МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ЧЕРЕПОВЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт информационных технологий

Кафедра математики и информатики

УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки (специальность):
01.03.02 Прикладная математика и информатика

Образовательная программа:
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Очная форма обучения

Составители:

Лавров В.В., старший
преподаватель кафедры МиИ

г. Череповец - 2022

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

Основная литература:

1. Информационная безопасность и защита информации : учебное пособие / А. С. Минзов, С. В. Бобылева, П. А. Осипов, А. А. Попов. — Дубна : Государственный университет «Дубна», 2020. — 85 с. — ISBN 978-5-89847-608-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/154490
2. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-4067-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/206279

Дополнительная литература:

1. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : НГТУ, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/152227
2. Федин, Ф. О. Информационная безопасность баз данных : учебное пособие / Ф. О. Федин, О. В. Трубиенко, С. В. Чискидов. — Москва : РТУ МИРЭА, 2020 — Часть 1 — 2020. — 133 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167605

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля), включая перечень информационных справочных систем (при необходимости)

1 Электронная библиотека «Университетская библиотека online». URL: http://biblioclub.ru/

2 Информационная система «Единое окно доступа к образовательным ресурсам». URL: http://window.edu.ru/

3 Образовательный портал Череповецкого государственного университета. URL: https://edu.chsu.ru/

4 Аналитические и учебные материалы лаборатории Касперского http://www.securelist.com/ru/

5 Защита от Microsoft http://windows.microsoft.com/ru-RU/windows/products/security-essentials

6 Национальный институт стандартов и технологии. http://csrc.nist.gov/publications/PubsFIPS.htmlNIST-FIPS-201-2.pdf

7 Официальный сайт FIPShttp://www.itl.nist.gov/fipspubs/

8 Сайт материалов по информационной безопасности http://www.iso27000.ru/

9 ISO 27001 оригинал от Британского института стандартов

10 Электронный учебник Б. Шнайера "Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си" http://www.ssl.stu.neva.ru/psw/crypto/appl_rus/appl_cryp.htm

11 Электронный курс Ю. Лифшица "Современные задачи криптографии"http://yury.name/cryptography/-

Учебно-методические указания и рекомендации к изучению тем лекционных и практических занятий, самостоятельной работе студентов

Лекции

№ п/п	Тема лекции	Количество часов
1	Общие принципы проектирования систем защиты информации.	6
2	Криптографические методы защиты информации.	6
3	Компьютерные сети. Защита информации.	6
4	Политики и стандарты безопасности.	6
	Итого	24

Лабораторные работы

№ п/п	Тема лабораторной работы	Количество часов
1	Общие принципы проектирования систем защиты информации.	12
2	Криптографические методы защиты информации.	6
3	Компьютерные сети. Защита информации.	6
4	Политики и стандарты безопасности.	12
	Итого	36

Образцы заданий для самостоятельной работы:

По итогам самостоятельной работы студент готовит отчет, включающий в себя ответы на вопросы и решение заданий, предполагавшихся к выполнению в ходе самостоятельной работы. Отчет сдается преподавателю в электронной форме.

Раздел 1. Общие принципы проектирования систем защиты информации.

1. Каковы цели защиты информации?
2. В чем состоит целостность данных?
3. В чем состоит конфиденциальность данных?
4. В чем состоит доступность данных?
5. Приведите примеры технических угроз информационной безопасности.
6. Какие проблемы для информационной безопасности порождает человеческий фактор?
7. Приведите примеры технических средств обеспечения информационной безопасности и защиты информации.
8. Назовите организационные меры обеспечения информационной безопасности и защиты информации. Обоснуйте целесообразность этих мер.
9. Назовите правовые меры обеспечения информационной безопасности и защиты информации.
10. Перечислите основные угрозы надежности и безопасности программного обеспечения.

Раздел 2. Криптографические методы защиты информации.

1. Криптография, криптоанализ и криптология – каково соотношение между этими науками?
2. Каково соотношение между шифрованием и кодированием?
3. Каково соотношение между стеганографией и криптографией?

