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

«Криптографические методы защиты информации»

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. Цели дисциплины дать будущим инженерам, специализирующимся в области защиты информации, основы 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;
- дать студентам основы принципов анализа и синтеза шифров;
- ознакомить студентов с математическими методами, используемыми в криптографии;

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Криптографические методы защиты информации» относится к дисциплинам базовой части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Криптографические методы защиты информации» 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

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

ПК-18 - способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, 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:** - об основных методах и средствах криптографического анализа.
	Уметь: - оценивать уязвимость протоколов и интерфейсов компьютерных систем.
	Владеть: - типовыми криптографическими протоколами и их криптографическими качествами.
ПК-5	**Знать:** - о принципиальных подходах к созданию современных технических средств криптографической защиты информации.
	Уметь: - строить математические модели шифров и открытых текстов.
	Владеть: - основными требованиями, предъявляемыми к системам криптографической защиты информации с учетом возможных угроз.
ПК-10	**Знать:** - о методах и критериях оценки надежности защиты информации.
	Уметь: - использовать свойства криптографических средств при анализе комплексных систем защиты информации.
	Владеть: - Типовыми методами создания сетей засекреченной связи.
ПК-18	**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 «Криптографические методы защиты информации» составляет 6 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		8	9
Аудиторные занятия (всего)	126	54	72
В том числе:			
Лекции	54	18	36
Практические занятия (ПЗ)	72	36	36
Самостоятельная работа	54	18	36
Курсовой проект	+		+
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость: академические часы зач.ед.	 216 6	 72 2	 144 4

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	Прак зан.	СРС	Всего, час
1	Введение в криптографию	Содержание и задачи дисциплины. Ее особенности и связь с другими дисциплинами. Методические рекомендации по ее изучению и требования, предъявляемые при проверке знаний. Общая характеристика процессов защиты информации. Требования к защите, сетодология разработки и анализа средств зашиты. Классические модели защиты информации. Краткий исторический очерк развития криптографии. Исторические примеры: шифр Цезаря, квадрат Полибия, шифр Виженера, решетка Кардано, книжный шифр и др. Понятие о криптоанализе.	10	12	8	30
2	Имитостойкость и помехоустойчивост	Основные понятия криптографии. Определение шифра	10	12	8	30

	ь шифров	и его математические модели. Ручные и машинные шифры. Ключевая система и основные требования к шифрам. Понятие криптосистемы. Шифры перестановки. Маршрутные и вертикальные перестановки, решетки и лабиринты. Открытые сообщения. Частотные характеристики открытых сообщений. Математические модели открытых сообщений и критерии на открытый текст. Способы представления информации, подлежащей шифрованию. Шифры замены. Одноалфавитные и многоалфавитные шифры замены. Поточные и блочные шифры замены. Шифры гаммирования. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Теоретико-информационный подход к оценке стойкости шифров. Надежность ключей. Совершенные шифры. Стойкость шифра и избыточность языка. Имитостойкость и ее характеристики. Методы обеспечения имитостойкости. Помехоустойчивое кодирование. Характеристики помехоустойчивости				
3	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.	10	12	8	30

		Методы анализа криптографических алгоритмов. Алгоритмические, аналитические и статистические методы анализа поточных шифров.				
4	Шифрование с открытым ключом	Системы шифрования с открытым ключом. Понятие односто-ронней функции. Криптосистемы RSA и Эль-Гамаля. Проблема фак-торизации целых чисел в конечных полях. Криптосистемы с откры-тым ключом на базе задаче о рюкзаке и линейных кодов. Асимм-мет-ричные системы шифрования и их преимущества. Хэш-функции и их использование в криптографии.	8	12	10	30
5	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.	8	12	10	30
6	Криптосистемы на базе ЭВМ	Особенности реализации криптосистем на базе вычислительной техники. Криптографические интерфейсы. Применение смарт-карт в системах электронных платежей. Компьютерная стеганография - метод, дополняющий традиционные криптографические методы. “Полное” скрытие данных. Типы файл-контейнеров (графические, звуковые). Алгоритмы “упаковки” данных (регулярные, псевдослучайные, комбинированные).	8	12	10	30
		Итого	**54**	**72**	**54**	**180**

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 курсового проекта в 9 семестре для очной формы обучения.

