплект заданий для контрольной работы

- Время выполнения 45 мин.
- Количество вариантов контрольной работы - 3
- Количество заданий в каждом варианте контрольной работы - 3.
- Форма работы – самостоятельная, индивидуальная.

Вариант 1

Задание 1	Современные аспекты безопасности информационных систем.
Задание 2	Понятие «информационная безопасность» и «защита информации».
Задание 3	Назначение организационных средств защиты

Вариант 2

Задание 1	Понятие ПЭМИН
Задание 2	Методы защиты компьютеров от утечки ПЭМИН.
Задание 3	Назначение генератора шума.

Вариант 3

Задание 1	Классификация угроз безопасности.
Задание 2	Назначение средств защиты от НДС. Основные свойства защищаемой информации
Задание 3	Классификация угроз безопасности.

Аттестационная контрольная работа №2

Комплект заданий для контрольной работы

- Время выполнения 90 мин.
- Количество вариантов контрольной работы - 2
- Количество заданий в каждом варианте контрольной работы - 3.
- Форма работы – самостоятельная, индивидуальная.

Вариант 1

Задание 1	Криптографическая защита информации в каналах связи и компьютерах.
Задание 2	Основные термины и понятия криптографии. Классификация криптосистем
Задание 3	Криптографическая защита информации в каналах связи и компьютерах.

Вариант 2

Задание 1	Отечественный алгоритм шифрования ГОСТ 28147-89
Задание 2	Режимы шифрования криптосистемы ГОСТ 28147-89
Задание 3	Сравнительный анализ криптосистем DES и ГОСТ 28147-89.

Аттестационная контрольная работа №3

Комплект заданий для контрольной работы

- Время выполнения 90 мин.
- Количество вариантов контрольной работы - 3
- Количество заданий в каждом варианте контрольной работы 3.
- Форма работы – самостоятельная, индивидуальная.

Вариант 1

Задание 1	Алгоритмы рюкзака.
Задание 2	Алгоритм RSA.
Задание 3	Схема шифрования Эль-Гамаля

Вариант 2

Задание 1	Понятия идентификации, аутентификации и авторизации.
Задание 2	Парольная аутентификация.
Задание 3	Взаимная проверка пользователей

Вариант 3

Задание 1	Классификация способов защиты от изучения и разрушающих программ ных воздействий.
Задание 2	Методы перехвата и навязывания информации.
Задание 3	Методы внедрения программных закладок

Критерии оценки уровня сформированности компетенций при проведении контрольной работы:

- оценка «отлично»: продемонстрировано грамотное последовательное решение задач (заданий) при правильно выбранном алгоритме. Даны верные ответы на все вопросы и условия задач (заданий). При необходимости сделаны пояснения и выводы (содержательные,

достаточно полные, правильные, учитывающие специфику проблемной ситуации в задаче или с незначительными ошибками);

- оценка «хорошо»: грамотное последовательное решение задач (заданий) при правильно выбранном алгоритме. Однако, ответы на вопросы и условия задач (заданий) содержат незначительные ошибки. Пояснения и выводы отсутствуют или даны неверно;

- оценка «удовлетворительно»: обучающийся ориентируется в материале, но применяет его неверно, выбирает неправильный алгоритм решения задач (неверные исходные данные, неверная последовательность решения и др. ошибки), допускает вычислительные ошибки. Пояснения и выводы отсутствуют или даны неверно;

- оценка «неудовлетворительно»: обучающийся слабо ориентируется в материале, выбирает неправильный алгоритм решения, допускает значительное количество вычислительных ошибок. Пояснения и выводы отсутствуют.

Устный опрос по теме 1 «Введение»

• Содержит 3 вопроса.
• Форма опроса – фронтальный/индивидуальный/комбинированный.

Задания к устному опросу

1. Современные аспекты безопасности информационных систем.
2. Понятие «информационная безопасность» и «защита информации».
3. Назначение организационных средств защиты

Устный опрос по теме 2 «Каналы утечки информации из компьютерных систем»

• Содержит 3 вопроса.
• Форма опроса – фронтальный/индивидуальный/комбинированный.

Задания к устному опросу

1. Понятие ПЭМИН
2. Методы защиты компьютеров от утечки ПЭМИН.
3. Назначение генератора шума.

Устный опрос по теме 3 «Основы теории защиты информации в компьютерных системах»

• Содержит 3 вопроса.
• Форма опроса – фронтальный/индивидуальный/комбинированный.

Задания к устному опросу

1. Классификация угроз безопасности.
2. Назначение средств защиты от НДС.
3. Основные свойства защищаемой информации

Устный опрос по теме 4 «Основы криптографии»

• Содержит 3 вопроса.
• Форма опроса – фронтальный/индивидуальный/комбинированный.

Задания к устному опросу

1. Криптографическая защита информации в каналах связи и компьютерах.
2. Основные термины и понятия криптографии.
3. Классификация криптосистем.

