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

03.03.03 Радиофизика

Направленность (профиль) подготовки/ специализация:
Киберфизические системы, прикладная электроника и квантовые технологии

Форма обучения
Очная

Квалификация
Радиофизик-кибернетик, преподаватель. Разработчик киберфизических и квантовых систем

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
О.А. Доценко

Председатель УМК
А.П. Коханенко

Томск – 2025

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

БК-1 Способен применять общие и специализированные компьютерные программы при решении задач профессиональной деятельности.

ОПК-3 Способен использовать информационные технологии и программные средства при решении задач профессиональной деятельности, соблюдая требования информационной безопасности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

РОБК 1.1 Знает правила и принципы применения общих и специализированных компьютерных программ для решения задач профессиональной деятельности

РОБК 1.2 Умеет применять современные IT-технологии для сбора, анализа и представления информации; использовать в профессиональной деятельности общие и специализированные компьютерные программы

РООПК 3.1 Знает современные информационные технологии и программные средства при решении задач профессиональной деятельности.

РООПК 3.2 Умеет соблюдать требования информационной безопасности при использовании современных информационных технологий и программного обеспечения

2. Задачи освоения дисциплины

– Научиться 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 «Дисциплины (модули)».

Дисциплина относится к обязательной части образовательной программы.

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

Пятый семестр, зачет

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: 48 ч.

-практические занятия: 18 ч.

в том числе практическая подготовка:18 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, отчетов практическим занятиям и фиксируется в форме контрольной точки не менее одного раза в семестр.

Оценочные материалы текущего контроля размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Зачет в пятом семестре проводится в письменной форме по билетам. Экзаменационный билет состоит из двух частей. Продолжительность зачета 1 час.

Оценочные материалы для проведения промежуточной аттестации размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

11. Учебно-методическое обеспечение

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

б) Оценочные материалы текущего контроля и промежуточной аттестации 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 / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. – 2-е изд., испр. – Москва : Издательство Юрайт, 2025. – 473 с. – (Высшее образование). – ISBN 978-5-534-12474-3. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/560426

– Васильева И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. – Москва : Издательство Юрайт, 2025. – 310 с. – (Высшее образование). – ISBN 978-5-534-02883-6. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/560977

б) дополнительная литература:

– Бабенко Л. К.Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. – Москва : Издательство Юрайт, 2021. – 220 с. – (Высшее образование). – ISBN 978-5-9916-9244-1. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/471695

в) ресурсы сети Интернет:

– открытые онлайн-курсы

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office On-eNote, MS Office Publisher, MS Outlook, MS Office Web Apps (Word Excel MS PowerPoint Outlook)

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/

– ЭБС Консультант студента – http://www.studentlibrary.ru/

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

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения занятий семинарского типа, 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