МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ
Директор института прикладной
математики и компьютерных наук
_____А.В. Замятин
«_02_» _____июня_____ 2021 г.

Методы и средства криптографической защиты информации

рабочая программа дисциплины

Закреплена за кафедрой	*компьютерной безопасности*
Учебный план	*10.05.01 Компьютерная безопасность,* *профиль «Анализ безопасности компьютерных систем»*
Форма обучения	*очная*
Общая трудоёмкость	*9 з.е.*
Часов по учебному плану	*324*
в том числе:	
аудиторная контактная работа	*143*
самостоятельная работа	*181*
Вид(ы) контроля в семестрах *экзамен/зачет/зачет с оценкой*	*Семестр 7 – экзамен* *Семестр 8 –экзамен*

Томск-2021

Программу составил:
канд. техн. наук,
доцент кафедры компьютерной безопасности  В.Н. Тренькаев

Рецензент:
канд. техн. наук,
заведующий кафедрой компьютерной безопасности  С.А.Останин

Рабочая программа дисциплины «Методы и средства криптографической защиты информации» разработана в соответствии с образовательным стандартом высшего образования – специалитет, самостоятельно устанавливаемым федеральным государственным автономным образовательным учреждением высшего образования «Национальный исследовательский Томский государственный университет» по специальности 10.05.01 Компьютерная безопасность (Утвержден Ученым советом НИ ТГУ, протокол от 30.06.2021 г. № 06).

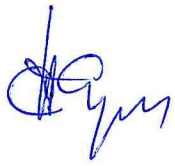
Рабочая программа одобрена на заседании кафедры компьютерной безопасности

Протокол от 02 июня 2021 г. № 06

Заведующий кафедрой компьютерной безопасности,
канд. техн. наук, доцент  С.А. Останин

Рабочая программа одобрена на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 17 июня 2021 г. № 05

Председатель УМК ИПМКН,
д-р техн. наук, профессор  С.П. Сущенко

Цель освоения дисциплины

Цель – сформировать у студентов способность анализировать тенденции развития методов и средств криптографической защиты информации, в частности дать представление о базовых понятиях и задачах криптографии, методах криптографического анализа, ознакомить с современными стандартами в области криптографии.

1. Место дисциплины в структуре ОПОП

Дисциплина «Методы и средства криптографической защиты информации» относится к обязательной части Блока 1 «Дисциплины», входит в модуль «Специализация».

Для освоения дисциплины необходимо знать основы информатики и программирования, компьютерных сетей, общей алгебры, теории вероятностей и математической статистики, теории чисел, дискретной математики.

Пререквизиты дисциплины: Языки программирования, Информатика , Введение в математику, Дискретная математика, Теория вероятностей и математическая статистика, Математическая логика и теория алгоритмов , Дискретная математика. Теория автоматов, Теория информации, Теория чисел, Общая алгебра, Теория вычислительной сложности, Профессиональный перевод специальной литературы.

Постреквизиты дисциплины: Основы построения защищённых компьютерных сетей, Основы построения защищённых баз данных, Теоретико-числовые методы в криптографии, Аппаратная реализация криптоалгоритмов, Булевы функции в криптографии, Криптографические протоколы.

2. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Таблица 1.

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций)
ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.	ИОПК-2.2 Определяет порядок настройки и эксплуатации программных средств системного и прикладного назначений, в том числе отечественного производства, используемых для решения задач профессиональной деятельности; ИОПК-2.3 Формулирует предложения по применению программных средств системного и прикладного назначений, в том числе отечественного производства, используемых для решения задач профессиональной деятельности.	ОР-2.2.1 **Уметь**: формулировать предложения по применению программных средств, реализующих криптографические алгоритмы
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при	ИОПК-10.1 Осуществляет анализ тенденций развития методов и средств криптографической защиты информации; ИОПК-10.2 Применяет средства криптографической защиты информации при решении задач профессиональной деятельности.	ОР-10.1.1 **Знать**: типовые криптографические алгоритмы, используемые в компьютерных системах и сетях