Примерная тематика курсового проекта:

Разработка алгоритма и программы исследования корреляционных свойств криптографических примитивов

Разработка алгоритма и программы по исследованию статистических свойств блочных алгоритмов шифрования

Разработка алгоритма и программы разложения целых чисел для анализа шифра RSA

Разработка алгоритма и программы по линейному анализу криптографических примитивов и блочных шифров

Разработка и реализация программного комплекса для исследования свойств криптографических ключей

Разработка алгоритма и программы по анализу шифра AES

Разработка программного комплекса анализа VPN.

Разработка алгоритма и программы реализации и исследованию свойств хэш-функций

Разработка алгоритма и программы по дифференциальному анализу криптографических примитивов и блочных шифров

Разработка электронного учебного пособия по курсу «Методы анализа криптографических систем»

Разработка лабораторной работы по статистическому анализу поточных шифров

Разработка лабораторной работы по алгебраическому анализу поточных шифров

Разработка лабораторной работы по анализу RSA-подобных криптосистем с открытыми ключами

Разработка лабораторной работы по анализу криптосистем с открытыми ключами на основе сложности дискретного логарифмирования

Задачи, решаемые при выполнении курсового проекта:

К задачам курсового проекта (работы) относятся обеспечение освоения основ:

системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;

принципов разработки шифров;

математических методов, используемых в криптографии.

Курсовой проект включат 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-2	**Знать:** - об основных методах и средствах криптографического анализа.	знание основных методах и средствах криптографического анализа	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: - оценивать уязвимость протоколов и интерфейсов компьютерных систем.	умение оценивать уязвимость протоколов и интерфейсов компьютерных систем.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: - типовыми криптографическими протоколами и их криптографическими качествами.	владение типовыми криптографическими протоколами и их криптографическими качествами.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-5	**Знать:** - о принципиальных подходах к созданию современных технических средств криптографической защиты информации.	знание принципиальных подходах к созданию современных технических средств криптографической защиты информации.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: - строить математические модели шифров и открытых текстов.	умение строить математические модели шифров и открытых текстов.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	Владеть: - основными требованиями, предъявляемыми к системам криптографической защиты информации с учетом возможных угроз.	владение основными требованиями, предъявляемыми к системам криптографической защиты информации с учетом возможных угроз.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-10	**Знать:** - о методах и критериях оценки надежности защиты информации.	знание методов и критериев оценки надежности защиты информации.	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: - Типовыми методами создания сетей засекреченной связи.	владение типовыми методами создания сетей засекреченной связи.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-18	**Знать:** - о принципиальных подходах к созданию современных технических средств криптографической защиты информации.	знание принципиальных подходах к созданию современных технических средств криптографической защиты информации.	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.	умение практически решать задачи защиты программ и данных криптографическими средствами.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: - основными принципами построения аппа-	владение основными принципами построения аппаратных и	Выполнение работ в срок, предусмотренный в ра-	Невыполнение работ в срок, предусмотренный в ра-

	ратных и программных реализации криптографических алгоритмов.	программных реализации криптографических алгоритмов.	бочих программах	бочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 8, 9 семестре для очной формы обучения по двух/четырехбалльной системе:

«зачтено»

«не зачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ОПК-2	**Знать:** - об основных методах и средствах криптографического анализа.	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь: - оценивать уязвимость протоколов и интерфейсов компьютерных систем.	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	Владеть: - типовыми криптографическими протоколами и их криптографическими качествами.	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ПК-5	**Знать:** - о принципиальных подходах к созданию современных технических средств криптографической защиты информации.	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь: - строить математические модели шифров и открытых текстов.	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	Владеть: - основными требованиями,	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

	предъявляемыми к системам криптографической защиты информации с учетом возможных угроз.			
ПК-10	**Знать:** - о методах и критериях оценки надежности защиты информации.	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь: - использовать свойства криптографических средств при анализе комплексных систем защиты информации.	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	Владеть: - Типовыми методами создания сетей засекреченной связи.	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ПК-18	**Знать:** - о принципиальных подходах к созданию современных технических средств криптографической защиты информации.	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь: - практически решать задачи защиты программ и данных криптографическими средствами.	Решение стандартных практических задач	Продемонстрирова н 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	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