Устный опрос по теме 5 «Применение симметричных криптосистем для защиты компьютерной информации»

• Содержит 3 вопроса.
• Форма опроса – фронтальный/индивидуальный/комбинированный.

Задания к устному опросу

1. Отечественный алгоритм шифрования ГОСТ 28147-89
2. Режимы шифрования криптосистемы ГОСТ 28147-89
3. Сравнительный анализ криптосистем DES и ГОСТ 28147-89.

Устный опрос по теме 6 «Инфраструктура открытых ключей»

• Содержит 3 вопроса.
• Форма опроса – фронтальный/индивидуальный/комбинированный.

Задания к устному опросу

1. Алгоритмы рюкзака.
2. Алгоритм RSA.
3. Схема шифрования Эль-Гамаля

Устный опрос по теме 7 «Методы идентификации и аутентификации пользователей компьютерных систем»

• Содержит 3 вопроса.
• Форма опроса – фронтальный/индивидуальный/комбинированный.

Задания к устному опросу

1. Понятия идентификации, аутентификации и авторизации.
2. Парольная аутентификация.
3. Взаимная проверка пользователей.
4. Система Kerberos.

Устный опрос по теме 8 «Защита компьютерных систем от удаленных атак через сеть Internet»

• Содержит 3 вопроса.
• Форма опроса – фронтальный/индивидуальный/комбинированный.

Задания к устному опросу

1. Туннелирование на канальном уровне. Протоколы PPTP и L2TP.
2. Туннелирование на сетевом уровне. Архитектура IPSec.

3. Защита соединения на сеансовом уровне. Протоколы SSL и TLS.

Устный опрос по теме 9 «Методы защита программ от изучения и разрушающих программных воздействий»

• Содержит 5 вопросов.
• Форма опроса – фронтальный/индивидуальный/комбинированный.

Задания к устному опросу

1. Классификация способов защиты от изучения и разрушающих программных воздействий.
2. Методы перехвата и навязывания информации.
3. Методы внедрения программных закладок.
4. Проблемы компьютерной безопасности.
5. Перспективные направления исследований в компьютерной безопасности

Критерии оценки уровня сформированности компетенций для устного опроса:

- оценка «отлично»: обучающимся дан полный, развернутый ответ на поставленный вопрос; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание по дисциплине демонстрируются на фоне понимания его в системе данной науки и междисциплинарных связей. Обучающийся владеет терминологией, способен приводить примеры, высказывает свою точку зрения с опорой на знания и опыт;

- оценка «хорошо»: обучающимся дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ логичен, выстроен, но совершены единичные ошибки. Не в полной мере владеет знаниями по всей дисциплине. Даны ответы на дополнительные, поясняющие вопросы;

- оценка «удовлетворительно»: ответ на вопрос не полный, с ошибками. Обучающийся путается в деталях, с затруднением пользуется профессиональной терминологией. Есть замечания к построению ответа, к логике и последовательности изложения. Не отвечает на дополнительные вопросы;

- оценка «неудовлетворительно»: ответ представляет собой разрозненные знания с существенными ошибками по вопросу, присутствует фрагментарность, нелогичность изложения. Обучающийся не осознает связь обсуждаемого вопроса с другими объектами дисциплины, речь неграмотная, не используется профессиональная терминология. Ответы на дополнительные вопросы не даны или неверные.

Критерии оценки уровня сформированности компетенций при выполнении курсовой работы/курсового проекта:

- оценка «отлично»: продемонстрировано блестящее владение проблемой исследования, материал выстроен логично, последовательно, обучающийся аргументированно отстаивает свою точку зрения. Во введении приводится обоснование выбора конкретной темы, чётко определены цель и задачи работы (проекта). Использован достаточный перечень источников и литературы для методологической базы исследования. Обучающийся грамотно использует профессиональные термины, актуальные исходные данные. Проведен самостоятельный анализ (исследование) объекта. По результатам работы сделаны логичные выводы. Оформление работы соответствует методическим рекомендациям. Объем и содержание работы соответствует требованиям. На защите обучающийся исчерпывающе отвечает на все дополнительные вопросы;

- оценка «хорошо»: обучающийся демонстрирует повышенный уровень владения проблемой исследования, логично, последовательно и аргументированно отстаивает ее концептуальное содержание. Во введении содержатся небольшие неточности в формулировках цели, задач. В основной части допущены незначительные погрешности в расчетах (в исследовании). Выводы обоснованы, аргументированы. Оформление работы соответствует методическим рекомендациям. Объем работы соответствует требованиям. На защите обучающийся отвечает на все дополнительные вопросы;

- оценка «удовлетворительно»: обучающийся демонстрирует базовый уровень владения проблемой исследования. Во введении указаны цель и задачи исследования, но отсутствуют их четкие формулировки. Работа является компиляцией чужих исследований с попыткой формулировки собственных выводов в конце работы. Изложине материала логично и аргументировано. Наблюдается отступление от требований в оформлении и объеме работы. При ответе на вопросы обучающийся испытывает затруднения;

- оценка «неудовлетворительно»: обнаруживается несамостоятельность выполнения курсовой работы, некомпетентность в исследуемой проблеме. Нарушена логика изложения. Работа не соответствует требованиям, предъявляемым к оформлению и содержанию. На защите курсовой работы обучающийся не отвечает на вопросы.