решении задач профессиональной деятельности.		
ОПК-13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.	ИОПК-13.1 Предпринимает необходимые действия по сбору и анализу исходных данных для проектирования компонент программных и программно-аппаратных средств защиты информации в компьютерных системах; ИОПК-13.2 Определяет параметры функционирования, архитектуру и интерфейсы компонент программных и программно-аппаратных средств защиты информации в компьютерных системах; ИОПК-13.3 Проводит анализ компонент программных и программно-аппаратных средств защиты информации в компьютерных системах с целью определения уровня обеспечиваемой ими защищенности и доверия.	ОР-13.1.1 **Уметь**: разрабатывать компоненты программных средств защиты информации, реализующих криптографические алгоритмы
ПК-2 Способен разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей	ИПК-2.1 Определяет угрозы безопасности и их возможные источники, каналы утечки информации ИПК-2.2 Разрабатывает математические модели, реализуемые в средствах защиты информации ИПК-2.3 Проводит исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации	ОР-2.1.1 З**нать**: математические методы исследования криптографических алгоритмов.
ПК-3 Способен проектировать программно-аппаратные средств защиты информации компьютерных систем и сетей	ИПК-3.2 Разработка проектов программных и аппаратных средств защиты информации в соответствии с техническим заданием	ОР-3.2.1 **Уметь:** корректно использовать криптографические алгоритмы при решении задач защиты информации

3. Структура и содержание дисциплины

3.1. Структура и трудоемкость видов учебной работы по дисциплине

Общая трудоемкость дисциплины составляет 9 зачетных единиц, 324 часа.

Таблица 2.

Вид учебной работы	Трудоемкость в академических часах		
	7 семестр	8 семестр	всего
Общая трудоемкость	144	180	324
Контактная работа:	71,5	71,5	143
Лекции (Л):	32	32	64
Практики (ПЗ)	32	16	48
Лабораторные работы (ЛР)		16	16
Семинары (СЗ)			
Групповые консультации	2	2	4
Индивидуальные консультации	3,2	3,2	6,4
Промежуточная аттестация	2,3	2,3	4,6
Самостоятельная работа обучающегося:	40,8	76,8	117,6
- выполнение контрольных заданий	20	20	40
- изучение учебного материала, публикаций	10	20	30
- подготовка к лабораторным/практическим занятиям	10,8	36,8	47,6
- подготовка к рубежному контролю по теме/разделу	31,7	31,7	63,4
Вид промежуточной аттестации (зачет, зачет с оценкой, экзамен)	**Экзамен**	**Экзамен**	**экзамен, экзамен**

3.2. Содержание и трудоемкость разделов дисциплины

Таблица 3.

Код занятия	Наименование разделов и тем и их содержание	Вид учебной работы, занятий, контроля	Семестр	Часы в электронной форме	Всего (час.)	Литература	Код (ы) результата(ов) обучения
	Раздел 1. Введение в криптографию		7		**8**	1-6	ОР-10.1.1, ОР-2.1.1
1.1.	Основные понятия и задачи криптографии.	Лекция	7		2		
1.2.	Криптографический анализ.	Лекция	7		2		
1.3.	История криптографии.	СРС	7		4,8		
	Раздел 2. Шифры замены и перестановки		7		**14**	1-6	ОР-10.1.1, ОР-2.1.1
2.1.	Шифры замены. Криптоанализ шифров замены.	Лекция	7		2		
2.2.	Шифры перестановки. Криптоанализ шифров перестановки.	Лекция	7		2		
2.3.	Шифры замены и перестановки.	Практики	7		4		
2.4.	Роторные шифры.	СРС	7		6		
	Раздел 3. Абсолютно стойкие шифры		7		**8**	6	ОР-2.1.1
3.1.	Вероятностная модель шифра по К.Шеннону.	Лекция	7		2		
3.2.	Необходимые и достаточные условия абсолютной стойкости шифра.	Лекция	7		2		
3.3.	Атака на основе шифртекста.	Практики	7		4		
	Раздел 4. Блочные шифры		7		**16**		ОР-10.1.1, ОР-2.1.1 ОР-3.2.1
4.1.	Принципы построения. Базовые операции. Сеть Фейстеля. SP-сеть.	Лекция	7		2	1-6,11,12	
4.2.	Шифр DES. Шифр ГОСТ 28147-89 («Магма»). Шифр AES.	Лекция	7		2		
4.3.	Упрощенные шифры DES и AES.	Практики	7		6		
4.4.	Шифр «Кузнечик».	СРС	7		6		
	Раздел 5. Поточные шифры		7		**14**		ОР-10.1.1, ОР-2.1.1, ОР-3.2.1
5.1.	Схема поточного шифра. Генераторы псевдослучайных чисел.	Лекция	7		2	1-6,11,12	
5.2.	Комбинирующий и фильтрующий генераторы. Шифр A5. Шифр RC4.	Лекция	7		2		
5.3.	Примеры генераторов псевдослучайных чисел. Упрощенные шифры A5 и RC4.	Практики	7		4		
5.4.	Генераторы псевдослучайных чисел.	СРС	7		6		
	Раздел 6. Ассиметричные шифры		7		**14**		ОР-10.1.1, ОР-2.1.1, ОР-3.2.1
6.1.	Односторонняя функция с лазейкой. Шифр RSA.	Лекция	7		2	1-6,11,12	

