

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета ФИТКБ
 /Гусев П.Ю./
28.02.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Методы и средства криптографической защиты информации»

Специальность 10.05.01 Компьютерная безопасность

Специализация специализация № 4 "Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2023

Автор программы
Заведующий кафедрой
Систем информационной
безопасности

 Н.М. Радько
 А.Г. Остапенко
 К.А. Разинкин

Руководитель ОПОП

Воронеж 2023

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины - получение знаний о принципах защиты информации с помощью криптографических методов и особенностях реализации этих методов на практике.

1.2. Задачи освоения дисциплины

- дать студентам основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами, на основе применения криптографических методов;
- изучение основных принципов анализа и синтеза шифров;
- изучение математических методов, используемых в криптографии;
- изучение перспективных направлений и тенденций развития криптографических систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Методы и средства криптографической защиты информации» относится к дисциплинам обязательной части блока Б1 учебного плана.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Методы и средства криптографической защиты информации» направлен на формирование следующих компетенций:

ОПК-10 - способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-10	Знать: - о принципиальных подходах к созданию современных технических средств криптографической защиты информации.
	Уметь: - практически решать задачи защиты программ и данных криптографическими средствами.
	Владеть: - основными принципами построения аппаратных и программных реализации криптографических алгоритмов.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Методы и средства криптографической защиты информации» составляет 7 з.е.

Распределение трудоемкости дисциплины по видам занятий

Виды учебной работы	Всего часов	Семестры	
		8	9
Аудиторные занятия (всего)	144	72	72
В том числе:			
Лекции	72	36	36
Практические занятия (ПЗ)	72	36	36
Самостоятельная работа	72	36	36
Курсовой проект	+	+	
Часы на контроль	36	-	36
Виды промежуточной аттестации		Зачет с оценкой	Экзамен
Общая трудоемкость академические часы зач.ед.	252 7	108 3	144 4

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

№ п/п	Наименование темы	Содержание раздела	Лекц	Практ. зан.	СРС	Всего, час
8 семестр						
1	Основные понятия криптографии	Содержание и задачи дисциплины. Ее особенности и связь с другими дисциплинами. Методические рекомендации по ее изучению и требованию, предъявляемые при проверке знаний. Общая характеристика процессов защиты информации. Требования к защите, сетодология разработки и анализа средств защиты. Классические модели защиты информации. Стеганографические и криптографические методы защиты информации.	6	6	6	18
2	Простые криптографические шфры	Краткий исторический очерк развития криптографии. Исторические примеры: шифр Цезаря, квадрат Полибия, шифр Виженера, решетка Кардано, книжный шифр и др. Понятие о криптоанализе. Основные этапы становления и развития криптографии, как науки.	6	6	6	18
3	Открытые сообщения	Открытые сообщения. Частотные характеристики открытых сообщений. Математические модели открытых	6	6	6	18

		сообщений и критерии на открытый текст. Способы представления информации, подлежащей шифрованию. Особенности нетекстовых сообщений				
4	Шифры	Определение шифра и его математические модели. Ручные и машинные шифры. Ключевая система и основные требования к шифрам. Понятие криптосистемы. Вопросы распределения ключей в сети шифрованной связи.	6	6	6	18
5	Принципы построения и реализации криптографических алгоритмов	Основные способы реализации криптографических алгоритмов и требования, предъявляемые к ним. Датчики псевдослучайных последовательностей (регистры сдвига, линейный конгруэнтный метод, линейные рекуррентные последовательности, мультиплексорные методы). Периодичность случайных последовательностей. Распределение элементов в псевдослучайных последовательностях. Основные узлы и блоки криптосистем. Блоки выработки шифрующей последовательности и блоки шифрования.	6	6	6	18
6	Методы анализа криптографических алгоритмов	Алгоритмические, аналитические и статистические методы анализа поточных шифров. Особенности криптоанализа блочных шифров	6	6	6	18
9 семестр						
7	Шифрование с открытым ключом	Системы шифрования с открытым ключом. Понятие односторонней функции. Криптосистемы RSA и Эль-Гамала. Проблема факторизации целых чисел в конечных полях. Криптосистемы с открытым ключом на базе задачи о рюкзаке и линейных кодов. Асимметричные системы шифрования и их преимущества. Хэш-функции и их использование в криптографии. Алгоритмы выработки хэш-функций.	10	10	10	30
8	Криптографические протоколы	Понятие криптографического протокола. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. Цифровая подпись. Стандарты цифровой подписи. Протоколы аутентификации и их связь с цифровой подписью. Протоколы сертификации и предварительного распределения ключей. Открытое распределение ключей (по Диффи-Хеллману).	10	10	10	30
9	Криптосистемы на базе ПЭВМ	Особенности реализации криптосистем на базе вычислительной техники. Криптографические интерфейсы. Применение смарт-карт в системах электронных платежей. Протоколы SET.	6	6	6	18
10	Компьютерная стеганография	Компьютерная стеганография - метод, дополняющий традиционные криптографические методы. "Полное" скрывание данных. Типы файл-контейнеров (графические, звуковые). Алгоритмы "упаковки" данных (регулярные, псевдослучайные, комбинированные). Объем информации, помещаемой в файл-контейнеры различных типов	10	10	10	30
Итого			72	72	72	216