4. Что такое ключ шифрования?
5. В чем принципиальное различие между симметричными и ассимитричными шифрами?
6. Почему шифр Цезаря очень неустойчив к взлому?
7. На чем основан взлом шифра Виженера по Казинскому?
8. В чем состоит различие между принципом устройства шифров подстановой и шифров перестановок?
9. В чем заключаются преимущества и недостатки гаммирования по сравнению с другими симметричными шифрами?
10. В сем состоит различие между блочными и потоковыми шифрами?
11. В чем состоит принцип Керкхоффса?
12. В чем заключаются принципы рассеивания и перемешивания? В чем из целесообразность?
13. Почему алгоритм DES не удовлетворяет современным требованиям к секретности?
14. В чем заключается атака методом грубой силы?
15. Что такое «проблема распределения ключей» в криптографии с закрытым ключом?
16. В чем состоит проблема доверия между пользователями в криптографии с закрытым ключом?
17. Что такое однонаправленная функция?
18. Какая однонаправленная функция лежит в основе алгоритма RSA ассиметричного шифрования?
19. Для каких действий используется открытый ключ в ассиметричной криптографии?
20. Для каких действий используется закрытый ключ в ассиметричной криптографии?

Раздел 3. Компьютерные сети. Защита информации.

1. Опишите, как осуществляется защита информации в локальных и глобальных компьютерных сетях.
2. Как осуществляется использование программ шифрования в компьютерной сети?
3. Для чего осуществляется резервное копирование и архивация данных?
4. Какие протоколы локальной сети используются для обеспечения безопасности работы?
5. Какие протоколы глобальной сети используются для обеспечения безопасности работы?

Раздел 4. Политики и стандарты безопасности.

6. Что запрещено пропагандировать согласно Конституции РФ?
7. Если международным договором РФ установлены иные правила, чем предусмотрено законом РФ, то правила какого нормативного акта должны применяться, согласно Конституции?
8. На какие виды подразделяется информация в зависимости от порядка ее предоставления (распространения) согласно Федеральному закону «Об информации, информационных технологиях и о защите информации»?
9. К каким видам информации не может быть ограничен доступ согласно Федеральному закону ««Об информации, информационных технологиях и о защите информации»?
10. Распространение каких видов информации запрещается Федеральным законом «Об информации, информационных технологиях и о защите информации»?
11. Каковы национальные интересы РФ согласно Доктрине информационной безопасности Российской Федерации?

Образцы заданий для лабораторных работ

По итогам выполнения лабораторной работы студент демонстрирует результаты работы преподавателю, а также сдает в электронном виде отчет, содержащий порядок выполнения работы.

Раздел 1. Общие принципы проектирования систем защиты информации
Решите кейс, предложенный преподавателем.

Раздел 2. Криптографические методы защиты информации.
Лабораторная работа «Шифрование»

1. Имеется таблица замены для двух шифров простой замены: шифра №1 и шифра №2.Расшифруйте сообщения, зашифрованные с помощью шифра №1
    - И.РЮУ.ЪФОБГНО
    - СЛХГ.ЪЛХО.ФОО.ЩВ
2. Пусть исходный алфавит содержит следующие символы:
   АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
   Зашифруйте с помощью шифра Вижинера и ключа ЯБЛОКО сообщения:
    - КРИПТОСТОЙКОСТЬ
    - ГАММИРОВАНИЕ
3. Пусть исходный алфавит состоит из следующих знаков (символ "_" (подчеркивание) будем использовать для пробела):
   АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_
   Расшифруйте сообщения, зашифрованные с помощью шифра Вижинера и ключа ОРЕХ:
    - ШВМБУЖНЯ
    - ЯБХЪШЮМХ
4. Первый байт фрагмента текста в шестнадцатеричном виде имеет вид A5. На него накладывается по модулю два 4-х битовая гамма 0111 (в двоичном виде). Что получится после шифрования?
5. Первый байт фрагмента текста, зашифрованного методом гаммирования (по модулю 2), в шестнадцатеричном виде имеет вид 9A. До шифрования текст имел первый байт, равный 74 (в шестнадцатеричном виде). Какой ключ использовался при шифровании?
6. Зашифруйте методом перестановки с фиксированным периодом d=6 с ключом 436215 сообщения:
    - ЖЕЛТЫЙ_ОГОНЬ
    - МЫ_НАСТУПАЕМ