Темы рефератов по дисциплине «Методы и средства защиты информации»

1. Автоматизированные системы.
2. Защита от несанкционированного доступа к информации.
3. Классификация автоматизированных систем и требования по защите информации.
4. Безопасность информационных технологий.
5. ГОСТ 34.10-94. Информационная технология. Криптографическая защита информации.
6. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
7. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.
8. Средства вычислительной техники. Защита от несанкционированного доступа к информации.
9. Показатели защищенности СВТ от НСД к информации.

3.3. Задания для промежуточной аттестации (экзамен)

Список вопросов к экзамену

1. Что такое информационная безопасность?
2. Какие предпосылки и цели обеспечения информационной безопасности?
3. В чем заключаются национальные интересы РФ в информационной сфере?
4. Что включает в себя информационная борьба?
5. Какие пути решения проблем информационной безопасности РФ существуют?
6. Каковы общие принципы обеспечения защиты информации?
7. Какие имеются виды угроз информационной безопасности предприятия (организации)?
8. Какие источники наиболее распространенных угроз информационной безопасности существуют?

9. Какие виды сетевых атак имеются?
10. Какими способами снизить угрозу сниффинга пакетов?
11. Какие меры по устранению угрозы IP -спуфинга существуют?
12. Что включает борьба с атаками на уровне приложений?
13. Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
14. В чем заключается распределенное хранение файлов?
15. Что включают в себя требования по обеспечению комплексной системы информационной безопасности?
16. Основные принципы цифровых медиа.
17. Современные аспекты безопасности информационных систем.
18. Понятие «информационная безопасность» и «защита информации».
19. Назначение организационных средств защиты
20. Понятие ПЭМИН
21. Методы защиты компьютеров от утечки ПЭМИН.
22. Назначение генератора шума.
23. Классификация угроз безопасности.
24. Назначение средств защиты от НДС.
25. Основные свойства защищаемой информации.
26. Криптографическая защита информации в каналах связи и компьютерах.
27. Основные термины и понятия криптографии. 3.Классификация криптосистем.
28. Отечественный алгоритм шифрования ГОСТ 28147-89
29. Режимы шифрования криптосистемы ГОСТ 28147-89
30. Сравнительный анализ криптосистем DES и ГОСТ 28147-89.
31. Алгоритмы рюкзака.
32. Алгоритм RSA.
33. Схема шифрования Эль-Гамаля.
34. Понятия идентификации, аутентификации и авторизации.
35. Парольная аутентификация.
36. Взаимная проверка пользователей.
37. Система Kerberos.
38. Туннелирование на канальном уровне. Протоколы PPTP и L2TP.
39. Туннелирование на сетевом уровне. Архитектура IPSec.
40. Защита соединения на сеансовом уровне. Протоколы SSL и TLS.
41. Классификация способов защиты от изучения и разрушающих программных воздействий.
42. Методы перехвата и навязывания информации.
43. Методы внедрения программных закладок.
44. Проблемы компьютерной безопасности.
45. Перспективные направления исследований в компьютерной безопасности.

Зачеты могут быть проведены в письменной форме, а также в письменной форме с устным дополнением ответа. Зачеты служат формой проверки качества выполнения студентами лабораторных работ, усвоения семестрового учебного материала по дисциплине (модулю), практических и семинарских занятий (при отсутствии экзамена по дисциплине).

По итогам зачета, соответствии с модульно – рейтинговой системой университета, выставляются баллы с последующим переходом по шкале баллы – оценки за зачет, выставляемый как по наименованию «зачтено», «не зачтено», так и дифференцированно

т.е. с выставлением отметки по схеме – «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно», определяемое решением Ученого совета университета и прописываемого в учебном плане.

Критерии оценки уровня сформированности компетенций по результатам проведения зачета:

- оценка «зачтено»: обучающийся демонстрирует всестороннее, систематическое и глубокое знание материала, свободно выполняет задания, предусмотренные программой дисциплины, усвоивший основную и дополнительную литературу. Обучающийся выполняет задания, предусмотренные программой дисциплины, на уровне не ниже базового;
- оценка «не зачтено»: обучающийся демонстрирует незнание материала, не выполняет задания, предусмотренные программой дисциплины. Обучающийся не выполняет задания, предусмотренные программой дисциплины, на уровне ниже базового. Дальнейшее освоение ОПОП невозможно без дополнительного изучения материала и подготовки к зачету.