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

Кафедра оптических информационных технологий

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

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

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
# Квантовая криптография

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

Курс: 2, семестр : 3

Физико-технический факультет,

| | | Семестр |
|---|---|---|
| № | Вид деятельности | 3 |
| 1 | Всего зачетных единиц (кредитов) | 4 |
| 2 | Всего часов | 144 |
| 3 | Всего занятий в контактной форме, час. | 19 |
| 4 | Лекции, час. | 8 |
| 5 | Практические занятия, час. | 2 |
| 6 | Лабораторные занятия, час. | 0 |
| 7 | из них в активной и интерактивной форме, час. | 0 |
| 8 | из них практической подготовки, час. | 3 |
| 9 | Аттестация, час. | 2 |
| 10 | Консультации, час. | 7 |
| 11 | Самостоятельная работа, час. | 125 |
| 12 | Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ(Р)/реферат, подготовка к контрольной работе) | контр. |
| 13 | Вид аттестации | 3 |

Новосибирск 2026

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 12.04.02 Оптотехника

ФГОС введен в действие приказом №941 от 19.09.2017 г. , дата утверждения: 06.10.2017 г.

Место дисциплины в структуре учебного плана: Факультативные дисциплины, формируемая участниками образовательных отношений

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 12.04.02 Оптотехника

Рабочая программа обсуждена на заседании кафедры

ОИТ, 31.08.2026

Утверждена на совете физико-технического факультета, протокол № 6 от 31.08.2026

Заведующий кафедрой:

доцент, к.т.н. Завьялова М. А.

Ответственный за образовательную программу:

профессор Дубнищев Ю. Н.

## 1. Внешние требования

Таблица 1.1

| Группа | Компетенции |
|---|---|
| | **Индикаторы достижения компетенций** |
| Общепрофессиональные компетенции | 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 |
| | ОПК-1. 1 Представляет современную научную картину мира, выявляет естественнонаучную сущность проблемы |
| | ОПК-1. 2 Формулирует задачи, определяет пути их решения и оценивает эффективность выбора |
| Профессиональные компетенции | ПК-1/НА Способность к анализу состояния научно-технической проблемы, технического задания и постановке цели и задач проектирования оптических и оптико-электронных приборов, систем и комплексов на основе подбора и изучения литературных и патентных источников |
| | ПК-1/НА. 2 Проводит поиск и анализ научно-технической информации, отечественного и зарубежного опыта по разработке оптических и оптико-электронных приборов и комплексов |
| Профессиональные компетенции | ПК-2/НА Способность к построению математических моделей объектов исследования и выбору численного метода их моделирования, разработке нового или выбор готового алгоритма решения задачи |
| | ПК-2/НА. 1 Формулирует постановку задачи и определяет набор параметров, с учётом которых должно быть проведено моделирование процессов, явлений и особенностей работы изделий оптотехники |
| | ПК-2/НА. 3 Разрабатывает математические модели функционирования оптико-электронных приборов на основе физических процессов и явлений |
| | ПК-2/НА. 4 Проводит компьютерное моделирование функционирования оптико-электронных приборов на основе физических процессов и явлений |
| Универсальные компетенции | УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия |
| | УК-4. 2 Представляет результаты академической и профессиональной деятельности на различных научных мероприятиях, включая международные |

## 2. Требования НГТУ к планируемым результатам обучения, соотнесенным с индикаторами достижения компетенций

Таблица 2.1

| Индикаторы достижения компетенций | Формы организации занятий |
|---|---|
| **Результаты обучения** | |
| **ОПК-1. 1 Представляет современную научную картину мира, выявляет естественнонаучную сущность проблемы** | |
| уметь читать и реферировать литературу на иностранном языке | Лекции; Самостоятельная работа |
| **ОПК-1. 2 Формулирует задачи, определяет пути их решения и оценивает эффективность выбора** | |
| Готов формулировать задачи, определять пути их решения и оценивать эффективность выбора | Лекции; Самостоятельная работа |
| **ПК-1/НА. 2 Проводит поиск и анализ научно-технической информации, отечественного и зарубежного опыта по разработке оптических и оптико-электронных приборов и комплексов** | |

