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_» _____ 2021 г.

Криптографические протоколы

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	*4 з.е.*
Часов по учебному плану	*144*
в том числе:	
аудиторная контактная работа	*71,5*
самостоятельная работа	*72,5*
Вид(ы) контроля в семестрах *экзамен/зачет/зачет с оценкой*	*Семестр 9 – 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 «Криптографические протоколы» 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 ознакомить с различными видами современных криптографических протоколов, стандартами в области криптографических протоколов.

1. Место дисциплины в структуре ОПОП

Дисциплина «Криптографические протоколы» 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, теории чисел, дискретной математики, криптографии.

Пререквизиты дисциплины: Языки программирования, Компьютерные сети, Теория вероятностей и математическая статистика, Дискретная математика, Теория графов, Теория чисел, Общая алгебра, Профессиональный перевод специальной литературы, Методы и средства криптографической защиты информации, Основы построения защищённых компьютерных сетей.

Постреквизиты дисциплины: Защита в операционных системах, Безопасность веб-приложений, Квантовые вычисления, Производственная практика, Преддипломная практика.

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 протоколы
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной	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 протоколы, используемые в компьютерных сетях

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 протоколы
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 **Знать**: типовые атаки на криптографические протоколы
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 **Знать**: основные типы криптографических протоколов и принципы их построения с использованием шифрсистем

3. Структура и содержание дисциплины

3.1. Структура и трудоемкость видов учебной работы по дисциплине

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

Таблица 2.

Вид учебной работы	Трудоемкость в академических часах	
	9 семестр	всего
Общая трудоемкость	144	144
Контактная работа:	71,5	71,5

Лекции (Л):	32	32
Практики (ПЗ)		
Лабораторные работы (ЛР)	32	32
Семинары (СЗ)		
Групповые консультации	2	2
Индивидуальные консультации	3,2	3,2
Промежуточная аттестация	2,3	2,3
Самостоятельная работа обучающегося:	40,8	40,8
- подготовка к лабораторным занятиям	30	30
- изучение учебного материала, публикаций	10,8	10,8
- подготовка к рубежному контролю по теме/разделу	31,7	31,7
Вид промежуточной аттестации (зачет, зачет с оценкой, 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 криптографические протоколы		9		**6**	1-3	ОР-10.1.1, ОР-2.1.1
1.1.	Основные понятия. Классификация криптографических протоколов.	Лекция	9		2		
1.2.	Атаки на криптографические протоколы.	Лекция	9		2		
1.3	Свойства, характеризующие безопасность протоколов.	СРС	9		2		
	Раздел 2. Протоколы аутентификации сообщений		9		**6**	1-3	ОР-3.2.1, ОР-2.1.1
2.1.	Схема имитозащиты. Оптимальные коды аутентификации.	Лекция	9		4		
2.2.	Атаки на протоколы аутентификации сообщений.	СРС	9		2		
	Раздел 3. Протоколы идентификации		9		**26**	1-3,4,5	ОР-3.2.1, ОР-2.1.1, ОР-2.2.1, ОР-13.1.1
3.1.	Парольные схемы идентификации.	Лекция	9		2		
3.2.	Протоколы идентификации на основе техники “запрос-ответ”.	Лекция	9		2		
3.3.	Протоколы идентификации на основе техники доказательства знания.	Лекция	9		2		
3.4.	Протоколы с нулевым разглашением.	Лекция	9		2		
3.5.	Схема Лэмпорта (S/KEY)	ЛР	9		4		
3.6.	Протокол CHAP/MS-CHAP	ЛР	9		6		
3.7.	Атаки на протоколы идентификации.	СРС	9		8		
	Раздел 4. Протоколы распределения ключей		9		**28**	1-3,4,6,9	ОР-3.2.1, ОР-2.1.1, ОР-2.2.1, ОР-13.1.1
4.1.	Протоколы передачи ключей	Лекция	9		4		
4.2.	Протоколы открытого распределения ключей	Лекция	9		2		
4.3.	Протоколы предварительного распределения ключей	Лекция	9		2		
4.4.	Протокол Диффи – Хеллмана.	ЛР	9		6		
4.5.	Протокола Oakley.	ЛР	9		4		
4.6.	Атаки на протоколы распределения ключей.	СРС	9		10		
	Раздел 5. Групповые криптографические протоколы.		9		**10**	1-3,4,7	ОР-3.2.1, ОР-2.1.1, ОР-2.2.1, ОР-13.1.1
5.1.	Схемы разделение секрета.	Лекция	9		4		
5.2.	Схемы цифровой подписи.	ЛР	9		6		

5.3.	Атаки на **г**рупповые криптографические протоколы.	СРС	9		8		
	Раздел 6. Прикладные криптографические протоколы.		9		**18**	1-3,4,8	ОР-3.2.1, ОР-2.1.1, ОР-2.2.1, ОР-13.1.1
6.1.	Семейство протоколов IPsec..	Лекция	9		2		
6.2.	Протокол SSL/TLS.	Лекция	9		2		
6.3.	VPN-протоколы.	ЛР	9		6		
6.4.	Атаки на прикладные криптографические протоколы	СРС	9		8		
	Подготовка к промежуточной аттестации в форме экзамена	СРС	9		**31,7**	1-9	ОР-10.1.1, ОР-3.2.1, ОР-2.1.1, ОР-2.2.1, ОР-13.1.1
	Прохождение промежуточной аттестации в форме экзамена	Э	9		**4,3**		

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

Образовательная технология – посещение студентом последовательности из набора лекций по разным темам дисциплины с последующим выполнением лабораторных работ по пройденным темам. Самостоятельная работа студентов включает подготовку к лабораторным 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 лабораторных работ. Промежуточная аттестация осуществляется в форме экзамена при условии выполнения студентом 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.	Рябко Б.Я., Фионов А.Н.	Криптографические методы защиты информации	М.: Горячая Линия - Телеком	2014 г., 229 с.
3.	Фомичёв В.М., Мельников Д.А.	Криптографические методы защиты информации	М.: Юрайт	2017 г., 209 с.
Дополнительная литература				
4.	Черемушкин А.В.	Криптографические протоколы. Основные свойства и уязвимости	М.: Академия	2009 г., 271 с.
5.	Агибалов Г.П.	Избранные теоремы начального курса криптографии	Томск: НТЛ	2005 г., 116 с.
6.	Венбо Мао	Современная криптография: теория и практика	М.: Вильямс	2005 г., 768 с.
7.	Шнайер Брюс	Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си	М.: Триумф	2002 г., 816 с.
8.	Смарт Н.	Криптография	М.: Техносфера	2005 г., 528 с.
9.	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. Агибалов Г. П. Избранные теоремы начального курса криптографии : учебно-методический комплекс / Агибалов Г. П. - Томск : ИДО ТГУ, 2007. URL: http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000243893

2. Курс Управление ключами шифрования и безопасность сети [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/553/409/info

3. Николенко С. Курс Криптографические протоколы [Электронный ресурс] // Лекториум - академический образовательный проект . URL: https://www.lektorium.tv/course/26036

4.3. Перечень лицензионного и программного обеспечения

- ОС Windows/Linux
- Браузер Firefox/Яндекс

4.4. Оборудование и технические средства обучения

Для реализации дисциплины необходимы лекционные аудитории и аудитории для проведения лабораторных работ. Специальные технические средства (проектор, компьютер и т.д.) требуются для демонстрации материала в рамках изучаемых разделов, проведения лабораторных работ. 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.