МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета _____ С.М. Пасмурнов

«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Теоретико-числовые методы в криптографии»

Специальность 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация «Безопасность распределённых компьютерных систем»

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2017

Автор программы _____/Радько Н.М./

Заведующий кафедрой Систем информационной безопасности _____/Остапенко А.Г./

Руководитель ОПОП _____/ Остапенко А.Г./

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины - дать будущим инженерам, специализирующимся в области защиты информации, основы знаний о принципах защиты информации с помощью теоретико-числовых методов криптографии.

1.2. Задачи освоения дисциплины

- ознакомить студентов с математическими методами, используемыми в криптографии;
- дать студентам основы принципов анализа и синтеза криптографических шифров;
- изучение перспективных направлений и тенденций развития криптографических систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Теоретико-числовые методы в криптографии» относится к дисциплинам обязательной части блока Б1 учебного плана.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Теоретико-числовые методы в криптографии» 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:** - основные теоретико-числовые методы в криптографии и алгоритмы их реализации; - математические модели шифров, подходы к оценке их стойкости.
	Уметь: - применять математические методы при исследовании криптографических алгоритмов; - оценивать уязвимость методов защиты компьютерных систем.
	Владеть: - типовыми криптографическими методами

	организации криптографических систем защиты информации; - способностью к проведению анализа эффективности компьютерных систем.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Теоретико-числовые методы в криптографии» составляет 4 з.е.

Распределение трудоемкости дисциплины по видам занятий

Виды учебной работы	Всего часов	Семестры
		7
Контактная работа по видам занятий (всего)	108	108
В том числе:		
Лекции	36	36
Практические занятия (ПЗ)	72	72
Самостоятельная работа	36	36
Часы на контроль	-	-
Виды промежуточной аттестации		Зачет с оценкой
Общая трудоемкость час з.е.	144 4	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
7 семестр						
1	Основные целочисленные алгоритмы	Группы. Кольца. Поля. Подгруппы и факторгруппы. Векторные пространства и линейные алгебры. Матрицы. Сложность основных целочисленных алгоритмов в кольце целых чисел, кольцах вычетов и конечных полях Дискретное преобразование Фурье для кольца целых чисел.	6	12	6	24
2	Квадратичные вычеты и невычеты, квадратичный закон взаимности Гаусса	Идеалы, классы вычетов и кольцо классов вычетов. Идеалы и классы вычетов целых чисел. Идеалы многочленов и классы вычетов. Алгебра классов вычетов многочленов. Поля Галуа. Структура конечных полей. Векторные подпространства и линейные преобразования конечных полей. Цепные дроби.	6	12	6	24
3	Асимптотический закон распределения простых чисел	Проверка чисел на простоту. Построение больших простых чисел. Модулярная арифметика. Простые числа. Обратные значения по модулю. Малая теорема Ферма. Функция Эйлера. Тест Соловея-Штрассена.	6	12	6	24

		Тест Леманна. Тест Рабина-Миллера. Сильные простые числа.				
4	Методы разложения чисел на множители	Алгоритмы дискретного логарифмирования в конечном поле. Линейное решето. Схема целых чисел Гаусса. Решето числового поля. Дискретные логарифмы мультипликативной группы полей простых чисел. Дискретные логарифмы мультипликативной группы конечных полей характеристики 2. Дискретные логарифмы группы эллиптических кривых над конечными полями.	6	12	6	24
5	Криптографическая система RSA	Аппаратные реализации RSA. Скорость работы RSA. Программные ускорители. Стойкость RSA. Взлом RSA на основе подобранного шифртекста. Атака при использовании общего модуля. Раскрытие малого открытого показателя. Раскрытие малого секретного показателя. Полученные уроки. Атаки зашифрование и подпись.	6	12	6	24
6	Протокол Диффи-Хеллмана	Алгоритм Диффи-Хеллмана с трёмя и более участниками. Расширенный алгоритм Диффи-Хеллмана. Алгоритм Хьюза. Обмен ключей без обмена ключами.	6	12	6	24
		Итого	**36**	**72**	**36**	**144**

