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 2016

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. Цель 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

- дать студентам основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами, на основе применения криптографических методов;
- дать студентам основы принципов анализа и синтеза шифров;
- ознакомить студентов с математическими методами, используемыми в криптографии;
- разработка математических моделей защищаемых процессов и средств защиты;
- информации и систем, обеспечивающих информационную безопасность;
- обоснование и выбор рационального решения по уровню обеспечения
- защищенности компьютерной системы с учетом заданных требований;
- подготовка научно-технических отчетов, обзоров, публикаций по результатам;
- выполненных исследований;
- выполнение экспериментально-исследовательских работ при проведении
- сертификации средств защиты и анализ результатов;
- проведение аттестации технических средств, программ, алгоритмов на предмет;
- соответствия требованиям защиты информации по соответствующим классам;
-
- безопасности или профилям защиты

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

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

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Теоретико-числовые методы в криптографии» направлен на формирование следующих компетенций:

ОПК-2 - способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов

ОПК-10 - способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах

ПК-5 - способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации

ПК-10 - способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**
ОПК-2	**Знать:** - основные средства криптографического анализа.
	Уметь: - использовать свойства криптографических средств при анализе комплексных систем защиты информации.
	Владеть: - алгоритмами дискретного логарифмирования.
ОПК-10	**Знать:** - основные теоретико-числовые методы в криптографии и алгоритмы их реализации.
	Уметь: - применять теоретико-числовые методы в криптографии.
	Владеть: - способностью к проведению анализа эффективности компьютерных систем.
ПК-5	**Знать:** - основные целочисленные алгоритмы, закон распределения простых чисел.
	Уметь: - использовать теоретико-числовые методы криптографии при анализе комплексных систем защиты информации.
	Владеть: - алгоритмами дискретного логарифмирования, методами разложения чисел на множители.
ПК-10	**Знать:** - современные тенденции развития средств и методов криптографической защиты информации.
	Уметь: - оценивать уязвимость методов защиты компьютерных систем.
	Владеть: - типовыми криптографическими методами организации криптографических систем защиты информации.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Теоретико-числовые методы в криптографии» составляет 5 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		9
Аудиторные занятия (всего)	72	72
В том числе:		
Лекции	36	36
Практические занятия (ПЗ)	36	36
Самостоятельная работа	72	72
Часы на контроль	36	36
Виды промежуточной аттестации - экзамен	+	+
Общая трудоемкость: академические часы зач.ед.	 180 5	 180 5

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Практ зан.	СРС	Всего, час
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	6	12	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	6	12	24
3	Асимптотический закон	Проверка чисел на простоту. Построение больших	6	6	12	24

	распределения про-стых чисел	простых чисел. Модулярная арифметика. Простые числа. Обратные значения по модулю. Малая теорема Ферма. Функция Эйлера. Тест Соловея-Штрассена. 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 Дискретные логарифмы группы эллиптических кривых над конечными полями.	6	6	12	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	6	12	24
6	Протокол Диффи-Хеллмана	Алгоритм Диффи-Хеллмана с трѐмя и более участниками. Расширенный алгоритм Диффи-Хеллмана. Алгоритм Хьюза. Обмен ключей без обмена ключами.	6	6	12	24
Итого			**36**	**36**	**72**	**144**

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 не предусматривает выполнение курсового проекта (работы) или контрольной работы.

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-2	**Знать:** - основные средства криптографического анализа.	знание основных средств криптографического анализа.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: - использовать свойства криптографических средств при анализе комплексных систем защиты информации.	умение использовать свойства криптографических средств при анализе комплексных систем защиты информации.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: - алгоритмами дискретного логарифмирования.	владение алгоритмами дискретного логарифмирования.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-10	**Знать:** - основные теоретико-числовые методы в криптографии и алгоритмы их реализации.	знание основных теоретико-числовых методов в криптографии и алгоритмы их реализации.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: - применять теоретико-числовые методы в криптографии.	умение применять теоретико-числовые методы в криптографии.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: - способностью к проведению анализа эффективности компьютерных систем.	владение способностью к проведению анализа эффективности компьютерных систем.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-5	**Знать:** - основные целочисленные алго-	знание основных целочисленных алгоритмов, закон распределения	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих про-