6.1.	Шифр Эль-Гамаля. Свойства шифра Эль-Гамаля.	Лекция	7		2		
6.3.	Алгоритмы ассиметричного шифрования.	Практики	7		4		
6.4.	Атаки на RSA.	СРС			6		
	Раздел 7. Цифровая подпись		7		**14**		ОР-10.1.1, ОР-2.1.1, ОР-3.2.1
7.1.	Цифровая подпись RSA, Эль-Гамаля, Фиата-Шамира.	Лекция	7		2	1-6,11,12	
7.2.	Инфраструктура открытых ключей.	Лекция	7		2		
7.3.	Цифровая подпись RSA и Эль-Гамаля.	Практики	7		4		
7.4.	Атаки на цифровые подписи.	СРС	7		6		
	Раздел 8. Криптографические функции хеширования.		7		**16**		ОР-10.1.1, ОР-2.1.1, ОР-3.2.1
8.1.	Имитовставка. Бесключевые и ключевые хэш-функции.	Лекция	7		2	1-6,11,12	
8.2.	Конструкция Меркла-Дамгарда. Конструкция Губка. Стрибог. SHA.	Лекция	7		2		
8.3.	HMAC. Упрощенная хэш-функция MD4.	Практики	7		6		
8.4.	Атаки на хэш-функции.	СРС	7		6		
	Подготовка к промежуточной аттестации в форме экзамена	СРС	7		**31,7**		
	Прохождение промежуточной аттестации в форме экзамена	Э	7		**4,3**		
	Раздел 9. Теория секретных систем Шеннона.		8		**32**	9	ОР-2.1.1
9.1.	Алгебра секретных систем. Виды секретных систем.	Лекции	8		8		
9.2.	Примеры секретных систем. Свойства секретных систем.	Практики	8		8		
9.3.	Теория имитостойкости Симмонса.	СРС	8		16		
	Раздел 10. Методы криптоанализа.		8		**34**	7,9,10	ОР-2.1.1, ОР-13.1.1, ОР-3.2.1
10.1.	Обзор методов криптоанализа.	Лекции	8		8		
10.2.	Линейный криптоанализ. Дифференциальный криптоанализ.	ЛР	8		8		
10.3.	Атаки по побочным каналам.	СРС	8		18		
	Раздел 11. Автоматная криптография.		8		**32**	8	ОР-2.1.1
11.1.	Автоматы как компоненты криптосистем. Автоматные шифрсистемы.	Лекции	8		8		
11.2.	Конечно-автоматная криптосистема с открытым ключом (FAPKC).	Практики	8		8		
11.3.	Поточные и автоматные шифрсистемы.	СРС	8		16		
	Раздел 12. Средства криптографической защиты информации.		8		**38**	1-5	ОР-2.2.1, ОР-3.2.1
12.1.	Обзор средств криптографической защиты информации.	Лекции	8		8		
12.2.	Криптоконтейнеры. Криптопровайдеры. VPN-шлюзы.	ЛР	8		8		
12.3.	Криптографические файловые системы.	СРС	8		26,8		
	Подготовка к промежуточной аттестации в форме экзамена	СРС	8		**31,7**	1-12	ОР-2.2.1, ОР-3.2.1,

							ОР-13.1.1, ОР-2.1.1, ОР-10.1.1
	Прохождение промежуточной аттестации в форме экзамена	Э	8		**4,3**		

4. Образовательные технологии, учебно-методическое и информационное обеспечение для освоения дисциплины