5.2 Перечень практических занятий

7 семестр

1. Матрицы – 4 ч.
2. Дискретное преобразование Фурье для кольца целых чисел – 8 ч.
3. Алгебра классов вычетов многочленов – 8 ч.
4. Цепные дроби – 8 ч.
5. Модулярная арифметика – 8 ч.
6. Решето – 4 ч.
7. Дискретные логарифмы – 8 ч.
8. Атака при использовании общего модуля – 8 ч.
9. Атаки зашифрование и подпись – 8 ч.
10. Алгоритм Хьюза – 8 ч.

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

Учебным планом по дисциплине «Теоретико-числовые методы в криптографии» не предусмотрено выполнение курсового проекта (работы).

Предусмотрено выполнение контрольных работ по следующим темам:

- Сложность основных целочисленных алгоритмов в кольце целых чисел, кольцах вычетов и конечных полях;
- Идеалы, классы вычетов и кольцо классов вычетов;
- Поля Галуа;
- Проверка чисел на простоту;
- Алгоритмы дискретного логарифмирования в конечном поле;

- Дискретные логарифмы мультипликативной группы полей простых чисел;
- Тест Соловея-Штрассена;
- Алгоритм Диффи-Хеллмана с трёмя и более участниками.

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».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-10	**Знать:** - основные теоретико-числовые методы в криптографии и алгоритмы их реализации; - математические модели шифров, подходы к оценке их стойкости.	Тест	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: - применять математические методы при исследовании криптографических алгоритмов; - оценивать уязвимость методов защиты компьютерных систем.	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: - типовыми криптографическими методами организации криптографических систем защиты информации; - способностью к проведению анализа эффективности компьютерных систем.	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

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

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	**Результаты обучения,, характеризующие сформированность компетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл**	**Неудовл**
ОПК-10	**Знать:** - основные теоретико-числовые методы в криптографии и алгоритмы их реализации; - математические модели шифров, подходы к оценке их стойкости.	знание учебного материала и использование учебного материала в процессе выполнения заданий	Студент демонстрирует полное понимание учебного материала. Студент демонстрирует ярко выраженную способность использовать знания, умения, навыки в процессе выполнения заданий	Студент демонстрирует значительное понимание материала. Студент демонстрирует способность использовать знания, умения, навыки в процессе выполнения заданий	Студент демонстрирует частичное понимание материала. Способность студента продемонстрировать знание, умение, навык выражена слабо	1. Студент демонстрирует незначительное понимание материала. 2. Студент демонстрирует непонимание заданий. 3. У студента нет ответа. Не было попытки выполнить задания.
	Уметь: применять математические методы при исследовании криптографических алгоритмов; - оценивать уязвимость методов защиты компьютерных систем.	умение использовать учебный материал в процессе выполнения практических работ				
	Владеть: - типовыми криптографическими методами организации криптографических систем защиты информации; - способностью к проведению анализа эффективности компьютерных систем.	применение учебного материала при решении практических задач				

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

(минимум 10 вопросов для тестирования с вариантами ответов)

1) По способу использования средств шифрования информации различают:

- **поточное и блочное симметричное шифрование**
- симметричное и несимметричное
- канальное шифрование и оконечное (абонентское) шифрование.
- односторонней и взаимной идентификации

2) Вскрытие (взламывание) шифра это:

- преобразование шифрованного сообщения в защищаемую информацию с помощью определенных правил, содержащихся в шифре
- **процесс получения защищаемой информации из шифрованного сообщения без знания примененного шифра**
- преобразование защищаемой информации в шифрованное сообщение с помощью определенных правил, содержащихся в шифре
- наука о способах преобразования информации с целью ее защиты от незаконных пользователей