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

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-2	**Знать:** - об основных методах и средствах 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: - оценивать уязвимость протоколов и интерфейсов компьютерных систем.	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
	Владеть: - типовыми криптографическими протоколами и их криптографическими качествами.	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
ПК-5	**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: - строить математические модели шифров и открытых текстов.	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
	Владеть: - основными требованиями, предъявляемыми к системам криптографиче-	Решение прикладных задач в конкретной предметной обла-	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный от-	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены

	ской защиты информации с учетом возможных угроз.	сти		вет во всех задачах		
ПК-10	**Знать:** - о методах и критериях оценки надежности 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: - использовать свойства криптографических средств при анализе комплексных систем защиты информации.	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
	Владеть: - Типовыми методами создания сетей засекреченной связи.	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
ПК-18	**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	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
	Владеть: - основными принципами построения аппаратных и программных реализации криптографических ал-	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены

	горитмов.					

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. Вопросы распределения ключей в сети шифрованной связи. Криптоанализ шифров перестановки.

2. Криптоанализ шифров замены.

3. Криптограммы, полученные при повторном использовании ключа.

4. Имитация и подмена сообщения.

5. Блоки выработки шифрующей последовательности и блоки шифрования.

6. Особенности криптоанализа блочных шифров.

7. Алгоритмы выработки хэш-функций.

8. Открытое распределение ключей (по Диффи-Хеллману).

9. Протоколы SET.

10. Объем информации, помещаемой в файл-контейнеры различных типов.

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. 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.
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. Классификация шифров. 2. Блочные шифры. 3. Поточные шифры. 4. Алфавиты открытых сообщений. 5. Частотные характеристики текстовых сообщений. 6. Основные положения.
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. Пример функции хэширования – ГОСТ Р 34.11-94. 2. Цифровая подпись. 3. Основные положения криптосистемы RSA.

4. Построение кодирующей процедуры E для криптосистемы RSA. 5. Построение декодирующей процедуры D для криптосистемы RSA. **6.** Алгоритмические задачи, связанные со схемой RSA.
ПК- 18 - способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
1. Общая идея шифра Эль-Гамаля. 2. Пароли шифра Эль-Гамаля. 3. Электронная подпись шифра Эль-Гамаля. 4. Задача аутентификации данных. 5. Задача имитозащиты данных. **6.** Подходы к контролю неизменности данных.

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	На чём специализируется метод brute force? o переполнение базы данных системы; o путём DDoS атаки на систему; o изменение шифрованного текста; o **перебор всех значений ключа.**
2	Поясните метод атаки с заданным текстом: o **имеется возможность получить шифрованный документ для любого нужного ему текста, но нет ключа;** o не имеется возможности получить шифрованный документ для нужного ему текста, но имеется ключ; o известно содержимое всего или части зашифрованного текста; o известен ключ, но необходимо расшифровать документ.
3	Шифрование это: o процедура, использующая некое необратимое преобразование**;** o процедура, использующая некий алгоритм возведения в степень**;** o процедура, использующая некий алгоритм взятия корня**;** o **процедура, использующая некое обратимое преобразование**.
4	Как называют бесключевые хэш-функции? o **кодами обнаружения ошибок**; o открытыми ключами; o кодами верификации сообщения; o кодами аутентификации сообщения.
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	Если фрагменты открытого текста заменяются некоторыми их эквивалентами в шифртексте, то соответствующий шифр относится к классу: o шифров перестановки; o **шифров замены;** o шифров подстановки; o композиционных шифров.
2	Как называют алфавиты, полученные из нормального на основе некоторого пра-