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсовых проектов в 8 семестре для очной формы обучения.

Примерная тематика курсового проекта: «Методы и средства криптографической защиты информации»

Задачи, решаемые при выполнении курсового проекта:

- использование криптографических методов защиты информации в компьютерных системах;
- решение практических задач защиты информации в компьютерных системах;
- обоснование эффективности выбранного метода шифрования.

Курсовой проект включает в себя графическую часть и расчетно-пояснительную записку.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-10	Знать: - о принципиальных подходах к созданию современных технических средств криптографической защиты информации.	Тест	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: - практически решать задачи защиты программ и данных криптографическими средствами.	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: - основными принципами построения аппаратных и программных реализаций	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	криптографических алгоритмов.			программах
--	-------------------------------	--	--	------------

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 8 семестре по четырехбальной системе:

- «отлично»;
- «хорошо»;
- «удовлетворительно»;
- «неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл	Неудовл
ОПК-10	Знать: - о принципиальных подходах к созданию современных технических средств криптографической защиты информации.	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Уметь: - практически решать задачи защиты программ и данных криптографическими средствами.	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть: - основными принципами построения аппаратных и программных реализации криптографических алгоритмов.	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

Результаты промежуточного контроля знаний оцениваются в 9 семестре по четырехбальной системе:

- «отлично»;
- «хорошо»;
- «удовлетворительно»;
- «неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл	Неудовл
ОПК-10	Знать: - о принципиальных подходах к созданию современных технических средств криптографической защиты информации.	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Уметь: - практически решать задачи защиты программ и данных криптографическими средствами.	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть: - основными принципами построения аппаратных и программных реализации криптографических алгоритмов.	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1) Симметричные алгоритмы подразделяются на:

- блочные шифры;
- алгоритмические шифры;
- потоковые шифры;
- ассиметричные шифры.

2) Какие значения обычно производят криптографические хэш-функции?

- 2 и более бита;
- 128 и более бит;
- 1 байт и более;
- Менее 4 байт.

3) На чём специализируется метод brute force?

- переполнение базы данных системы;
- путём DDoS атаки на систему;
- изменение шифрованного текста;
- перебор всех значений ключа.

4) Поясните метод атаки с заданным текстом:

- имеется возможность получить шифрованный документ для любого нужного ему текста, но нет ключа;
- не имеется возможности получить шифрованный документ для нужного ему текста, но имеется ключ;
- известно содержимое всего или части зашифрованного текста;
- известен ключ, но необходимо расшифровать документ.

5) Шифрование это:

- процедура, использующая некое необратимое преобразование;
- процедура, использующая некий алгоритм возведения в степень;
- процедура, использующая некий алгоритм взятия корня;
- процедура, использующая некое обратимое преобразование.

6) Правило зашифрования это:

- способ вычисления значения функции для произвольного аргумента;
- способ вычисления значения аргумента;
- способ поиска ключа для определённой функции;
- обратный процесс дешифрования.

7) Если фрагменты открытого текста заменяются некоторыми их эквивалентами в шифртексте, то соответствующий шифр относится к классу:

- шифров перестановки;
- шифров замены;
- шифров подстановки;
- композиционных шифров.

8) Как называется преобразование, представляющее нелинейную замену байт, выполняемую независимо с каждым байтом состояния:

- замена байт;
- уничтожение байт;
- искажение байт;
- изменение байт.