3) Основными видами криптографического закрытия являются:

- замена (подстановка), перестановка, гаммирование защищаемых данных
- дешифрование и кодирование защищаемых данных
- **шифрование и кодирование защищаемых данных**
- шифрование и дешифрование защищаемых данных

4) Основной характеристикой меры защищенности информации криптографическим закрытием является:

- **стойкость шифра**
- структура шифра
- распад шифра
- совершеннность шифра

5) Что понимается под аутентификацией информации:

- **установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от источника этой информации, установление законным получателем (возможно арбитром) факта, что полученная информация наиболее вероятно была передана законным отправителем (источником) и что она при этом не заменена и не искажена**
- установление подлинности личности пользователя сети, которому требуется доступ к защищаемой информации или необходимо подключиться к сети
- установление подлинности сети, к которой получен доступ
- установление факта, что данный массив не был изменен в течение времени, когда он был вне посредственного контроля, а также решение вопросов об авторстве этого массива данных

6) Аутентификация сети это:

- установление подлинности личности пользователя сети, которому требуется доступ к защищаемой информации или необходимо подключиться к сети
- установление подлинности содержания полученного по каналам связи сообщения и решение вопросов об авторстве сообщения.
- **установление подлинности сети, к которой получен доступ**
- установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от источника этой информации

7) Что понимается под аутентификацией хранящихся массивов программ и данных:

- установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от источника этой информации, установление законным получателем (возможно арбитром) факта, что полученная информация наиболее вероятно была передана законным отправителем (источником) и что она при этом не заменена и не искажена
- установление подлинности личности пользователя сети, которому требуется доступ к защищаемой информации или необходимо подключиться к сети
- установление подлинности сети, к которой получен доступ
- **установление факта, что данный массив не был изменен в течение времени, когда он был вне посредственного контроля, а также решение вопросов об авторстве этого массива данных**

8) Аутентификация пользователя сети это:

- **установление подлинности личности пользователя сети, которому требуется доступ к защищаемой информации или необходимо подключиться к сети**
- установление подлинности содержания полученного по каналам связи сообщения и решение вопросов об авторстве сообщения
- установление подлинности сети, к которой получен доступ
- установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от источника этой информации

9) Цифровая подпись обеспечивает:

- скрытие содержания сообщения
- **аутентификацию источника данных**
- **целостность сообщения**
- **юридическую значимость сообщения**

10) Имитозащита обеспечивает:

- **целостность сообщения в соответствии со свойствами контрольной суммы.**
- формировании контрольной суммы (имитовставки, кода аутентификации сообщения) по криптоалгоритму, добавляемой к сообщению
- разработку пакета программных средств обеспечения юридической значимости лицензий посредством цифровой подписи
- проверку получателем документа и независимой третьей стороной (арбитром) и обеспечением аутентификации создателя подписи

7.2.2 Примерный перечень заданий для решения стандартных задач

1) Функция *f* называется честной, если существует полином *q* такой, что:
- $n>q(m(n))$, для всех n.
- **$n<q(m(n))$, для всех n.**
- $n \geq <q(m(n))$, для всех n.
- $n \leq q(m(n))$, для всех n.

2) В работе . . . предложен общий метод доказательства необходимости односторонних функций для существования стойких криптографических схем различных типов.
- **Импальяццо и Луби**
- Импальяццо, Левин и Луби
- Импальяццо
- Импальяццо и Рудиха

3) Самая важная характеристика генератора псевдослучайных чисел это:
- возможное число ключей системы
- степень секретности данных
- получения псевдослучайных чисел
- **информационная длина периода**

4) Один из наиболее простых способов комбинации двух сдвиговых регистров с линейными обратными связями состоит в применении переключателя с отношением переключаемых разрядов 2:1 и носит имя:
- генератор Дженнинга
- **генератор Джеффи**
- критерий Вейля
- тест Миллера-Рабина