Образовательная технология – посещение студентом последовательности из набора лекций/практических занятий по разным темам дисциплины с последующим выполнением лабораторных работ и/или контрольных заданий по пройденным темам. Самостоятельная работа студентов включает подготовку к лабораторным/практическим занятиям, изучение учебного материала, подготовку к рубежному контролю по разделу. Учебно-методическое обеспечение включает: список основной и дополнительной учебной литературы, список информационные ресурсов в сети Интернет, слайды лекционных занятий, методические рекомендации по выполнению контрольных заданий и лабораторных работ. Промежуточная аттестация осуществляется в форме экзамена при условии выполнения студентом контрольных заданий и/или лабораторных работ. Экзамен подразумевает подготовку студента и ответы в устной или письменной форме на несколько контрольных вопросов по всему курсу.

Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций, и методические материалы, определяющие процедуры оценивания результатов обучения, приведены в Приложении 1 к рабочей программе «Фонд оценочных средств».

Типовые контрольные задания или иные материалы, необходимые для текущей аттестации, и методические материалы, определяющие процедуры оценивания результатов текущей аттестации, приведены в Приложении 2 к рабочей программе «Примерные оценочные средства текущей аттестации».

4.1. Рекомендуемая литература и учебно-методическое обеспечение

№ п/п	Авторы / составители	Заглавие	Издательство	Год издания, количество страниц
Основная литература				
1.	Запечников С.В., Казарин О.В., Тарасов А.А.	Криптографические методы защиты информации	М.: Юрайт	2016 г., 308 с.
2.	Лось А.Б.	Криптографические методы защиты информации	М.: Юрайт	2018 г., 473 с.
3.	Рябко Б.Я., Фионов А.Н.	Криптографические методы защиты информации	М.: Горячая Линия - Телеком	2014 г., 229 с.
4.	Фомичёв В.М., Мельников Д.А.	Криптографические методы защиты информации	М.: Юрайт	2017 г., 209 с.
5.	Бабаш А.В.	Криптографические методы защиты информации	М.: РИОР	2019 г., 413 с.
Дополнительная литература				
6.	Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.	Основы криптографии. Учебное пособие.	М.: Гелиос АРВ	2002 г., 480 с.
7.	Бабенко Л.К., Ищукова Е.А.	Современные алгоритмы блочного шифрования и методы их анализа.,	М.: Гелиос АРВ	2006 г., 376 с.
8.	Агибалов Г.П.	Конечные автоматы в криптографии	Прикладная дискретная математика	2009, Приложение № 2, С. 43–73

9.	Агибалов Г.П.	Избранные теоремы начального курса криптографии	Томск: НТЛ	2005 г., 116 с.
10.	Венбо Мао	Современная криптография: теория и практика	М.: Вильямс	2005 г., 768 с.
11.	Шнайер Брюс	Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си	М.: Триумф	2002 г., 816 с.
12.	Кузьминов Т.В.	Криптографические методы защиты информации	Новосибирск: Наука	1998 г., 194 с.

4.2. Базы данных и информационно-справочные системы, в том числе зарубежные

1. Курс "Основы криптографии" [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/691/547/info
2. Курс "Математика криптографии и теория шифрования» [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/552/408/info
3. Курс "Криптографические основы безопасности" [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/28/28/info

4.3. Перечень лицензионного и программного обеспечения

- ОС Windows/Linux
- Браузер Firefox/Яндекс
- КриптоПро CSP
- JaCarta SecurLogon

4.4. Оборудование и технические средства обучения

Для реализации дисциплины необходимы лекционные аудитории и аудитории для проведения лабораторных работ/практических занятий. Специальные технические средства (проектор, компьютер и т.д.) требуются для демонстрации материала в рамках изучаемых разделов, проведения практических занятий. Вся основная и дополнительная литература, необходимая для самостоятельной работы и подготовки к экзамену, имеется в научной библиотеке ТГУ.

5. Методические указания обучающимся по освоению дисциплины

-целенаправленно, систематически и планомерно работать со слайдами лекций;
-изучать рекомендуемую литературу, добывая новые/обобщая полученные знания;
-тратить не менее часа в день на самостоятельную работу;
-консультироваться с преподавателем при возникновении вопросов;
-активно использовать учебно-методический комплекс на базе Moodle ТГУ;
-работать с тематическими форумами в сети Интернет.

6. Преподавательский состав, реализующий дисциплину

Тренькаев Вадим Николаевич, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности

7. Язык преподавания – русский язык.