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

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н. Томилов И. Н.

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Математическое прикладное программное обеспечение для задач защиты информации

Образовательная программа: 10.04.01 Информационная безопасность, магистерская программа: Методы и средства обеспечения технической защиты информации

Курс: 1, семестр : 2

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**2**
1	Всего зачетных единиц (кредитов)	3
2	Всего часов	108
3	Всего занятий в контактной форме, час.	64
4	Лекции, час.	36
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	18
7	из них в активной и интерактивной форме, час.	0
8	из них практической подготовки, час.	2
9	Аттестация, час.	2
10	Консультации, час.	8
11	Самостоятельная работа, час.	44
12	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ(Р)/реферат, подготовка к контрольной работе)	
13	Вид аттестации	3

Новосибирск 2026

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 10.04.01 Информационная безопасность

ФГОС введен в действие приказом №1455 от 26.11.2020 г. , дата утверждения: 18.02.2021 г.

Место дисциплины в структуре учебного плана: Блок 1, обязательная

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 10.04.01 Информационная безопасность

Рабочая программа обсуждена на заседании кафедры

ЗИ, 31.08.2026

Утверждена на совете факультета автоматики и вычислительной техники, протокол № 8 от 31.08.2026

Заведующий кафедрой:

доцент, к.т.н. Иванов А. В.

Ответственный за образовательную программу:

заведующий кафедрой Иванов А. В.

1. Внешние требования

Таблица 1.1

Группа	Компетенции
	Индикаторы достижения компетенций
Общепрофессиональные компетенции	ОПК-5 Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи
	ОПК-5. 1 знает современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы для решения профессиональных задач
	ОПК-5. 3 умеет применять методы научных исследований в научной деятельности, в частности, при написании магистерской диссертации и научных статей
	ОПК-5. 4 знает теоретические и эмпирические методы научных исследований

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

Таблица 2.1

Индикаторы достижения компетенций	Формы организации занятий
Результаты обучения	
ОПК-5. 1 знает современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы для решения профессиональных задач	
Применяет современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы для решения профессиональных задач	Лекции; Лабораторные работы; Самостоятельная работа
Понимает процедуры критического анализа, методики анализа результатов исследования и разработки стратегий проведения исследований, организации процесса принятия решения	Лекции; Лабораторные работы; Самостоятельная работа
ОПК-5. 3 умеет применять методы научных исследований в научной деятельности, в частности, при написании магистерской диссертации и научных статей	
Применяет современное программное обеспечение в ходе работы над научными статьями и над диссертацией	Лекции; Лабораторные работы;
ОПК-5. 4 знает теоретические и эмпирические методы научных исследований	
Готов практически применять теоретические и эмпирические методы научных исследований	Лекции; Лабораторные работы;

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: 2					
Дидактическая единица: Криптографические хэш-функции					
1. Стойкие хэш-функции	4	0	0	ОПК-5.1,ОПК-5.4	Практическое применение стойких хэш-функций
Дидактическая единица: Криптографический анализ					
2. Симметричные криптосистемы	8	0	0	ОПК-5.1,ОПК-5.4	Анализ симметричных криптосистем

3. Криптографические системы с открытым ключом	8	0	0	ОПК-5.1,ОПК-5.3,ОПК-5.4	Анализ криптографических систем с открытым ключом
Дидактическая единица: Управление непрерывностью бизнеса и киберустойчивостью					
4. Проблематика киберустойчивости с учетом требований бизнес-процессов с ростом масштабирования систем	12	0	0	ОПК-5.1,ОПК-5.4	Сравнительный анализ методологий кибербезопасности
Дидактическая единица: Технологии кибербезопасности будущего					
5. Современные тренды в рамках задач защиты информации	4	0	0	ОПК-5.1,ОПК-5.3,ОПК-5.4	Современные тренды в рамках задач защиты информации

Темы лабораторных работ	Часы	Из них в форме практ. подг., час.	Активные формы, час.	Индикаторы достижения компетенций	Учебная деятельность
Семестр: 2					
Дидактическая единица: Криптографические хэш-функции					
1. Практическое применение стойких хэш-функций	6	2	0	ОПК-5.1,ОПК-5.3,ОПК-5.4	Практическое применение стойких хэш-функций
Дидактическая единица: Криптографический анализ					
2. Анализ симметричных криптосистем	6	0	0	ОПК-5.1,ОПК-5.4	Анализ симметричных криптосистем
3. Анализ криптографических систем с открытым ключом	6	0	0	ОПК-5.1,ОПК-5.3,ОПК-5.4	Анализ криптографических систем с открытым ключом