9) В какой операции цикловой ключ добавляется к состоянию посредством простого EXOR?

- преобразование сдвига строк;
- преобразование замешивания столбцов;
- добавление циклового ключа;
- расширение ключа.

10) Расширенный ключ это:

- линейный массив 4-ех байтовых слов;
- линейный массив 4-ех битовых слов;
- нелинейный массив 8-ми байтовых слов;
- нелинейный массив 8-ми битовых слов.

7.2.2 Примерный перечень заданий для решения стандартных задач

1) нормальным алфавитом называют:

- алфавит, в котором буквы расположены в их естественном порядке;
- алфавит, в котором цифры расположены в их естественном порядке;
- алфавит, в котором цифры расположены в неестественном порядке;
- алфавит, в котором буквы расположены в неестественном порядке.

2) Как называют алфавиты, полученные из нормального на основе некоторого правила?

- случайные;
- систематически перемешанные;
- нормальные;
- элементарные.

3) Какие последствия могут быть от избыточности открытого текста, проникающего в шифртекст:

- повышенная стойкость текста;
- трудность расшифровки;
- повышенная слабость текста;
- вовлечение дополнительных структур для дешифровки.

4) Биграмм-это:

- пара букв;
- пара чисел;
- зеркальный процесс;
- параметрическая функция.

5) Как позволяют шифровать информацию потоковые шифры?

- побайтово;
 - наборами бит данных;
 - побитово;
 - наборами байт данных.
- 6) Для чего используется алгоритм с открытым ключом?
- чтобы передать случайным образом сгенерированный секретный ключ;
 - чтобы передать определённым образом сгенерированный секретный ключ;
 - чтобы передать случайным образом сгенерированный открытый ключ;
 - чтобы передать определённым образом сгенерированный открытый ключ.
- 7) Цифровая подпись это:
- подпись в электронном варианте ;
 - блок данных, сгенерированный с использованием некоторого секретного ключа;
 - символы случайного алфавита;
 - шифрование определённых данных.
- 8) Для чего используются криптографические генераторы случайных чисел:
- для создания баз данных;
 - для теории относительности;
 - для проверки работоспособности системы;
 - для генерации ключей.
- 9) Какие выделяют важные типы криптографических хэш-функций?
- последовательные;
 - ключевые;
 - бесключевые;
 - беспорядочные.
- 10) Как называют бесключевые хэш-функции?
- кодами обнаружения ошибок;
 - открытыми ключами;
 - кодами верификации сообщения;
 - кодами аутентификации сообщения.

7.2.3 Примерный перечень заданий для решения прикладных задач

- 1) Что является надёжностью схемы цифровой подписи?
- подделка подписи;
 - подмена сообщения;
 - дешифрация сообщения
 - создание подписанного сообщения.
- 2) Что такое MAC?
- Microsoft Access Code.

- Message Apple Company.
- Message Authentication Code.
- Micro Alphabet Code.

3) Что подразумевают под имитозащитой данных?

- защиту от навязывания ложных данных;
- защиту от навязывания паролей;
- защиту от навязывания открытых ключей;
- имитацию дешифрования данных.

4) Какие важные свойства необходимо гарантировать для каждого обрабатываемого массива данных?

- подлинность;
- авторство;
- полную защищённость;
- специальную цифровую подпись.

5) Хеш-функции – это:

- функции, предназначенные для “сжатия” произвольного сообщения или набора данных, записанных, как правило, в двоичном алфавите, в некоторую битовую комбинацию фиксированной длины, называемую свёрткой
- структура данных, реализующая интерфейс ассоциативного массива, а именно, она позволяет хранить пары (ключ, значение) и выполнять три операции: операцию добавления новой пары, операцию поиска и операцию удаления пары по ключу
- некоторое значение, рассчитанное из последовательности данных путём применения определённого алгоритма, используемое для проверки правильности передачи данных
- «закон», по которому каждому элементу x из некоторого множества X ставится в соответствие единственный элемент y из множества Y .

6) Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования?

- 1
- 2
- 3
- 4

7) Сколько ключей используется в системах с открытым ключом?

- 1
- 2
- 3
- 4

8) Криптостойкость – это ...