	ритмы, закон распределения простых чисел.	простых чисел.		граммах
	Уметь: - использовать теоретико-числовые методы криптографии при анализе комплексных систем защиты информации.	умение использовать теоретико-числовые методы криптографии при анализе комплексных систем защиты информации.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: - алгоритмами дискретного логарифмирования, методами разложения чисел на множители.	владение алгоритмами дискретного логарифмирования, методами разложения чисел на множители.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-10	**Знать:** - современные тенденции развития средств и методов криптографической защиты информации.	знание современных тенденций развития средств и методов криптографической защиты информации.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: - оценивать уязвимость методов защиты компьютерных систем.	умение оценивать уязвимость методов защиты компьютерных систем.	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.	владение типовыми криптографическими методами организации криптографических систем защиты информации.	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 9 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-2	**Знать:** - основные средства криптографического анализа.	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Уметь:	Решение	Задачи ре-	Продемонстр	Продемонстр	Задачи не

	- использовать свойства криптографических средств при анализе комплексных систем защиты информации.	стандартных практических задач	шены в полном объеме и получены верные ответы	ирован верный ход решения всех, но не получен верный ответ во всех задачах	ирован верный ход решения в большинстве задач	решены
	Владеть: - алгоритмами дискретного логарифмирования.	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
ОПК-10	**Знать:** - основные теоретико-числовые методы в криптографии и алгоритмы их реализации.	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Уметь: - применять теоретико-числовые методы в криптографии.	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: - способностью к проведению анализа эффективности компьютерных систем.	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
ПК-5	**Знать:** - основные целочисленные алгоритмы, закон распределения простых чисел.	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Уметь: - использовать теоретико-числовые методы криптографии при анализе комплексных систем защиты информации.	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: - алгоритмами дискретного логарифмирования, методами разложения чисел на множители.	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	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

				задачах		
ПК-10	**Знать:** - современные тенденции развития средств и методов 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: - оценивать уязвимость методов защиты компьютерных систем.	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: - типовыми криптографическими методами организации криптографических систем защиты информации.	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.Как называется натуральное число, которое не имеет делителей, кроме самого себя и единицы?

простое число +

составное число

каноническое число

криптографическое число

2. Как называется натуральное число, которое делится, помимо самого себя и единицы, еще хотя бы на одно число?

простое число

составное число +

каноническое число

криптографическое число

3. Как называются числа, не имеющие общих делителей кроме единицы?

взаимно простые числа +

числа Эйлера

канонические числа

криптографические числа

4. Выберите вариант ответа, содержащий только взаимно простые числа

3, 5, 19, 38

4, 7, 15, 59 +

5, 9, 27, 54

7, 27, 77, 147

5. Выберите вариант ответа, содержащий только взаимно простые числа

5, 19, 49, 64 +

5, 7, 15, 58

5, 9, 27, 54

7, 27, 77, 147

6. Определите число натуральных чисел, не превосходящих 33 и взаимно простых с 33. Ответ: 20

7. Определите число натуральных чисел, не превосходящих 53 и, взаимно простых с 53. Ответ: 52

8. Определите наибольший общий делитель чисел 133 и 171. Ответ: 19

9. Алгоритмы шифрования с открытым ключом по-другому называются

асимметричными алгоритмами шифрования +

симметричными алгоритмами шифрования

односторонними алгоритмами шифрования

помехоустойчивыми алгоритмами шифрования

10. Асимметричные алгоритмы шифрования по-другому называются

алгоритмами шифрования с открытым ключом +

симметричными алгоритмами шифрования

односторонними алгоритмами шифрования

помехоустойчивыми алгоритмами шифрования

7.2.2 Примерный перечень заданий для решения стандартных задач

ОПК-2 - способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов
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.
ОПК-10 - способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах
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.
ПК-5 - способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
24. Методы разложения чисел на множители 25. Алгоритмы дискретного логарифмирования в конечном поле. 26. Линейное решето. 27. Схема целых чисел Гаусса. 28. Решето числового поля. 29. Дискретные логарифмы мультипликативной группы полей простых чисел. 30. Дискретные логарифмы мультипликативной группы конечных полей характеристики 31. Дискретные логарифмы группы эллиптических кривых над конечными полями. 32. Аппаратные реализации RSA. 33. Скорость работы RSA. 34. Программные ускорители.
ПК-10 - способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
35. Стойкость RSA. Взлом RSA на основе подобранного шифртекста. 36. Атака при использовании общего модуля. 37. Раскрытие малого открытого показателя. 38. Раскрытие малого секретного показателя. 39. Полученные уроки. Атаки зашифрование и подпись. 40. Алгоритм Диффи-Хеллмана с трёмя и более участниками. 41. Расширенный алгоритм Диффи-Хеллмана. 42. Алгоритм Хьюза. 43. Обмен ключей без обмена ключами.