5) Один из наиболее известных протоколов идентификации с нулевым разглашением (Zero-knowledge protocol). Надежность алгоритма основывается на сложности вычисления дискретного логарифма. Данный алгоритм позволяет проводить предварительные вычисления, что удобно при малых вычислительных ресурсах.
- **схема Шнорра**
- схема Фиата-Шамира
- схема Гиллу-Кискатра
- Схема Эль-Гамаля

6) Семейство $\{H_n\}$ называется семейством односторонних хэш-функции, если для любого такого алгоритма *B,* для любого полинома *P* и для всех достаточно больших n
- $Pr\{B(h\} = y : y \in \Sigma^n, y = x \& h(x) = h(y)\} < 1/P(n)$
- $Pr\{B(h\} = y : y \in \Sigma^n, y \neq x \& h(x) \neq h(y)\} < 1/P(n)$
- $Pr\{B(h\} = y : y \in \Sigma^n, y \neq x \& h(x) = h(y)\} > 1/P(n)$
- **$Pr\{B(h\} = y : y \in \Sigma^n, y \neq x \& h(x) = h(y)\} < 1/P(n)$**

7) Кто построил семейство односторонних хэш-функции, исходя из предположения о существовании односторонней перестановки:
- Ромпель
- Наор

- Юнг
- **Наор и Юнг**

8) Способ преобразования протокола аутентификации в схему электронной подписи путем замены случайного запроса неким «суррогатом» предложили:
- Наор и Юнг
- **Фиат и Шамир**
- Шнорр
- Ромпель

9) . . . предназначена для встраивания в прикладное программное обеспечение, в результате чего к функциям ПО добавляются возможности шифрования файлов и областей оперативной памяти, формирования и проверки электронной цифровой подписи в соответствии с российскими стандартами ГОСТ Р 34.10-94, ГОСТ Р 34.11-94, ГОСТ 28147-89.
- **Верба-U**
- Верба-W
- Верба-O
- Кулон-1

10) Под управлением какой операционной системы функционирует СКЗИ «Верба-U»:
- MS WINDOWS 3.1, 3.11
- Mac OS
- **UNIX**
- MS DOS 5.0

7.2.3 Примерный перечень заданий для решения прикладных задач

1) Какие криптосистемы используются для формирования цифровой подписи и шифрования (формирования) симметричных ключей при их рассылке по каналам связи:
- симметричные
- **несимметричные**
- блочные подстановки перестановки гаммирование
- Эль-Гамаля Ривестра-Шамира-Эйделмана Меркля-Хеллмана и Хора-Ривестра

2) Стандарт доступа и управления передачей файлов FTAM (File Transfer Access and Management) определяющий все необходимые правила работы с файлами:
- Triple-DES
- Advanced Encryption Standard (AES)
- OpenPGP
- **ISO-OSI**

3) Стандарт ISO 8571, протокол прикладного уровня OSI для передачи, доступа и управления файлами:
- SMB
- NFS
- **FTAM**
- Andrew File System

4) Процесс преобразования открытого текста в шифртекст с использованием ключа это:
- алгоритм шифрования
- **зашифрование**

- расшифрование
- дешифрование

5) Под управлением какой операционной системы функционирует СКЗИ «Верба-OU»:
- WINDOWS 3.1,-3.11, WINDOWS-95
- Mac OS
- **UNIX**
- MS DOS 5.0

6) Генерирование нового ключа из предыдущего значения ключа с помощью односторонней (однонапрвленной) функции это:
- ключевая информация
- управление ключами
- **модификация ключа**
- функция хранения ключей

7) Иерархия ключей может быть:
- одноуровневой, двухуровневой
- **двухуровневой, трёхуровневой**
- трёхуровневой, четырехуровневой
- трёхуровневой

8) Последовательность шагов, которые предпринимают две или более сторон для совместного решения некоторой задачи это
- **протокол**
- ключ
- шифр
- код