- Характеристика шрифта, определяющая его стойкость к шифрованию без знания ключа

- Свойство гаммы
- Все ответы верны

9) Для современных криптографических систем защиты информации сформулированы следующие общепринятые правила:

- Длина шифрованного текста должна быть равна длине исходного текста
- Зашифрованное сообщение должно поддаваться чтению только при наличии ключа
- Нет правильного ответа

10) Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

- Знание алгоритма шифрования не должно влиять на надежность системы
- Структурные элементы алгоритма шифрования должны быть неизменными
- Не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования
- Знание алгоритма шифрования влияет на надежность системы

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Сетодология разработки и анализа средств защиты.
2. Классические модели защиты информации.
3. Стеганографические и криптографические методы защиты информации.
4. Шифр Цезаря, квадрат Полибия, шифр Виженера.
5. Решетка Кардано, книжный шифр.
6. Открытые сообщения. Частотные характеристики открытых сообщений.
7. Математические модели открытых сообщений и критерии на открытый текст.
8. Способы представления информации, подлежащей шифрованию.
9. Определение шифра и его математические модели. Ручные и машинные шифры.
10. Вопросы распределения ключей в сети шифрованной связи.
11. Датчики псевдослучайных последовательностей.
12. Распределение элементов в псевдослучайных последовательностях.
13. Основные узлы и блоки криптосистем.
14. Алгоритмические, аналитические и статистические методы анализа поточных шифров.

7.2.5 Примерный перечень вопросов для подготовки к экзамену

1. Основные алгоритмы шифрования.
2. Цифровые подписи.
3. Криптографические хеш-функции.
4. Криптографические генераторы случайных чисел.
5. Обеспечиваемая шифром степень защиты.

6. Криптоанализ и атаки на криптосистемы.
7. Классификация шифров.
8. Блочные шифры.
9. Поточные шифры.
10. Алфавиты открытых сообщений.
11. Частотные характеристики текстовых сообщений.
12. Основные положения.
13. Пример функции хэширования – ГОСТ Р 34.11-94.
14. Цифровая подпись.
15. Основные положения криптосистемы RSA.
16. Построение кодирующей процедуры E для криптосистемы RSA.
17. Построение декодирующей процедуры D для криптосистемы RSA.
18. Алгоритмические задачи, связанные со схемой RSA.
19. Общая идея шифра Эль-Гамала.
20. Пароли шифра Эль-Гамала.
21. Электронная подпись шифра Эль-Гамала.
22. Задача аутентификации данных.
23. Задача имитозащиты данных.
24. Подходы к контролю неизменности данных.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Зачет с оценкой и экзамен проводятся по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Основные понятия криптографии	ОПК-10	Тест, решение стандартных и прикладных задач
2	Простые криптографические	ОПК-10	Тест, решение

	шифры		стандартных и прикладных задач
3	Открытые сообщения	ОПК-10	Тест, решение стандартных и прикладных задач
4	Шифры	ОПК-10	Тест, решение стандартных и прикладных задач
5	Принципы построения и реализации криптографических алгоритмов	ОПК-10	Тест, решение стандартных и прикладных задач
6	Методы анализа криптографических алгоритмов	ОПК-10	Тест, решение стандартных и прикладных задач
7	Шифрование с открытым ключом	ОПК-10	Тест, решение стандартных и прикладных задач
8	Криптографические протоколы	ОПК-10	Тест, решение стандартных и прикладных задач
9	Криптосистемы на базе ПЭВМ	ОПК-10	Тест, решение стандартных и прикладных задач
10	Компьютерная стеганография	ОПК-10	Тест, решение стандартных и прикладных задач

7.3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

При преподавании дисциплины «Методы и средства криптографической защиты информации» в качестве формы оценки знаний студентов используются: тесты, решение практических задач различной сложности, выполнение курсового проекта, зачет с оценкой, экзамен.

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных и прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная:

1. Алфёров А.П. Основы криптографии: учеб. пособие / А.П. Алфёров, Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. - М.: Гелиос АРВ, 2002. - 480 с.: ил. - ISBN 5-85438-025-0
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ / В. В. Золотарев, Г. В. Овечкин. - М.: Горячая линия - Телеком, 2004. - 126 с.: ил. - ISBN 5-93517-169-4: 130-00.
3. Петраков А.В. Основы практической защиты информации / А.В. Петраков. - 4-е изд., стереотип. - М.: Радио и связь, 2005. - 384 с. - ISBN 5-256-01507-9

Дополнительная:

