Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Радиофизический факультет

УТВЕРЖДЕНО:
Декан
А. Г. Коротаев

Рабочая программа дисциплины

Защита информации

по направлению подготовки / специальности

11.05.01 Радиоэлектронные системы и комплексы

Направленность (профиль) подготовки / специализация:
радиоэлектронные системы передачи информации
Форма обучения
Очная

Квалификация
Инженер

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
В.А. Мещеряков

Председатель УМК
А.П. Коханенко

Томск – 2025

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-7 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности;

ОПК-8 Способен использовать современные программные и инструментальные средства компьютерного моделирования для решения различных исследовательских и профессиональных задач;

ОПК-9 Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения;

ПК-2 Способен проводить научно-исследовательские и опытно-конструкторские разработки функциональных приборов и устройств радиоэлектроники.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК 7.1 Использует современные информационно-коммуникационные технологии для обработки, анализа и представления в требуемом формате информации;

ИОПК 7.2 Решает информационно-коммуникационные задачи с помощью современных систем автоматизации;

ИОПК 8.1 Использует современные информационные технологии и программное обеспечение при решении задач профессиональной деятельности;

ИОПК 8.2 Использует компьютерные системы поиска, хранения, обработки, анализа и представления информации;

ИОПК 8.3 Соблюдает требования информационной безопасности при использовании современных информационных технологий и программного обеспечения;

ИОПК 9.1 Применяет современные инструментальные системы программирования и компьютерного моделирования при решении прикладных задач;

ИОПК 9.2 Владеет навыками работы в компьютерной среде;

ИПК 2.2 Использует современные пакеты прикладных программ для разработки структурных, функциональных и принципиальных схем радиоэлектронных устройств комплексов передачи информации.

2. Задачи освоения дисциплины

– Научить студентов соблюдать требования информационной безопасности при использовании современных информационных технологий и программного обеспечения.

– Оценивать безопасность используемого программного обеспечения.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к Блоку 1 «Дисциплина (модули)».

Дисциплина относится к обязательной части образовательной программы.

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Пятый семестр, зачет с оценкой

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: математический анализ, линейная алгебра, основы информатики.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:
-лекции: 24 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Введение
Уровни обеспечения информационной безопасности. Характеристика основных методов и средств защиты информации: организационные, физические, программно-технические, криптографические методы защиты информации.

Тема 2. Основные понятия и задачи криптографии
Конфиденциальность, целостность, доступность. Криптографическая система (симметричная, несимметричная, гибридная). Блочное и поточное шифрование.

Тема 3. Криптоанализ шифров
Атаки на криптографические системы, взлом шифра. Криптографическая стойкость шифров. Абсолютно стойкий шифр по Шеннону.

Тема 4. Исторические шифры
Шифры замены, перестановки, гаммирования.

Тема 5. Криптографическая система DES
Принципы функционирования.

Тема 6. Криптографическая система ГОСТ 28147-89
Принципы функционирования.

Тема 7. Режимы работы алгоритмов блочного шифрования
Режим простой замены, обратной связи, в том числе, по выходам, гаммирования, выборки имитовставки.

Тема 8. Поточные шифры на основе линейных регистров сдвига
Потоковые генераторы на базе регистров сдвига с линейной обратной связью, генератор «стоп-пошел», пороговый генератор, генератор Геффе.
.
Тема 9. Криптографическая система RSA
Принципы функционирования.

Тема 10. Электронно-цифровая подпись
Принципы функционирования. Реализации электронно-цифровой подписи с помощью симметричных и несимметричных криптосистем.

Тема 11. Криптографические протоколы
Схема аутентификации Шнорра, электронные деньги, протоколы голосования.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем проведения тестов по лекционному материалу и фиксируется в форме контрольной точки не менее одного раза в семестр.