| | |
|---|---|
| уметь проводить поиск и анализ отечественной и зарубежной научно-технической информации по разработке оптических и оптико-электронных приборов и комплексов | Лекции; Самостоятельная работа |
| **ПК-2/НА. 1 Формулирует постановку задачи и определяет набор параметров, с учётом которых должно быть проведено моделирование процессов, явлений и особенностей работы изделий оптотехники** | |
| уметь определять набор входных параметров, с учётом которых должно быть проведено моделирование процессов, явлений и особенностей работы изделий оптотехники | Лекции; Самостоятельная работа |
| **ПК-2/НА. 3 Разрабатывает математические модели функционирования оптико-электронных приборов на основе физических процессов и явлений** | |
| уметь проводить технические расчеты по проектам, технико-экономическому и функционально-стоимостному анализу эффективности проектируемых приборов и систем, включая оценку инновационных рисков коммерциализации проектов | Лекции; Самостоятельная работа |
| **ПК-2/НА. 4 Проводит компьютерное моделирование функционирования оптико-электронных приборов на основе физических процессов и явлений** | |
| знать основы методов шифрования информации с различным уровнем криптостойкости | Лекции; Самостоятельная работа |
| уметь программно реализовать вышеупомянутые методы | Лекции; Практические занятия; Самостоятельная работа |
| **УК-4. 2 Представляет результаты академической и профессиональной деятельности на различных научных мероприятиях, включая международные** | |
| Иметь опыт представления результатов исследования на научных конференциях, включая международные | Лекции; |

## 3. Содержание и структура дисциплины

Таблица 3.1

| Темы лекций | Часы | Из них в форме практ. подг., час. | Активные формы, час. | Индикаторы достижения компетенций | Учебная деятельность |
|---|---|---|---|---|---|
| **Семестр: 3** | | | | | |
| **Дидактическая единица: Введение в криптографию** | | | | | |
| 1. Основные понятия, термины, определения. Предмет криптографии | 4 | 1 | 0 | ОПК-1.1,ОПК-1.2,ПК-1/НА.2,ПК-2/НА.1,ПК-2/НА.3,ПК-2/НА.4 | Лекция |
| 2. Математические основы криптографии. Направления современной криптографии | 4 | 1 | 0 | ПК-2/НА.4, УК-4.2 | Лекция |

| Темы практических занятий | Часы | Из них в форме практ. подг., час. | Активные формы, час. | Индикаторы достижения компетенций | Учебная деятельность |
|---|---|---|---|---|---|
| **Семестр: 3** | | | | | |
| **Дидактическая единица: Современная криптография** | | | | | |
| 15. Криптографические протоколы | 2 | 0 | 0 | ПК-2/НА.4 | Практическое занятие |