9) СКЗИ «Верба-О» решает следующие задачи:
- **осуществляет шифрование/дешифрование информации на уровне файлов и блоков памяти**
- **производит обнаружение искажений, вносимых злоумышленниками или вирусами в защищаемую информацию**
- генерацию ключей электронной цифровой подписи (ЭЦП), ключей шифрования;
- проверку ЭЦП
- **формирование и проверку ЭЦП на уровне файлов и блоков памяти**

10) СКЗИ «Верба-U» имеет сертификат:
- ФАПСИ № СФ/114-0005 от 14.04.1996 г.
- ФАПСИ № СФ/114-0178 от 10 апреля 1998 г.
- ФАПСИ № СФ/114-0176 от 10 апреля 1997 г.
- **ФАПСИ № СФ/114-0175 от 10 апреля 1997 г.**

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Группы. Кольца.
2. Поля.
3. Подгруппы и факторгруппы.
4. Векторные пространства и линейные алгебры.

5. Матрицы.
6. Сложность основных целочисленных алгоритмов в кольце целых чисел, кольцах вычетов и конечных полях
7. Дискретное преобразование Фурье для кольца целых чисел.
8. Идеалы, классы вычетов и кольцо классов вычетов.
9. Идеалы и классы вычетов целых чисел.
10. Идеалы многочленов и классы вычетов.
11. Алгебра классов вычетов многочленов.
12. Поля Галуа.
13. Структура конечных полей.
14. Векторные подпространства и линейные преобразования конечных полей.
15. Цепные дроби.
16. Проверка чисел на простоту.
17. Построение больших простых чисел.
18. Модулярная арифметика.
19. Простые числа.
20. Обратные значения по модулю.
21. Малая теорема Ферма. Функция Эйлера.
22. Тест Соловея-Штрассена.
23. Тест Леманна. Тест Рабина-Миллера.
24. Сильные простые числа.
25. Методы разложения чисел на множители
26. Алгоритмы дискретного логарифмирования в конечном поле.
27. Линейное решето.
28. Схема целых чисел Гаусса.
29. Решето числового поля.
30. Дискретные логарифмы мультипликативной группы полей простых чисел.
31. Дискретные логарифмы мультипликативной группы конечных полей характеристики
32. Дискретные логарифмы группы эллиптических кривых над конечными полями.
33. Аппаратные реализации RSA.
34. Скорость работы RSA.
35. Программные ускорители.
36. Стойкость RSA. Взлом RSA на основе подобранного шифртекста.
37. Атака при использовании общего модуля.
38. Раскрытие малого открытого показателя.
39. Раскрытие малого секретного показателя.
40. Полученные уроки. Атаки зашифрование и подпись.
41. Алгоритм Диффи-Хеллмана с трёмя и более участниками.
42. Расширенный алгоритм Диффи-Хеллмана.
43. Алгоритм Хьюза.
44. Обмен ключей без обмена ключами.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Оценивание может осуществляться либо на основе тестирования, либо путем ответа на вопросы экзаменационного билета.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Основные целочисленные алгоритмы	ОПК-10	Контрольная работа, решение практических задач
2	Квадратичные вычеты и невычеты, квадратичный закон взаимности Гаусса	ОПК-10	Контрольная работа, решение практических задач
3	Асимптотический закон распределения простых чисел	ОПК-10	Контрольная работа, решение практических задач
4	Методы разложения чисел на множители	ОПК-10	Контрольная работа, решение практических задач
5	Криптографическая система RSA	ОПК-10	Контрольная работа, решение практических задач
6	Протокол Диффи-Хеллмана	ОПК-10	Контрольная работа, решение практических задач

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

При преподавании дисциплины «Теоретико-числовые методы в криптографии» в качестве формы оценки знаний студентов используются: контрольные работы, решение практических задач различной сложности, зачет с оценкой в 7-ом семестре.