Примеры тестовых заданий

1. Какие исторические шифры Вы знаете:
   а) *шифры замены*;
   б) *шифры перестановки*;
   в) *шифра гаммирования*;
   г) шифры подмены;
   д) шифры подстановки.
2. Под конфиденциальностью понимается свойство информации:
   а) *быть доступной только ограниченному кругу пользователей*;
   б) сохранять свое содержание/структуру в процессе хранения/передачи;
   в) совершать действия незаметно для других.
3. Методы защиты информации называются стеганографическими, если:
   а) *сам факт передачи информации замаскировывается*;
   б) защищают от разрушения встраиваемых и внешних средств защиты;
   в) защищают от неправомочных действий пользователей.
4. Существует ли абсолютно стойкий шифр:
   а) *да, если он удовлетворяет трем условиям, доказанным Шенноном*;
   б) всякий шифр является абсолютно стойким;
   в) абсолютно стойкого шифра не существует.
5. В алгоритме шифрования DES длина блока открытого текста равна:
   а) 32 бита;
   б) *64 бита*;
   в) 128 бит;
   г) может быть задана произвольно.
6. В алгоритме шифрования DES длина ключа равна:
   а) 32 бита;
   б) *56 бит*;
   в) 128 бит;
   г) может быть задана произвольно.
7. В алгоритме шифрования ГОСТ 28147-89 длина блока открытого текста равна:
   а) 32 бита;
   б) *64 бита*;
   в) 128 бит;
   г) может быть задана произвольно.
8. В алгоритме шифрования ГОСТ 28147-89 длина ключа равна:
   а) 32 бита;
   б) 128 бит;
   в) *256 бит*;
   г) может быть задана произвольно.
9. Электронно-цифровая подпись предназначена для того, чтобы:
   а) *доказать подлинность электронного документа*;
   б) зашифровать электронный документ;
   в) расшифровать электронный документ;
   г) в электронном информационном пространстве она вообще не нужна.
10. Метки даты и времени в электронных документах используются, чтобы:
   а) *предотвратить повторное использование электронного документа*;
   б) использовать электронный документ в определенную дату и время;
   в) вообще не использовать электронный документ.

Самостоятельная работа заключается в подготовке к тестам, а также рассмотрению теоретических вопросов, возможно, с использованием ресурсов, указанных в п. 12.

Вопросы для самостоятельной работы

1. Что называется криптографической атакой.
2. Что понимается под стойкостью шифра.
3. Существует ли абсолютно стойкий шифр.
4. Алгоритм шифрования DES.
5. Функция раундового шифрования в DES.
6. Генерация ключа раундового шифрования в DES.
7. Алгоритм шифрования ГОСТ 28147-89.
8. Режимы использования блочных шифров.
9. За счет чего достигается нелинейность в алгоритмах блочного шифрования.
10. Односторонние функции.
11. Реализация электронно-цифровой подписи с помощью симметричных криптосистем.
12. Реализация электронно-цифровой подписи с помощью несимметричных криптосистем.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Зачет с оценкой в пятом семестре проводится в письменной форме по билетам. Билет содержит два теоретических вопроса. Продолжительность зачета 1,5 часа.

Первый вопрос в каждом билете сформулирован для проверки сформированности следующих компетенций/индикаторов компетенций: ОПК-7, ИОПК 7.1, ИОПК 2.2, ОПК-8, ИОПК 8.1, ИОПК 8.2, ИОПК 8.3.

Второй вопрос в каждом билете сформулирован для проверки сформированности следующих компетенций/индикаторов компетенций: ОПК-9, ИОПК 9.1, ИОПК 9.2, ПК-2, ИПК 2.1, ИПК 2.2.

Примерный перечень теоретических вопросов

1. Основные понятия и задачи криптографии.
2. Основные криптоаналитические атаки.
3. Стойкость криптоалгоритмов.
4. Криптографическая система DES.
5. Криптографическая система ГОСТ 28147-89.
6. Режимы использования блочных шифров.
7. Криптографическая система RSA.
8. Шифры простой замены.
9. Криптоанализ шифров простой замены.
10. Шифры многоалфавитной замены.
11. Шифры перестановки.
12. Криптоанализ шифров перестановки.
13. Организация секретной связи с использованием симметричной и несимметричной криптосистем**.**
14. Математическая модель шифра по К. Шеннону.
15. Поточные шифры.
16. Блочные шифры: принципы построения блочных шифров.
17. Криптографические протоколы.
18. Протоколы идентификации.
19. Электронно-цифровая подпись.

Результаты промежуточной аттестации определяются оценками «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

Критерии оценивания

Компетенция	Индикатор компетенции	Критерии оценивания результатов обучения			
		Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
ОПК-7: Способен решать стандартные задачи профессиональной деятельности с применением современных методов исследования и информационно-коммуникационных технологий	**ИОПК 7.1:** Использует современные информационно-коммуникационные технологии для обработки, анализа и представления в требуемом формате информации	Слабо освоенные навыки и умения работы с источниками информации	Частично освоенные навыки и умения работы с источниками информации	В целом успешно применяемые навыки и умения работы с информационно-коммуникационными системами для представления в требуемом формате информации	Успешно применяемые навыки и умения работы с информационно-коммуникационными системами для обработки , анализа и представления в требуемом формате информации
	ИОПК 7.2: Решает информационно-коммуникационные задачи с помощью современных систем автоматизации	Слабо сформированные навыки и умения решения задач	Частично освоенные навыки и умения решения задач	В целом успешно применяемые навыки работы с системами автоматизации для решения задач	Успешно применяемые навыки и умения работы с современными системами автоматизации для решения задач
ОПК-8: Способен использовать современные программные и инструментальные средства компьютерного моделирования для решения различных исследовательских и профессиональных задач	**ИОПК 8.1:** Использует современные информационные технологии и программное обеспечение при решении задач профессиональной деятельности	Слабо сформированные навыки и умения работы с источниками информации	Частично освоенные умения работы с источниками информации	В целом успешно применяемые навыки и умения поиска информации и работы с источниками информации	Успешно применяемые навыки и умения поиска источников информации и программных средств, необходимых для работы
	ИОПК 8.2: Использует компьютерные системы поиска, хранения, обработки, анализа и представления информации	Слабо сформированные навыки и умения работы с информационно-поисковыми системами	Частично освоенные навыки и умения работы с информационно-поисковыми системами	В целом успешно применяемые навыки работы с системами поиска и обработки информации, а также с базами данных	Успешно применяемые навыки использования компьютерных систем поиска, хранения, обработки, анализа и представления информации
	ИОПК 8.3: Соблюдает требования	Фрагментарные знания об информационно	Общие, но не структурированные знания	Сформированные, но содержащие	Сформированные системные знания об

	информационной безопасности при использовании современных информационных технологий и программного обеспечения	й безопасности, слабо сформированные навыки и умения оценки безопасности современных информационных систем	об информационной безопасности, частично сформированные навыки и умения оценки безопасности современных информационных систем	отдельные пробелы знания об информационной безопасности; в целом успешно применяемые навыки и умения оценки безопасности современных информационных систем	информационной безопасности; сформированные навыки и умения оценки безопасности используемого программного обеспечения
ОПК-9: Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения	**ИОПК 9.1:** Применяет современные инструментальные системы программирования и компьютерного моделирования при решении прикладных задач	Слабо освоенные навыки и умения оценки безопасности современных инструментальных систем программирования	Частично освоенные навыки и умения оценки безопасности современных инструментальных систем программирования	В целом успешно применяемые навыки и умения оценки безопасности современных инструментальных систем программирования и компьютерного моделирования	Успешно применяемые навыки и умения оценки безопасности современных инструментальных систем программирования и компьютерного моделирования
	ИОПК 9.2: Владеет навыками работы в компьютерной среде	Слабо освоенные навыки и умения поиска и представления информации	Частично освоенные навыки и умения поиска и представления информации	В целом успешно применяемые навыки и умения поиска, обработки и представления информации	Успешно применяемые навыки и умения поиска, обработки и представления информации
ПК-2: Способен проводить научно-исследовательские и опытно-конструкторские разработки функциональных приборов и устройств радиоэлектроники	**ИПК 2.2:** Использует современные пакеты прикладных программ для разработки структурных, функциональных и принципиальных схем радиоэлектронных устройств комплексов передачи информации	Слабо освоенные навыки и умения выбора необходимых для работы пакетов прикладных программ	Частично освоенные навыки и умения выбора необходимых для работы пакетов прикладных программ	В целом успешно применяемые навыки и умения для работы с различными пакетами прикладных программ	Успешно применяемые навыки и умения для работы с различными пакетами прикладных программ