| Темы для самостоятельного изучения | Часы | Из них в форме практ. подг., час. | Активные формы, час. | Индикаторы достижения компетенций | Учебная деятельность |
|---|---|---|---|---|---|
| **Семестр: 3** | | | | | |
| **Дидактическая единица: Классическая криптография** | | | | | |
| 1. Шифр «Сцитала» | 6 | 0 | 0 | ОПК-1.1,ПК-2/НА.3,ПК-2/НА.4 | Самостоятельное изучение материала |
| 3. Шифр Виженера | 6 | 0 | 0 | ОПК-1.1,ПК-2/НА.3,ПК-2/НА.4 | Самостоятельное изучение материала |
| 4. Шифр Цезаря | 4 | 1 | 0 | ПК-2/НА.1, ПК-2/НА.4 | Лекция |
| 4. Шифр XOR | 6 | 0 | 0 | ОПК-1.1,ПК-2/НА.3,ПК-2/НА.4 | Самостоятельное изучение материалов |
| 7. Алгоритмы шифрования DES и ГОСТ 28146-89 | 4 | 0 | 0 | ПК-2/НА.4 | Самостоятельное изучение материала |
| **Дидактическая единица: Теория связи в секретных системах** | | | | | |
| 8. Постановка задачи | 6 | 0 | 0 | ПК-2/НА.4 | Самостоятельное изучение материала |
| 9. Секретные системы | 6 | 0 | 0 | ОПК-1.1,ОПК-1.2,ПК-1/НА.2,ПК-2/НА.4 | Самостоятельное изучение материала |
| 10. Способы изображения секретных систем. Примеры секретных систем | 6 | 0 | 0 | ОПК-1.1,ПК-2/НА.3,ПК-2/НА.4 | Самостоятельное изучение материала |
| 11. Теоретическая секретность | 6 | 0 | 0 | ОПК-1.1,ОПК-1.2,ПК-2/НА.1,ПК-2/НА.3,ПК-2/НА.4 | Самостоятельное изучение материала |
| **Дидактическая единица: Современная криптография** | | | | | |
| 13. Шифрование с открытым ключом | 8 | 0 | 0 | ОПК-1.1,ПК-2/НА.4 | Самостоятельное изучение материала |
| 14. Алгоритм RSA | 8 | 0 | 0 | ОПК-1.1,ПК-1/НА.2,ПК-2/НА.1,ПК-2/НА.3,ПК-2/НА.4 | Самостоятельное изучение материала |

## 3.1 Практическая подготовка

Таблица 3.2

| № | Темы занятий | Формы организации занятий | Содержание практической подготовки (виды работ) |
|---|---|---|---|
| 1 | Основные понятия, термины, определения. Предмет криптографии | Л | Выполняет следующие виды работ: владеет терминологией предмета криптографии |
| 2 | Математические основы криптографии. Направления современной криптографии | Л | Выполняет следующие виды работ: проводит математические расчеты для целей криптоанализа |

| | | | |
|---|---|---|---|
| 3 | Шифр Цезаря | Самост. | Выполняет следующие виды работ: разрабатывает и доказывает криптографическую стойкость систем квантовой криптографии на основе шифра Цезаря |

### 3.2 Самостоятельная работа обучающегося

Таблица 3.3

| № | Виды самостоятельной работы | Индикаторы достижения компетенций | Часы на выполнение | Часы на консультации |
|---|---|---|---|---|
| **Семестр: 3** | | | | |
| 1 | Контрольные работы | ОПК-1.1,ОПК-1.2,ПК-1/НА.2, ПК-2/НА.4 | 10 | 0 |
| : Дудкина М. П. Организация самостоятельной работы студентов Новосибирского государственного технического университета : учебно-методическое пособие / М. П. Дудкина, Ю. В. Никитин ; Новосиб. гос. техн. ун-т.- Новосибирск: Изд-во НГТУ, 2022.- 61, [1] с. : табл.- Текст : непосредственный.- Режим доступа: http://elibrary.nstu.ru/source?bib_id=223022 | | | | |
| 2 | Подготовка к занятиям | ПК-2/НА.4 | 43 | 7 |
| : Гультяева Т. А. Программные средства защиты информации [Электронный ресурс] : электронный учебно-методический комплекс / Т. А. Гультяева, Н. Л. Долозов, С. А. Курлаев ; Новосиб. гос. техн. ун-т.- Новосибирск, [2017].- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234876.- Загл. с экрана. | | | | |
| 3 | Подготовка к аттестации | ОПК-1.1 | 6 | 0 |
| : Основы теории информации и криптографии : методические указания к выполнению лабораторных работ для 3 курса образовательной программы 02.03.03 - Математическое обеспечение и администрирование информационных систем, профиль - Математическое и программное обеспечение информационных технологий факультета прикладной математики и информатики / Новосиб. гос. техн. ун-т ; [сост.: Т. А. Гультяева, С. А. Курлаев ].- Новосибирск: Изд-во НГТУ, 2017.- 68, [1] с. : ил., табл.- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235026 | | | | |
| 4 | Самостоятельное изучение теоретического материала | ОПК-1.1,ОПК-1.2,ПК-1/НА.2, ПК-2/НА.1,ПК-2/НА.3,ПК-2/НА.4 | 66 | 0 |
| Студент изучает темы, приведенные в таблице 3.1 : Дудкина М. П. Организация самостоятельной работы студентов Новосибирского государственного технического университета : учебно-методическое пособие / М. П. Дудкина, Ю. В. Никитин ; Новосиб. гос. техн. ун-т.- Новосибирск: Изд-во НГТУ, 2022.- 61, [1] с. : табл.- Текст : непосредственный.- Режим доступа: http://elibrary.nstu.ru/source?bib_id=223022 | | | | |