Контрольные работы выполняется в письменном виде, либо при помощи компьютерной системы ответов на вопросы. Время выполнения контрольной работы - 45 мин. Затем осуществляется проверка преподавателем 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. Выполнение практических заданий осуществляется согласно учебного плана в соответствии с «Методическими

указаниями по выполнению практических заданий…».

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная:

1. Маховенко Е.Б. Теоретико-числовые методы в криптографии: учеб. пособие / Е.Б. Маховенко - М.: Гелиос АРВ, 2006. - 320 с.: ил . - ISBN 5-85438-143-5
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 5-94365-012-5: 130-00.
3. Ростовцев А.Г. Теоретическая криптография / А.Г. Ростовцев, Е.Б. Маховенко - СПб.: Профессионал, 2005. - 480 с. - ISBN 5-256-01507-9

Дополнительная:

1. Бутакова Н.Г. Криптографические методы и средства защиты информации: учебное пособие / Н.Г. Бутакова, Н.В. Федоров. - Санкт-Петербург: Интермедия, 2020. - 380 с. - ISBN 978-5-4383-0210-0. - Текст: электронный // Лань: электронно-библиотечная система.
2. Рацеев С.М. Математические методы защиты информации: учебное пособие для вузов / С.М. Рацеев. - Санкт-Петербург : Лань, 2022. - 544 с. - ISBN 978-5-8114-8589-5. - Текст: электронный // Лань: электронно-библиотечная система.
3. Басалова Г.В. Основы криптографии: учебное пособие / Г.В. Басалова. - 2-е изд. - Москва : ИНТУИТ, 2016. - 282 с. - Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/100302
4. Хоффман Л.Дж. Современные методы защиты информации/ под ред. Ю.Н. Мельникова - М.: Сов. Радио, 2007. - 368 с.

Методические разработки:

1. Радько Н. М. Основы криптографической защиты информации: учеб. пособие [Электронный ресурс]. – Электрон. текстовые, граф. данные (1,04 Мб) / Н. М. Радько, А. Н. Мокроусов. – Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2014. – 1 электрон. опт. диск (CD-ROM).
2. Радько Н.М. Математические методы в криптографии [Электронный

ресурс] : учеб. пособие / Н. М. Радько, А. Н. Мокроусов. - Электрон. дан. (1 файл :4 763 648 байта). - Воронеж: ГОУВПО "Воронежский государственный технический университет", 2006. - 1 дискета. - 30-00.

3. Криптографические методы обеспечения информационной безопасности. Методические указания к практическим занятиям по дисциплине "Криптографические методы и средства ИБ" для студентов специальностей 090102 “Компьютерная безопасность”, 090105 “Комплексное обеспечение информационной безопасности автоматизированных систем”, 090106 “Информационная безопасность телекоммуникационных систем” очной формы обучения/ Воронеж. гос. техн. ун-т; Сост. Н.М. Радько, А Н. Мокроусов. Воронеж, 2011. - 36 с.
4. Методические указания к самостоятельным работам по дисциплине «Теоретико-числовые методы в криптографии» для студентов специальности 090301 «Компьютерная безопасность» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост. Н. М. Радько. - Электрон. текстовые, граф. дан. (405 Мб). - 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:

http://www.eios.vorstu.ru (электронная информационно-обучающая система ВГТУ)

http://e.lanbook.com/ (ЭБС Лань)

http://znanium.com/ (ЭБС Знаниум)

http://IPRbookshop.ru/ (ЭБС IPRbooks (Айбукс))

http://urait.ru/ (Образовательная платформа «Юрайт»)

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 «Теоретико-числовые методы в криптографии» 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 решение стандартных и прикладных 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 контрольных работ и практических занятий. Освоение дисциплины оценивается на дифференцированном зачете 7-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 удается 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, ознакомится 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 усвоения 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 экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.