7.2.3 Примерный перечень заданий для решения прикладных задач

ОПК-2 - способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов	
1	Функция *f* называется честной, если существует полином *q* такой, что: o $n>q(m(n))$, для всех n. o **$n<q(m(n))$, для всех n.** o $n \geq <q(m(n))$, для всех n. o $n \leq q(m(n))$, для всех n.
2	Семейство $\{H_n\}$ называется семейством односторонних хэш-функции, если для любого такого алгоритма *B,* для любого полинома *P* и для всех достаточно больших *n* o $Pr\{B(h\} = y : y \in \Sigma^n, y = x \& h(x) = h(y)\} < 1/P(n)$

	o $Pr\{B(h\} = y : y \in \Sigma^n, y \neq x \& h(x) \neq h(y)\} < 1/P(n)$ o $Pr\{B(h\} = y : y \in \Sigma^n, y \neq x \& h(x) = h(y)\} > 1/P(n)$ o **$Pr\{B(h\} = y : y \in \Sigma^n, y \neq x \& h(x) = h(y)\} < 1/P(n)$**
3	Алгоритм, позволяющий двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищённый от подмены, канал связи. Этот ключ может быть использован для шифрования дальнейшего обмена с помощью алгоритма симметричного шифрования: o метод цифрового конверта o метода Эль-Гамаля o **Диффи-Хеллмана** o RSA
ОПК-10 - способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	
1	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. o **схема Шнорра** o схема Фиата-Шамира o схема Гиллу-Кискатра o Схема Эль-Гамаля
2	Самая важная характеристика генератора псевдослучайных чисел это: o возможное число ключей системы o степень секретности данных o получения псевдослучайных чисел o **информационная длина периода**
3	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: o генератор Дженнинга o **генератор Джеффи** o критерий Вейля o тест Миллера-Рабина
ПК-5 - способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	
1	Основной характеристикой меры защищенности информации криптографическим закрытием является: o **стойкость шифра** o структура шифра

	o распад шифра o совершеннность шифра
2	В работе . . . предложен общий метод доказательства необходимости односторонних функций для существования стойких криптографических схем различных типов. o **Импальяццо и Луби** o *Импальяццо*, Левин и Луби o *Импальяццо* o Импальяццо и Рудиха
3	Кто построил семейство односторонних хэш-функции, исходя из предположения о существовании односторонней перестановки: o Ромпель o Наор o Юнг o **Наор и Юнг**
ПК-10 - способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	
1	. . . 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. o **Верба-U** o Верба-W o Верба-О o Кулон-1
2	СКЗИ «Верба-О» решает следующие задачи: o **осуществляет шифрование/дешифрование информации на уровне файлов и блоков памяти** o **производит обнаружение искажений, вносимых злоумышленниками или вирусами в защищаемую информацию** o генерацию ключей электронной цифровой подписи (ЭЦП), ключей шифрования; o проверку ЭЦП o **формирование и проверку ЭЦП на уровне файлов и блоков памяти**
3	Система криптографической защиты информации **. . .** используется для защиты информации конфиденциального характера в системах банк-клиент, автоматизированной бухгалтерии, торговых, клиринговых комплексах и др. o Верба-U o Верба-W

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

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень заданий для решения прикладных задач

1.Основные целочисленные алгоритмы

2.Квадратичные вычеты и невычеты, квадра-тичный закон взаимности Гаусса.

3.Асимптотический закон распределения про-стых чисел

4.Методы разложения чисел на множители

5.Криптографическая система RSA

6.Протокол Диффи-Хеллмана

7.Группы. Кольца. Поля. Подгруппы и факторгруппы. Векторные пространства и линейные алгебры. Матрицы.

8.Сложность основных целочисленных алгоритмов в кольце целых чисел, кольцах вычетов и конечных полях Дискретное преобразование Фурье для кольца целых чисел.

