МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Тульский государственный университет»

Институт прикладной математики и компьютерных наук
Кафедра «Прикладная математика и информатика»

Утверждено на заседании кафедры
«Прикладная математика и информатика»
24 января 2022 г., протокол № 5

Заведующий кафедрой

_____М.В. Грязев

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по самостоятельной работе студентов
по дисциплине (модулю)
«Методы защиты информации»

основной профессиональной образовательной программы
высшего образования – программы бакалавриата

по направлению подготовки
01.03.02 Прикладная математика и информатика

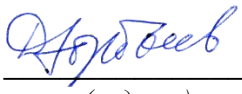
с направленностью (профилем)
Прикладная математика и информатика

Форма обучения: очная

Идентификационный номер образовательной программы: 010302-01-22

Тула 2022 год

Разработчик методических указаний

Горбачев Д.В., профессор каф. ПМиИ, д.ф.-м.н.	
(ФИО, должность, ученая степень, ученое звание)	*(подпись)*

1. Цели и задачи самостоятельной работы студента

Целью освоения дисциплины «Методы защиты информации» является изучение математических методов и программных средств защиты цифровой информации, включая элементы теории кодирования и криптографии.

Задачами освоения дисциплины являются:

- изучение теории и методов защиты информации;
- освоение программных средств защиты информации;
- знакомство с современными проблемами в области информационной безопасности.

2. Самостоятельное изучение разделов дисциплины

№ п/п	Наименование видов самостоятельной работы	Рекомендуемая литература
1	Самостоятельное изучение отдельных тем или разделов дисциплины: Коды, исправляющие ошибки Криптографические протоколы	[2, 4]
2	Подготовка к лабораторным работам	[1–19]

Вопросы для самопроверки

1. Проблемы защиты информации
2. Регулярные выражения
3. Префиксные коды
4. Словарные методы сжатия
5. Алгоритм сжатия BZIP
6. Расширенный алгоритм Евклида
7. Малая теорема Ферма, теорема Эйлера
8. Поле вычетов
9. Поле Галуа
10. Дискретный логарифм
11. Контрольные суммы
12. CRC-код
13. Коды, исправляющие ошибки
14. БЧХ-коды
15. Криптографическая защита информации
16. Симметрические криптоалгоритмы
17. Блочные шифры
18. Криптографические хэш-функции
19. Криптоанализ хэш-функций
20. Асимметричные (с открытым ключом) криптоалгоритмы
21. Алгоритм Диффи–Хеллмана
22. Алгоритм RSA
23. Криптографические протоколы
24. SSH, SSL
25. Git

3. Рекомендуемая литература

1. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах : учеб. пособие для вузов / П.Б. Хорев. — 3-е изд., стер. — М. : Академия, 2007. — 256с. : ил. — (Высшее профессиональное образование: Информатика и вычислительная техника). — Библиогр. в конце кн. — ISBN 978-5-7695-4157-5 /в пер./ : 229.00.
2. Ященко, В.В. Введение в криптографию: Новые математические дисциплины : Учебник / В.В. Ященко, Н.П. Варновский, Ю.В. Нестеренко и др.; Под общ. ред. В.В. Ященко. — СПб. и др. : МЦНМО: Питер, 2001. — 288с. : ил. — Библиогр. в конце гл. — ISBN 5-318-00443-1 /в пер./ : 81.00.
3. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко; Ин-т проблем информационной безопасности МГУ. — М. : МЦНМО, 2003. — 328с. : ил. — (Информационная безопасность: криптография). — Библиогр. в конце кн. — ISBN 5-94057-103-4 /в пер./ : 73.00.
4. Глаголев, Валерий Владимирович. Алгебраическая теория кодирования : учебн. пособие / В.В. Глаголев ; ТуГУ, Механико-математ. фак. — Тула : Изд-во ТулГУ, 2004 .— 116 с. — в дар от каф. ПМиИ ТулГУ ТулГУ : 1308509-1308517. — Библиогр. в конце кн. — ISBN 5-7679-0564-9.
5. Сэломон, Д. Сжатие данных, изображений и звука : учеб. пособие для вузов / Д. Сэломон; пер. с англ. В.В. Чепыжова. — М. : Техносфера, 2004. — 368с. : ил. — (Мир программирования). — Библиогр. в конце кн. — ISBN 5-94836-027-X : 202.50.
6. Куприянов, А.И. Основы защиты информации : учеб. пособие / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. — 2-е изд., стер. — М. : Академия, 2007. — 256с. : ил. — (Высшее профессиональное образование: Радиоэлектроника). — Библиогр. в конце кн. — ISBN 978-5-7695-4416-3 /в пер./ : 247.00.
7. Шнайер, Б. Секреты и ложь : Безопасность данных в цифровом мире: Пер.с англ. / Б. Шнайер. — М.и др. : Питер, 2003. — 368с. — (Классика Computer Science). — Библиогр. в конце кн. — ISBN 5-318-00193-9 /в пер./ : 235.00. — ISBN 0-471-25311-1 (англ.).
8. Лапонина, О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : курс лекций: учеб. пособие для вузов / О.Р. Лапонина; под ред. В.А. Сухомлина. — М. : Интернет-Ун-т Информ. Технологий, 2005. — 608с. : ил. — (Основы информационных технологий). — Библиогр. в конце кн. — ISBN 5-9556-0020-5 /в пер./ : 400.00.
9. Касперски, К. Записки исследователя компьютерных вирусов / К. Касперски. — М. и др. : Питер, 2006. — 316с. : ил. — ISBN 5-469-00331-0 : 85.03.
10. Аграновский, А.В. Практическая криптография: алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади. — М. : Солон-Пресс, 2002. — 256с. : ил. + 1 CD. — (Аспекты защиты). — Библиогр. в конце кн. Приложение: Практическая криптография: алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади. — М. : Солон-Пресс, 2002. — 1 опт. диск (CD-ROM). — (Аспекты защиты). — ISBN 5-98003-002-6 : 187.00.
11. Фленов, М.Е. Web-сервер глазами хакера / М.Е. Фленов. — СПб. : БХВ-Петербург, 2007. — 288с. : ил. + 1опт.диск(CD ROM). Приложение: Web-сервер глазами хакера / М.Е. Фленов. — СПб. : БХВ-Петербург, 2007. — 1опт.диск (CD ROM). ISBN 5-94157-913-6 : 126.65.
12. Галатенко, В.А. Стандарты информационной безопасности : Курс лекций / В.А. Галатенко; Под ред. В.Б. Бетелина; Интернет ун-т информ. технологий. — М., 2004. — 328с. —

(Основы информационных технологий). — Библиогр. в конце кн. — ISBN 5-9556-0007-8 /в пер./ : 200.00.

13. Баричев, С.Г. Основы современной криптографии : Учеб. курс / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. — 2-е изд., перераб. и доп. — М. : Горячая линия-Телеком, 2002. — 175с. : ил. — Библиогр. в конце кн. — ISBN 5-93517-075-2 : 71.50.
14. Вопросы защиты информации : журнал. — М.: ВИМИ.
15. Information Security = Информационная безопасность : журнал. — М.: Гротек.
16. Information Security – Информационная безопасность: http://www.itsec.ru/
17. Citforum – Информационная безопасность: http://citforum.ru/security/
18. http://ru.wikipedia.org/wiki/Информационная_безопасность
19. Горбачев, Д.В. Конспект лекций по курсу «Методы защиты информации». — Тула: ТулГУ, 2013. — (Электронный ресурс кафедры.).

4. Форма отчетности

По изучаемым темам предусмотрены вопросы в билетах для зачета.