### 3.3 Технология обучения

Для организации и контроля самостоятельной работы обучающихся, а также проведения консультаций применяются информационно-коммуникационные технологии (табл. 3.4).

Таблица 3.4

| Деятельность | Информационно-коммуникационные технологии |
|---|---|
| Информирование | Портал НГТУ |
| Консультирование | e-mail |
| Контроль | Портал НГТУ |
| Размещение учебных материалов | ЭБС |

Таблица 3.5

Активные и интерактивные формы проведения занятий

| № | Наименование активных форм |
|---|---|
| 1 | Дискуссия |
| **Краткое описание применения:** Рассмотрение, анализ различных позиций, точек зрения ученых на содержание той или иной проблемы, концепции выбора путей практической реализации теоретических знаний. | |

| | |
|---|---|
| 2 | Лекция в форме дискуссии |
| **Краткое описание применения:** Одновременно лекция-дискуссия имеет своей целью обучение методике анализа важнейших проблем, ведение научных дискуссий, применение и умелое использование необходимых аргументов для защиты своих позиций или критики точек зрения оппонентов. | |

## 4. Правила аттестации обучающихся по дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставлять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 4.1.

Таблица 4.1

| Оцениваемые виды деятельности обучающихся | Мин. балл | Максимальный балл |
|---|---|---|
| **Семестр: 3** | | |
| *Практические занятия:* | 10 | 20 |
| *Контрольные работы:* | 20 | 40 |
| *Зачет:* | 20 | 40 |

В таблице 4.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 4.2

| Коды компетенций | Индикаторы достижения компетенций | Формы контроля | |
|---|---|---|---|
| | | Контр. раб. | Зачет |
| **ОПК-1** | ОПК-1 1. Представляет современную научную картину мира, выявляет естественнонаучную сущность проблемы | + | + |
| | ОПК-1 2. Формулирует задачи, определяет пути их решения и оценивает эффективность выбора | | + |
| **ПК-1/НА** | ПК-1/НА 2. Проводит поиск и анализ научно-технической информации, отечественного и зарубежного опыта по разработке оптических и оптико-электронных приборов и комплексов | | + |
| **ПК-2/НА** | ПК-2/НА 1. Формулирует постановку задачи и определяет набор параметров, с учётом которых должно быть проведено моделирование процессов, явлений и особенностей работы изделий оптотехники | | + |
| | ПК-2/НА 3. Разрабатывает математические модели функционирования оптико-электронных приборов на основе физических процессов и явлений | | + |

| | | | |
|---|---|---|---|
| | ПК-2/НА 4. Проводит компьютерное моделирование функционирования оптико-электронных приборов на основе физических процессов и явлений | + | + |
| **УК-4** | УК-4 2. Представляет результаты академической и профессиональной деятельности на различных научных мероприятиях, включая международные | | + |

Фонд оценочных средств по дисциплине представлен в приложении № 1 к рабочей программе.