Лабораторная работа «Шифр Цезаря»
На любом языке программирования напишите программу, реализующую алгоритм Цезаря. Техническое задание:

1. Зашифрование и расшифрование текстов, записанных кириллицей и латиницей.
2. Взлом зашифрованного русскоязычного текста методом наименьших квадратов.
3. Замена во вводимом тексте буквы ё на е.
4. Очистка вводимого текста от всех небуквенных символов, знаков препинания, пробелов, приведение всех букв к строчному регистру.
5. Приведение введенного значения ключа к диапазону [0; 32] для кириллицы, [0; 26] для латиницы.
6. Выдача обратного текста группами по пять слов.
7. Защита от неправильных действий пользователя.

8. Дружественный интерфейс.

Лабораторная работа «Шифр Виженера»

На любом языке программирования напишите программу, реализующую алгоритм Виженера.

Техническое задание:

1. Зашифрование и расшифрование текстов, записанных кириллицей.
2. Взлом зашифрованного русскоязычного текста методом наименьших квадратов на основе идей Казинского (в случае использования идей Фридмана необходимо уметь внятно объяснить эти идеи).
3. Замена во вводимом тексте буквы ё на е.
4. Очистка вводимого текста от всех небуквенных символов, знаков препинания, пробелов, приведение всех букв к строчному регистру.
5. Выдача обратного текста группами по пять символов.
6. Защита от неправильных действий пользователя.
7. Дружественный интерфейс.

Раздел 3. Компьютерные сети. Защита информации.

Лабораторная работа «Шифрование и цифровая подпись сообщений»

Используя программу PGP (англ. Pretty Good Privacy), выполните следующие задания:

1. Создайте пару ключей шифрования (открытый и закрытый)
2. Подпишите сообщение электронной цифровой подписью.
3. Зашифруйте сообщение для напарника по лабораторной работе. Отправьте сообщение напарнику.
4. Расшифруйте сообщение, полученное от напарника.
5. Проверьте подлинность электронной цифровой подписи в полученном сообщении.
6. Объясните смысл выполненных операций.

Раздел 4. Политики и стандарты безопасности.

Решите кейс, предложенный преподавателем.

Средства контроля качества обучения

Вопросы к экзамену:

1. Понятие информации и информационной безопасности.
2. Угрозы надежности и безопасности программного обеспечения.
3. Категории информационной безопасности.
4. Источники, риски, формы атак на информацию.
5. Построение систем защиты от угроз нарушения конфиденциальности, целостности, доступности информации.
6. Понятия идентификации и аутоинтефикации, протоколирование и аудит. Разграничение доступа.
7. Формальные модели защиты информации.
8. Криптография. Основные понятия и определения.
9. Классические шифры.
10. Понятие криптографической системы.
11. Симметричное и асимметричное шифрование.
12. Криптостойкость алгоритмов.
13. Современные алгоритмы шифрования.
14. Стандарты шифрования данных.
15. Методы генерации криптографически качественных псевдослучайных последовательностей.
16. Хеш-функции.
17. Электронно-цифровая подпись.
18. Системы управления ключами.
19. Понятия однонаправленной функции.
20. Общая характеристика и классификация компьютерных сетей. Сетевые сервисы и стандарты.
21. Защита информации в локальных и глобальных компьютерных сетях.
22. Правовые и организационные методы обеспечения информационной безопасности.
23. Особенности законодательства РФ в области информационной безопасности.
24. Политики информационной безопасности предприятий.
25. Стандарты в области управления информационной безопасностью.