	вила? o **случайные;** o систематически перемешанные; o нормальные; o элементарные.
3	Какие значения обычно производят криптографические хэш-функции? o 2 и более бита; o **128 и более бит;** o 1 байт и более; o Менее 4 байт.
4	Какие выделяют важные типы криптографических хэш-функций? o последовательные; o **ключевые;** o **бесключевые;** o беспорядочные.
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	Какие важные свойства необходимо гарантировать для каждого обрабатываемого массива данных? o **подлинность;** o **авторство;** o полную защищённость; o специальную цифровую подпись.
2	Какие последствия могут быть от избыточности открытого текста, роникающего в шифротекст: o повышенная стойкость текста; o трудность расшифровки; o **повышенная слабость текста;** o вовлечение дополнительных структур для дешифровки.
3	Для чего используется алгоритм с открытым ключом? o **чтобы передать случайным образом сгенерированный секретный ключ;** o чтобы передать определённым образом сгенерированный секретный ключ; o чтобы передать случайным образом сгенерированный открытый ключ; o чтобы передать определённым образом сгенерированный открытый ключ.
4	Для чего используются криптографические генераторы случайных чисел: o для создания баз данных; o для теории относительности; o для проверки работоспособности системы; o **для генерации ключей.**
ПК- 18 - способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	
1	Цифровая подпись это: o подпись в электронном варианте;

	o **блок данных, сгенерированный с использованием некоторого секретного ключа;** o символы случайного алфавита; o шифрование определённых данных.
2	Что подразумевают под имитозащитой данных? o **защиту от навязывания ложных данных;** o защиту от навязывания паролей**;** o защиту от навязывания открытых ключей**;** o имитацию дешифрования данных**.**
3	Как позволяют шифровать информацию потоковые шифры? o побайтово; o наборами бит данных; o **побитово;** o наборами байт данных.
4	Хеш-функции – это: o **функции, предназначенные для "сжатия" произвольного сообщения или набора данных, записанных, как правило, в двоичном алфавите, в некоторую битовую комбинацию фиксированной длины, называемую свёрткой** o 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 o некоторое значение, рассчитанное из последовательности данных путём применения определённого алгоритма, используемое для проверки правильности передачи данных o «закон», по которому каждому элементу *x* из некоторого множества *X* ставится в соответствие единственный элемент *y* из множества *Y*.

7.2.4 Примерный перечень вопросов для подготовки к зачету

1.Приведите примеры шифров, применявшихся еще до нашей эры

2. Приведите пример шифра, для которого сам открытый текст является ключом

3. Какие шифры являются омофонами, в чем их преимущество перед шифрами простой замены

4. Что является ключом шифра Виженера

5. Являлись ли трафареты, которые использовали А. Грибоедов и Ришелье для передачи тайных сообщений, средствами шифрования

6. Приведите пример шифра, допускающего неоднозначное зашифрование

7. Какими шифрами пользовались Цезарь, Галилей, Наполеон, Ришелье

8. В чем состоит правило Керхгоффса, почему это правило является общепризнанным в криптографии

9. Чем отличаются принципы шифрования в аналоговой телефонии от принципов шифрования телеграфных сообщений

10. Чем отличаются симметричные шифрсистемы от асимметричных шифрсистем

11. Когда родилась криптография с открытыми ключами и первая реальная система шифрования

12. Каких выдающихся криптографов XX в. Вы знаете

13. Чем отличаются подходы к обеспечению безопасности информации в криптографии и в методах сокрытия информации

14. Какими методами обеспечивается конфиденциальность информации

15. Что такое целостность информации

16. Для каких аспектов информационного взаимодействия необходима аутентификация

17. Какие средства используются для обеспечения невозможности отказа от авторства

18. В чем суть предварительного распределения ключей

19. В чем разница между обычным и открытым распределением ключей

20. Для чего нужны схемы разделения секрета

21. Что такое сертификат открытого распределения ключей

22. Каковы функции центра сертификации ключей

23. Чем отличаются алгебраическая и вероятностная модели шифра

24. С какими целями в криптографии вводятся модели открытых текстов

25. Как подсчитать вероятность данного открытого текста в модели первого приближения

26. Какие подходы используются для распознавания открытых текстов

27. С какими примерами шифров замены и перестановки вы познакомились в историческом обзоре

28. Существуют ли шифры, не являющиеся ни шифрами замены, ни шифрами перестановки

29. Приведите пример шифра многозначной замены

30. Может ли блочный шифр быть шифром разнозначной замены

7.2.5 Примерный перечень заданий для решения прикладных задач

1.Содержание и задачи дисциплины. Ее особенности и связь с другими дисциплинами.

2.Методические рекомендации по ее изучению и требования, предъявляемые при проверке знаний. Общая характеристика процессов защиты информации.

3.Требования к защите, сетодология разработки и анализа средств зашиты. Классические модели защиты информации.

