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

Кафедра оптических информационных технологий

“УТВЕРЖДАЮ”
ДЕКАН ФТФ
к.ф-м.н., доцент И.И. Корель

ДОКУМЕНТ ПОДПИСАН ПРОСТОЙ НЕКВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ
31.08.2026
Владелец: И.И. Корель
Срок действия: не ограничен
Адрес хранения электронного документа:
https://www.nstu.ru/university/info/sveden/education

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ДИСЦИПЛИНЫ

Квантовая криптография

Образовательная программа: 12.04.02 Оптотехника, магистерская программа: Оптические системы локации, связи и обработки информации

Новосибирск 2026

1. Обобщенная структура фонда оценочных средств дисциплины

Обобщенная структура фонда оценочных средств по **дисциплине** Квантовая криптография представлена в Таблице. Совокупность результатов обучения по дисциплине соотнесена с уровнями сформированности компетенций и соотнесенными с ними индикаторами. Индикаторы достижения компетенций измеряемы с помощью средств текущей и промежуточной аттестации по **дисциплине** Квантовая криптография.

Таблица

Формируемые компетенции	**Индикаторы компетенций**	**Темы**	**Этапы оценки результатов обучения и соотнесенных с ними индикаторов достижения компетенций**	
			Мероприятия текущего контроля (контрольная работа, курсовой проект, РГЗ(Р), реферат и др.)	**Промежуточная аттестация (экзамен, зачет)**
ОПК-1 Способен представлять современную научную картину мира, выявлять естественнонаучную сущность проблемы, формулировать задачи, определять пути их решения и оценивать эффективность выбора и методов правовой защиты результатов интеллектуальной деятельности с учетом специфики исследований для разработки оптической техники, оптических материалов и технологий оптического производства	1. Представляет современную научную картину мира, выявляет естественнонаучную сущность проблемы	Алгоритм RSA Секретные системы Способы изображения секретных систем. Примеры секретных систем Теоретическая секретность Шифр XOR Шифр Виженера Шифр «Сцитала» Шифрование с открытым ключом	Контрольные работы, раздел 3	Зачет, вопросы 4-8
ОПК-1	2. Формулирует задачи, определяет пути их решения и оценивает эффективность выбора	Основные понятия, термины, определения. Предмет криптографии Секретные системы Теоретическая секретность		Зачет, вопросы 1, 2, 3, 10
ПК-1/НА Способность к анализу состояния научно-технической проблемы, технического задания и постановке цели и	2. Проводит поиск и анализ научно-технической информации, отечественного и зарубежного опыта по разработке оптических и	Алгоритм RSA Основные понятия, термины, определения. Предмет криптографии Секретные системы		Зачет, вопрос 12

задач проектирования оптических и оптико-электронных приборов, систем и комплексов на основе подбора и изучения литературных и патентных источников	оптико-электронных приборов и комплексов			
ПК-2/НА Способность к построению математических моделей объектов исследования и выбору численного метода их моделирования, разработке нового или выбор готового алгоритма решения задачи	1. Формулирует постановку задачи и определяет набор параметров, с учётом которых должно быть проведено моделирование процессов, явлений и особенностей работы изделий оптотехники	Алгоритм RSA Основные понятия, термины, определения. Предмет криптографии Теоретическая секретность Шифр Цезаря		Зачет, вопрос 12
ПК-2/НА	3. Разрабатывает математические модели функционирования оптико-электронных приборов на основе физических процессов и явлений	Способы изображения секретных систем. Примеры секретных систем Шифр Виженера		Зачет, вопросы 6-9
ПК-2/НА	4. Проводит компьютерное моделирование функционирования оптико-электронных приборов на основе физических процессов и явлений	Алгоритм RSA Алгоритмы шифрования DES и ГОСТ 28146-89 Математические основы криптографии. Направления современной криптографии Основные понятия, термины, определения. Предмет криптографии Секретные системы Способы изображения секретных систем. Примеры секретных систем Теоретическая секретность Шифр XOR Шифр Виженера Шифр «Сцитала» Шифр Цезаря Шифрование с открытым ключом	Контрольные работы, разделы 1-5	Зачет, вопросы 1-15
УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	2. Представляет результаты академической и профессиональной деятельности на различных научных мероприятиях, включая международные	Математические основы криптографии. Направления современной криптографии	Контрольные работы, разделы 1-5	Зачет, вопрос 2

2. Методика оценки этапов формирования компетенций по дисциплине

Результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций проверяются при проведении мероприятий текущей аттестации (контроля) в процессе изучения дисциплины, указанных в таблице раздела 1.

В 3 семестре обязательным этапом текущей аттестации является контрольная работа. Требования к выполнению контрольной работы, состав и правила оценки сформулированы в паспорте контрольной работы.

Промежуточная аттестация по **дисциплине** проводится в 3 семестре - в форме зачета, который направлен на оценку сформированности результатов обучения по дисциплине (модулю), соотнесенных с установленными в программе индикаторами достижения компетенций ОПК-1, ПК-1/НА, ПК-2/НА, УК-4 и соотнесенных с ними индикаторов. (см. таблицу раздела 1).

Зачет проводится в устной форме, по билетам.

Общие правила выставления оценок текущей и промежуточной аттестации по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе дисциплины.

На основании критериев, приведенных в п. 3, осуществляется оценка уровней достигнутых результатов обучения по дисциплине, соотнесенных с установленными в программе индикаторами достижения компетенций ОПК-1, ПК-1/НА, ПК-2/НА, УК-4, закрепленных за дисциплиной.

3. Общая характеристика уровней результатов обучения, соотнесенных с индикаторами достижения компетенций

Продвинутый. Теоретическое содержание курса освоено полностью. Студент демонстрирует систематическое и глубокое понимание учебного материала и способность к самостоятельному пополнению и обновлению знаний в ходе дальнейшей учебной работы и профессиональной деятельности. Сформированы необходимые навыки практической работы. Все учебные задания, предусмотренные программой обучения, выполнены качественно, без замечаний. Результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов, входящим в диапазон продвинутого уровня.

Базовый. Теоретическое содержание курса освоено в объеме, необходимом для дальнейшей учебы и профессиональной деятельности. Навыки практической работы сформированы на базовом уровне. Все предусмотренные программой обучения учебные задания выполнены с небольшими погрешностями. Результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов в пределах базового уровня.

Пороговый. Теоретическое содержание курса освоено в объеме, необходимом для дальнейшей учебы и профессиональной деятельности. Некоторые практические навыки работы с сформированы с пробелами. Учебные задания, предусмотренные программой обучения, выполнялись с ошибками, исправленными под руководством преподавателя. Результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов в пределах порогового уровня.

Ниже порогового. Теоретическое содержание курса освоено фрагментарно. Необходимые навыки практической работы сформированы минимально. Большинство учебных заданий, предусмотренных программой обучения, не выполнены. Результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов, входящих в диапазон ниже порогового уровня.