Текущий контроль по дисциплине влияет на результаты промежуточной аттестации: регулярное прохождение тестов (не менее 70 %) является показателем для автоматического допуска к сдаче зачета.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» – https://moodle.tsu.ru/course/view.php?id=6914

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине размещены в электронном учебном курсе по дисциплине.

в) Лекционные материалы размещены в электронном учебном курсе по дисциплине.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Лось А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : Учебник для вузов / Лось А. Б., Нестеренко А. Ю., Рожков М. И. – Москва : Юрайт, 2020. – 473 с. – (Высшее образование) . URL: https://urait.ru/bcode/450277. URL: https://urait.ru/book/cover/04F8FEB5-57F2-4A7F-8BDC-E76F2FFA1551

– Васильева И. Н. Криптографические методы защиты информации : Учебник и практикум для вузов / Васильева И. Н. – Москва : Юрайт, 2020. – 349 с. – (Высшее образование) . URL: https://urait.ru/bcode/450998. URL: https://urait.ru/book/cover/142D68F4-E143-4A70-A1D2-C24C62482009

– Петров А. А. Компьютерная безопасность. Криптографические методы защиты / Петров А. А. – Москва : ДМК Пресс. – 448 с. URL: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=3027. URL: https://e.lanbook.com/img/cover/book/3027.jpg

– Бабенко Л. К. Криптографическая защита информации: симметричное шифрование : Учебное пособие для вузов / Бабенко Л. К., Ищукова Е. А. – Москва : Юрайт, 2020. – 220 с. – (Высшее образование) . URL: https://urait.ru/bcode/452871. URL: https://urait.ru/book/cover/9C91BAFE-E408-42D3-8791-3BC2B5384E30

– Фомичёв В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : Учебник для вузов / Фомичёв В. М., Мельников Д. А. ; под ред. Фомичёва В.М. – Москва : Юрайт, 2020. – 245 с. – (Высшее образование) . URL: https://urait.ru/bcode/451486. URL: https://urait.ru/book/cover/A48E1FB0-07DD-41BB-85E4-EB183D843FDA

б) дополнительная литература:

– Нестеров С. А. Основы информационной безопасности : учебное пособие / Нестеров С. А. – 5-е изд., стер. – Санкт-Петербург : Лань. – 324 с. URL: https://e.lanbook.com/book/114688. URL: https://e.lanbook.com/img/cover/book/114688.jpg

– Фомичёв В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : Учебник для вузов / Фомичёв В. М., Мельников Д. А. ; под ред. Фомичёва В.М. – Москва : Юрайт, 2020. – 209 с. – (Высшее образование) . URL: https://urait.ru/bcode/450820. URL: https://urait.ru/book/cover/78D639F7-58C5-4677-A800-77EA4A701B89

– Швечкова О. Г. Базовые криптографические алгоритмы защиты информации : учебное пособие : [для студентов высших учебных заведений, обучающихся по направлениям подготовки 2.09.03.04 "Программная инженерия" и 2.09.03.03 "Прикладная информатика"] / О. Г. Швечкова, А. Н. Пылькин, Д. В. Марчев. – Москва : Курс, 2020. – 167 с., [1] с.: ил., табл.

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– Microsoft Office Standart 2013 Russian: пакет программ

б) информационные справочные системы:

– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system

– Электронная библиотека (репозиторий) ТГУ – http://vital.lib.tsu.ru/vital/access/manager/Index

– ЭБС Лань – http://e.lanbook.com/

– Образовательная платформа Юрайт – https://urait.ru/

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

15. Информация о разработчиках

Прокопенко Светлана Анатольевна, к.т.н., доцент, ТГУ, доцент