4. Краткий исторический очерк развития криптографии. Исторические примеры: шифр Цезаря, квадрат Полибия, шифр Виженера, решетка Кардано, книжный шифр и др. Понятие о криптоанализе.

5. Основные понятия криптографии. Определение шифра и его математические модели. Ручные и машинные шифры. Ключевая система и основные требования к шифрам. Понятие криптосистемы.

6. Шифры перестановки. Маршрутные и вертикальные перестановки, решетки и лабиринты.

7. Открытые сообщения. Частотные характеристики открытых сообщений. Математические модели открытых сообщений и критерии на открытый текст. Способы представления информации, подлежащей шифрованию.

8. Шифры замены. Одноалфавитные и многоалфавитные шифры замены. Поточные и блочные шифры замены.

9. Шифры гаммирования. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы.

10.Теоретико-информационный подход к оценке стойкости шифров. Надежность ключей. Совершенные шифры.

11. Стойкость шифра и избыточность языка. Имитостойкость и ее характеристики. Методы обеспечения имитостойкости. Помехоустойчивое кодирование. Характеристики помехоустойчивости

12. Основные способы реализации криптографических алгоритмов и требования, предъявляемые к ним.

13. Датчики псевдослучайных последовательностей (регистры сдвига, линейный конгруэнтный метод, линейные рекуррентные последовательности, мультиплексорные методы).

14. Периодичность случайных последовательностей. Распределение элементов в псевдослучайных последовательностях. Основные узлы и блоки криптосистем.

15. Методы анализа криптографических алгоритмов. Алгоритмические, аналитические и статистические методы анализа поточных шифров.

16. Системы шифрования с открытым ключом. Понятие односторонней функции. Криптосистемы RSA и Эль-Гамаля.

17. Проблема факторизации целых чисел в конечных полях. Криптосистемы с открытым ключом на базе задаче о рюкзаке и линейных кодов. Асимметричные системы шифрования и их преимущества.

18. Хэш-функции и их использование в криптографии.

19. Понятие криптографического протокола. Связь стойкости протокола со стойкостью базовой криптографической системы.

20. Классификация криптографических протоколов. Цифровая подпись. Стандарты цифровой подписи.

21.Протоколы аутентификации и их связь с цифровой подписью. Протоколы сертификации и предварительного распределения ключей.

22. Особенности реализации криптосистем на базе вычислительной техники. Криптографические интерфейсы. Применение смарт-карт в системах электронных платежей.

23.Компьютерная стеганография - метод, дополняющий традиционные криптографические методы. “Полное” скрытие данных.

24.Типы файл-контейнеров (графические, звуковые).

25.Алгоритмы “упаковки” данных (регулярные, псевдослучайные, комбинированные).

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 контролир. компетенции	Наименование оценочного средства
1	Введение в криптографию	ОПК-2, ПК-5, ПК- 10, ПК-18	Тест, контрольная работа, защита практических работ, требования к курсовому проекту
2	Имитостойкость и помехоустойчивость шифров	ОПК-2, ПК-5, ПК- 10, ПК-18	Тест, контрольная работа, защита практических работ, требования к курсовому проекту
3	Принципы построения и реализации криптографических алгоритмов	ОПК-2, ПК-5, ПК- 10, ПК-18	Тест, контрольная работа, защита практических работ, требования к курсовому проекту
4	Шифрование с открытым ключом	ОПК-2, ПК-5, ПК- 10, ПК-18	Тест, контрольная работа, защита практических работ, требования к курсовому проекту
5	Криптографические протоколы	ОПК-2, ПК-5, ПК- 10, ПК-18	Тест, контрольная работа, защита практических работ, требования к курсовому проекту
6	Криптосистемы на базе ЭВМ	ОПК-2, ПК-5, ПК- 10, ПК-18	Тест, контрольная работа, защита практических работ, 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 про-

верка 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.

Защита курсовой работы, курсового проекта или отчета по всем видам практик осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная

1. Защита информации в беспроводных сетях [Электронный ресурс] : Учеб. пособие / Н.М. Радько, А.Н. Мокроусов. - Электрон. текстовые, граф. дан. (835 072 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2010. - 1 файл. - 30-00.

