Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра вычислительной техники
Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н., доцент И.Л. Рева
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Криптографические методы защиты информации

Образовательная программа: 09.04.01 Информатика и вычислительная техника, магистерская программа: Кибербезопасность информационных систем

Новосибирск 2017

1. **Обобщенная структура фонда оценочных средств учебной дисциплины**

Обобщенная структура фонда оценочных средств по **дисциплине** Криптографические методы защиты информации приведена в Таблице.

Таблица

Формируемые компетенции	**Показатели сформированности компетенций (знания, умения, навыки)**	**Темы**	**Этапы оценки компетенций**	
			Мероприятия текущего контроля (курсовой проект, РГЗ(Р) и др.)	**Промежуточная аттестация (экзамен, зачет)**
ОК.4 способность заниматься научными исследованиями	у1. способность осуществлять научно-исследовательскую деятельность в области задач математического моделирования объектов профессиональной деятельности	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 1-2	Зачет, вопросы 1-5
ОК.9 умение оформлять отчеты о проведенной научно-исследовательской работе и подготавливать публикации по результатам исследования	у1. составлять аналитические отчеты по результатам эксперимента, моделирования, сбора и обработки данных, содержащих постановку задачи, анализ и интерпретацию результатов, выводы и рекомендации	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 2-3	Зачет, вопросы 6-9
ОПК.2 культурой мышления, способность выстраивать логику рассуждений и высказываний, основанных на интерпретации данных, интегрированных из разных областей науки и техники, выносить суждения на основании неполных данных	з2. знать основные методы научного познания	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 1-3	Зачет, вопросы 10-15
ОПК.2	у2. анализировать и интерпретировать в терминах решаемой задачи результаты, полученные в процессе моделирования, сбора и обработки данных	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 4	Зачет, вопросы 16-18

ПК.2/НИ знанием методов научных исследований и владение навыками их проведения	з5. основные методы, области использования, ограничения, достоинства и недостатки, инструментальные средства математического моделирования объектов профессиональной деятельности	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 2-4	Зачет, вопросы 19-22
ПК.2/НИ	у4. выполнять сравнительный анализ эффективности применения различных методов математического моделирования в рамках решаемой задачи	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 1-4	Зачет, вопросы 22-25
ПК.2/НИ	у5. планировать и проводить машинные эксперименты с имитационными моделями объектов профессиональной деятельности, статистически обрабатывать и интерпретировать полученные результаты	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 1-4	Зачет, вопросы 26-28
ПК.2/НИ	у6. разрабатывать математические модели объектов профессиональной деятельности с использованием специализированны х инструментальных средств	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 1-4	Зачет, вопросы 18-21
ПК.3/НИ знанием методов оптимизации и умение применять их при решении задач профессиональной деятельности	з2. знать основные математические методы оптимизации процесса функционирования объектов профессиональной деятельности	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 1-4	Зачет, вопросы 22-24
ПК.3/НИ	у4. уметь осуществлять математическую постановку задачи оптимизации процесса функционирования объектов	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 1-4	Зачет, вопросы 25-28

	профессиональной деятельности (ОПД), решать ее с помощью специализированных инструментальных средств, анализировать полученные результаты, выдавать практические рекомендации по оптимизации работы ОПД.			

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 2 семестре - в форме дифференцированного зачета, который направлен на оценку сформированности компетенций ОК.4, ОК.9, ОПК.2, ПК.2/НИ, ПК.3/НИ.

Зачет проводится в устной форме, по билетам.

Кроме того, сформированность компетенций проверяется при проведении мероприятий текущего контроля, указанных в таблице раздела 1.

В 2 семестре обязательным этапом текущей аттестации является расчетно-графическое задание (работа) (РГЗ(Р)). Требования к выполнению РГЗ(Р), состав и правила оценки сформулированы в паспорте РГЗ(Р).

Общие правила выставления оценки по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе учебной дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ОК.4, ОК.9, ОПК.2, ПК.2/НИ, ПК.3/НИ, за которые отвечает дисциплина, на разных уровнях.

Общая характеристика уровней освоения компетенций.

Ниже порогового. Уровень выполнения работ не отвечает большинству основных требований, теоретическое содержание курса освоено частично, пробелы могут носить существенный характер, необходимые практические навыки работы с освоенным материалом сформированы не достаточно, большинство предусмотренных программой обучения учебных заданий не выполнены или выполнены с существенными ошибками.

Пороговый. Уровень выполнения работ отвечает большинству основных требований, теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые виды заданий выполнены с ошибками.

Базовый. Уровень выполнения работ отвечает всем основным требованиям, теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые из выполненных заданий, возможно, содержат ошибки.

Продвинутый. Уровень выполнения работ отвечает всем требованиям, теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.