9.Идеалы, классы вычетов и кольцо классов вычетов. Идеалы и классы вычетов целых чисел. Идеалы многочленов и классы вычетов. Алгебра классов вычетов многочленов.

10.Поля Галуа. Структура конечных полей. Векторные подпространства и линейные преобразования конечных полей. Цепные дроби.

11.Проверка чисел на простоту. Построение больших простых чисел. Моду¬лярная арифметика. Простые числа. Обратные значения по модулю. Малая теорема Ферма. Функция Эйлера.

12.Тест Соловея-Штрассена. Тест Леманна. Тест Рабина-Миллера. Сильные простые числа.

13.Алгоритмы дискретного логарифмирования в конечном поле. Линейное решето. Схема целых чисел Гаусса. Решето числового поля.

14.Дискретные логарифмы мультипликативной группы полей простых чисел. Дискретные логарифмы мультипликативной группы конечных полей характеристики

15. Дискретные логарифмы группы эллиптических кривых над конечными полями.

16.Аппаратные реализации RSA. Скорость работы RSA. Программные ускорители. Стойкость RSA. Взлом RSA на основе подобранного шифртекста. Атака при использовании общего модуля.

17.Раскрытие малого открытого показателя. Раскрытие малого секретного показателя. Полученные уроки. Атаки зашифрование и подпись

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

(Например: Экзамен проводится 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 целочисленные алгоритмы	ОПК-2, ОПК-10, ПК-5, ПК-10	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
2	Квадратичные вычеты и невычеты, квадратичный закон взаимности Гаусса.	ОПК-2, ОПК-10, ПК-5, ПК-10	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
3	Асимптотический закон распределения простых чисел	ОПК-2, ОПК-10, ПК-5, ПК-10	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
4	Методы разложения чисел на множители	ОПК-2, ОПК-10, ПК-5, ПК-10	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
5	Криптографическая система RSA	ОПК-2, ОПК-10, ПК-5, ПК-10	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
6	Протокол Диффи-Хеллмана	ОПК-2, ОПК-10, ПК-5, ПК-10	Тест, контрольная работа, защита лабораторных

			работ, защита реферата, требования к курсовому проекту….

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

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 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.

Решение 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. Радько Н.М. Математические методы в криптографии [Электронный ресурс] : учеб. пособие. - Электрон. дан. (1 файл :4 763 648 байта). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2006. - 1 дискета. - 30-00.

2. Радько Н.М. Криптографические протоколы [Электронный ресурс] : учеб. пособие. - Электрон. дан. (1 файл :770 560 байта). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2006. - 1 дискета. - 30-00.

Дополнительная

Теоретико-числовые методы в криптографии [Электронный ресурс]: учебное пособие/ — Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2017.— 107 с.— Режим доступа: http://www.iprbookshop.ru/75601.html

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:

1. Нестеренко А.Ю. Теоретике-числовые методы в криптографии: учебное пособие. Моск, гос. ин-т. электроники и математики. 2012, 224 с. https://miem.hse.ru/data/2012/12/09/1300531528/xntheory-fixed%20version.pdf

2. Теоретико-числовые методы криптографии : учебное пособие / В.Т. Еременко, А. П. Фисун, М. Ю. Рытов, В. А. Шкаберин, С. А. Шпичак ; под общ. ред. В. Т. Еременко. – Орѐл: ОГУ имени И. С. Тургенева, 2019. – 162 с. http://elib.oreluniver.ru/uchebniki-i-uch-posobiya/teoretiko-chislovye-metody-kriptografii.html

3. RSA: от простых чисел до электронной подписи https://habr.com/ru/post/534014/

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.

Практические занятия направлены на приобретение следующие практических навыков.

Неделя семестра	Тема и содержание практического занятия	Объем часов	В том числе, в интерактивной форме	Виды контроля
1-2	Матрицы	3	1	
3-4	Дискретное преобразование Фурье	3	1	
5-6	Алгебра классов вычетов многочленов	3	1	
7-8	Цепные дроби	3	1	
9-10	Модулярная арифметика	4	1	

13-14	Тесты	2	1	Контр. раб.
15	Решето	3	1	
16	Дискретные логарифмы	4		
1	Атака при использовании общего мо-	3	1	
2	Атаки зашифрование и подпись	3		
3	Алгоритм Хьюза	3		
Итого часов		**34**	**8**	

Занятия проводятся путем решения конкретных задач в аудитории.

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.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
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.