2. Коржик В.И. Основы криптографии [Электронный ресурс]: учебное пособие/ Коржик В.И., Яковлев В.А.— Электрон. текстовые данные.— Санкт-Петербург: Интермедия, 2017.— 312 с.— Режим доступа: http://www.iprbookshop.ru/66798.html.

Дополнительная

1. Основы криптографической защиты информации [Электронный ресурс] учеб. пособие / А. Н. Мокроусов, Н.М. Радько. - Электрон. дан. (1 файл). - Воронеж: ВГТУ, 2004. - 1 дискета. - Имеется вариант на бумажном носителе. - 30.00.

2. Методические указания по выполнению лабораторных работ по дисциплине "Криптография" для студентов специальностей 090102 "Компьютерная безопасность", 090105 "Комплексное обеспечение компьютерной безопасности автоматизированных систем", 090106 "Информационная безопасность телекоммуникационных систем" очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: Н.М. Радько, А.Н. Мокроусов. - Электрон. текстовые, граф. дан. (1 141 760 байта). - Воронеж : ВГТУ, 2006. - 1 файл. - Режим доступа : локальная сеть ВГТУ; Имеется вариант на бумажном носителе. - 00-00. № 164-2006

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. № 274-2011.

4.Методические указания к практическим занятиям по дисциплине «Криптографические методы защиты информации» для специальностей 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения / ФГБОУ ВПО «Воронежский государственный технический университет»; сост. А. Н. Мокроусов. Воронеж, 2014. 47 с. № № 274-2011

3. Торстейнсон П. Криптография и безопасность в технологии .NET [Электронный ресурс]/ Торстейнсон П., Ганеш Г.А.— Электрон. текстовые данные.— Москва: Лаборатория знаний, 2020.— 480 с.— Режим доступа: http://www.iprbookshop.ru/20709.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:

https://www.studmed.ru/shennon-k-raboty-po-teorii-informacii-i-kibernetike_ebac37a4934.html

К.Шеннон. Работы по тории информации и кибернетике. –М.: ИЛ,. – 1963.

http://cryptography.ru/wp-content/uploads/2013/09/intro_to_crypto.pdf

Введение в криптографию / Под общ. ред. В. В. Ященко. — 4-е изд., доп. М.: МЦНМО, 2012. — 348 с.

https://obuchalka.org/2017010592442/osnovi-kriptologii-professionalnoe-rukovodstvo-i-interaktivnii-uchebnik-tilborg-van-h-k-a-2000.html

Тилборг ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. – М.: Мир, 2006. – 471 с.

https://www.studmed.ru/varfolomeev-a-a-sovremennaya-prikladnaya-kriptografiya_65a67610b12.html

Варфоломеев А.А. Современная прикладная криптография: Учеб. пособие. – М.: РУДН, 2008. – 218 с.: ил.

https://studfile.net/preview/6311471/

Бабаш А. Криптография. - М.: Салон-Пресс. 2007. – 514 с.

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 «Криптографические методы защиты информации» читаются лекции, проводятся практические занятия, выполняется курсовой проект.

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:

Неделя семестра	Тема и содержание практического занятия	Объем часов	В том числе, в интерактивной форме (ИФ)	Виды контроля
1-2	Освоение процесса зашифрования и расшифрования для простейших шифров	4	1	
3-5	Анализ шифров замены с использованием статистических закономерностей открытых сообщений	6	1	
6-8	Шифр Виженера	6	1	
9-11	Шифр Вернама	6	1	
12-15	Расчет мощности ключевой системы различных шифров	8	1	
16-19	Расчет характеристик имитостойкости шифров	8	1	
20	**Контрольная работа**	2	1	Контр. раб.
1-3	Расчет характеристик помехоустойчивости шифров	6	1	
4-6	Вычисление характеристик датчиков псевдослучайных чисел	6	1	
7-10	Анализ некоторых алгоритмов выработки хэш-функций	8	1	
11-14	Исследование криптографического протокола	8	1	
15-18	Программная реализация криптографической системы	8	1	
Итого часов		**76**	**12**	

Занятия проводятся путем решения конкретных задач в аудитории.

Методика выполнения курсового проекта изложена в учебно-методическом пособии. Выполнять этапы курсового проекта должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой

курсового проекта, защитой курсового проекта.

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 зачетом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.