## 5. Литература

*Основная литература*

**1.** Котов Ю. А. Криптографические методы защиты информации. Шифры : учебное пособие / Ю. А. Котов ; Новосиб. гос. техн. ун-т.- Новосибирск: Изд-во НГТУ, 2016.- 57, [1] с.- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000232326

**2.** Гультяева Т. А. Основы защиты информации : [учебное пособие] / Т. А. Гультяева ; Новосиб. гос. техн. ун-т.- Новосибирск: Изд-во НГТУ, 2018.- 81, [1] с.- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000238835

*Дополнительная литература*

**1.** Гринберг Я. С. Элементарное введение в основы квантовой информатики (физические аспекты) : [учебное пособие] / Я. С. Гринберг ; Новосиб. гос. техн. ун-т. - Новосибирск, 2006. - 59 с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000060485

**2.** Ильичев Е. В. Квантовая информатика и квантовые биты на основе сверхпроводниковых джозефсоновских структур : [учебник] / Е. В. Ильичев, Я. С. Гринберг.- Новосибирск: Изд-во НГТУ, 2013.- 170, [1] с. : ил., табл.- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000182651

**3.** Физика [Электронный ресурс]. Т. I : 32 книги в PDF-формате. - Ижевск, 2005. - 1 электрон. опт. диск (CD-ROM). - Загл. с контейнера.

**4.** Квантовая информатика и квантовые биты на основе сверхпроводниковых джозефсоновских структур: Учебник / Е.В. Ильичев, Я.С. Гринберг. - Новосибирск: НГТУ, 2013. - 172 с.: 70x100 1/16. (переплет) ISBN 978-5-7782-2287-8, 3000 экз. - Режим доступа: http://znanium.com/catalog.php?bookinfo=490017 - Загл. с экрана.

*Интернет-ресурсы*

**1.** Квантовая криптография. Лекция 27. – Изображение : видео : электронное / Е. О. Киктенко, Д. А. Кронберг, Ю. В. Курочкин [и др.] // Математический институт им. В. А. Стеклова РАН. – 2023. – URL: https://www.mathnet.ru/php/seminars.phtml?option_lang=rus&presentid=17555 (дата обращения: 16.06.2023)

## 6. Методическое и программное обеспечение, информационные технологии

*6.1 Методическое обеспечение*

**1.** Основы теории информации и криптографии : методические указания к выполнению лабораторных работ для 3 курса образовательной программы 02.03.03 - Математическое обеспечение и администрирование информационных систем, профиль - Математическое и программное обеспечение информационных технологий факультета прикладной математики и информатики / Новосиб. гос. техн. ун-т ; [сост.: Т. А. Гультяева, С. А. Курлаев ].- Новосибирск: Изд-во НГТУ, 2017.- 68, [1] с. : ил., табл.- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235026

**2.** Дудкина М. П. Организация самостоятельной работы студентов Новосибирского государственного технического университета : учебно-методическое пособие / М. П. Дудкина, Ю. В. Никитин ; Новосиб. гос. техн. ун-т.- Новосибирск: Изд-во НГТУ, 2022.- 61, [1] с. : табл.- Текст : непосредственный.- Режим доступа: http://elibrary.nstu.ru/source?bib_id=223022

**3.** Гультяева Т. А. Программные средства защиты информации [Электронный ресурс] : электронный учебно-методический комплекс / Т. А. Гультяева, Н. Л. Долозов, С. А. Курлаев ; Новосиб. гос. техн. ун-т.- Новосибирск, [2017].- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234876.- Загл. с экрана.

*6.2 Специализированное программное обеспечение*

**1** Операционная система Microsoft Windows

**2** Пакет офисных приложений Microsoft Office

*6.3 Информационные технологии*

При осуществлении образовательного процесса по дисциплине применяются элементы дистанционных образовательных технологий, а также синхронного и асинхронного взаимодействия в электронной информационно-образовательной среды НГТУ.

## 7. Материально-техническое обеспечение

Презентационное оборудование

| № | Наименование | Назначение |
|---|---|---|
| 1 | Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления) | для демонстрации лекционного материала |