3.1 Практическая подготовка

Таблица 3.2

№	Темы занятий	Формы организации занятий	Содержание практической подготовки (виды работ)
1	Практическое применение стойких хэш-функций	Лб	Выполняет следующие виды работ: реализация программного алгоритма, выполняющего хэширование для нахождения контрольной суммы файла, передаваемого по сети

3.2 Самостоятельная работа обучающегося

Таблица 3.3

№	Виды самостоятельной работы	Индикаторы достижения компетенций	Часы на выполнение	Часы на консультации
Семестр: 2				
1	Подготовка к занятиям	ОПК-5.1	44	8

: Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). - Текст : электронный. - URL: https://znanium.com/catalog/product/1232287 (дата обращения: 24.09.2021). – Режим доступа: по подписке. Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие / А. В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 413 с. — (Высшее образование: Бакалавриат). - Текст : электронный. - URL: https://znanium.com/catalog/product/1215714 (дата обращения: 24.09.2021). – Режим доступа: по подписке.

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	e-mail; Среда электронного обучения НГТУ
Консультирование	e-mail; Среда электронного обучения НГТУ
Контроль	Среда электронного обучения НГТУ
Размещение учебных материалов	Среда электронного обучения НГТУ

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: 2		
Лабораторная:	40	80
Зачет:	10	20

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

Таблица 4.2

Коды компетенций	Индикаторы достижения компетенций	Формы контроля	
			Зачет
ОПК-5	ОПК-5 1. знает современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы для решения профессиональных задач		+
	ОПК-5 3. умеет применять методы научных исследований в научной деятельности, в частности, при написании магистерской диссертации и научных статей		+
	ОПК-5 4. знает теоретические и эмпирические методы научных исследований		+

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

5. Литература

Основная литература

1. Аппаратные и программные средства защиты информации: Учебное пособие / Душкин А.В., Кольцов А., Кравченко А. - Воронеж:Научная книга, 2016. - 232 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/923168 (дата обращения: 24.09.2021). – Режим доступа: по подписке.

2. Арзуманян, А. Б. Международные стандарты правовой защиты информации и информационных технологий : учебное пособие / А. Б. Арзуманян ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2020. - 140 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1308349 (дата обращения: 24.09.2021). – Режим доступа: по подписке.

3. Аппаратно-программные средства защиты информации: Практикум / Душкин А.В., Дубровин А.С., Здольник В.В. - Воронеж:Научная книга, 2017. - 198 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/977192 (дата обращения: 24.09.2021). – Режим доступа: по подписке.

Дополнительная литература

1. Поддержка принятия решений при проектировании систем защиты информации : монография / В.В. Бухтояров, М.Н. Жукова, В.В. Золотарев [и др.]. — Москва : ИНФРА-М, 2020. — 131 с. — (Научная мысль). - Текст : электронный. - URL: https://znanium.com/catalog/product/1036519 (дата обращения: 24.09.2021). – Режим доступа: по подписке.

Интернет-ресурсы

1. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Саратов : Профобразование, 2017.— 702 с. — Режим доступа : http://www.iprbookshop.ru/63594.html. — Загл. с экрана.

6. Методическое и программное обеспечение, информационные технологии

6.1 Методическое обеспечение

1. Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие / А. В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 413 с. — (Высшее образование: Бакалавриат). - Текст : электронный. - URL: https://znanium.com/catalog/product/1215714 (дата обращения: 24.09.2021). – Режим доступа: по подписке.

2. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). - Текст : электронный. - URL: https://znanium.com/catalog/product/1232287 (дата обращения: 24.09.2021). – Режим доступа: по подписке.

6.2 Специализированное программное обеспечение

1 Среда математических и научных расчетов MathWorks MATLAB Online

2 Создание отчётов для лабораторных работ. Microsoft 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

Компьютерный класс

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Для демонстрации материалов лекций
2	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Для проведния лабораторных работ