1. Варфоломеев А.А. Управление ключами в системах криптографической защиты банковской информации/ А.А. Варфоломеев, О.С. Домнина, М.Б. Пеленицын - М.: МИФИ, 1996. – 124 с.
2. Варфоломеев А.А. Методы криптографии и их применение в банковских технологиях/ А.А. Варфоломеев, М.Б. Пеленицын - М.: МИФИ, 1995. – 116 с.
3. Хоффман Л.Дж. Современные методы защиты информации/ под ред. Ю.Н. Мельникова - М.: Сов. Радио, 2007. - 368 с.
4. Жельников В. Криптография от папируса до компьютера/ В. Жельников - М.: АБФ, 1996. – 335 с. - ISBN 5-87484-054-0
5. К.Шеннон Работы по теории информации и кибернетике. – М.: Иностранная литература, 1963. – 832 с.
6. Радько Н.М. Основы криптографической защиты информации [Электронный ресурс]: Учеб. пособие / Н. М. Радько, А. Н. Мокроусов. - Электрон. текстовые, граф. дан. (1,04 Мб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 30-00.

Методические разработки:

1. Методические указания к практическим занятиям по дисциплине "Криптографические методы защиты информации" для студентов специальностей 090301 «Компьютерная безопасность», 090302 "Информационная безопасность телекоммуникационных систем", 090303 "Информационная безопасность автоматизированных систем" очной формы обучения [Электронный ресурс] / Каф. систем

- информационной безопасности; Сост. А. Н. Мокроусов. - Электрон. текстовые, граф. дан. (886 Мб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 00-00.
2. Радько Н.М. Защита информации в беспроводных сетях: Учеб. пособие / Н.М. Радько, А.Н. Мокроусов. Воронеж: ГОУВПО "Воронежский государственный технический университет", 2010. - 100 с.
 3. Криптографические методы обеспечения информационной безопасности [Электронный ресурс]: Методические указания к лабораторным работам по дисциплине "Средства криптографической защиты информации в радиосвязи" для студентов специальностей 090102 "Компьютерная безопасность", 090105 "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 "Информационная безопасность телекоммуникационных систем" очной формы обучения / Каф. систем информационной безопасности; Сост.: Н. М. Радько, А. Н. Мокроусов. - Электрон. текстовые, граф. дан. (780 800 байт). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2011. - 1 файл. - 00-00.
 4. Методические указания к самостоятельным работам по дисциплине «Криптографические методы защиты информации» для студентов специальностей 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост. Н.М. Радько. - Электрон. текстовые, граф. дан. (410 Мб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.
 5. Методические указания к курсовому проектированию по дисциплине "Криптографические методы защиты информации" для студентов специальности 090301 "Компьютерная безопасность" очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: Н.М. Радько, А.Н. Мокроусов. - Электрон. текстовые, граф. дан. (1026 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных

профессиональных баз данных и информационных справочных систем:

<https://old.education.cchgeu.ru>

<http://www.studentlibrary.ru/>

<http://znanium.com/>

<http://ibooks.ru/>

<http://e.lanbook.com/>

<http://www.iprbookshop.ru/>

GNU Octave – свободная система для математических вычислений

Mathworks Matlab&Simulink – среда технических
вычислений/визуального имитационного моделирования

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой.

Дисплейный класс, оснащенный компьютерными программами для проведения практических занятий.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Методы и средства криптографической защиты информации» читаются лекции, проводятся практические занятия.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

На практических занятиях проводится тестирование и решение задач в соответствии с темой занятия. Методики решения задач приведены в методических указаниях к практическим занятиям.

Большое значение по закреплению и совершенствованию знаний имеет самостоятельная работа студентов. Информацию о всех видах самостоятельной работы студенты получают на занятиях.

Контроль усвоения материала дисциплины производится проверкой выполнения тестов, практических работ и курсового проекта. Освоение дисциплины оценивается на зачете с оценкой в 8-ом семестре и на экзамене в 9-ом семестре.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий,

	словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практические занятия	Практические занятия позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности практических занятий для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомиться с соответствующим разделом учебного пособия по данной дисциплине, проработать дополнительную литературу и источники, решить задачи для самостоятельного решения из соответствующего раздела методических указаний к практическим занятиям.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоению учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом (экзаменом) три дня эффективнее всего использовать для повторения и систематизации материала.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП