МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ»

«УТВЕРЖДАЮ»
Проректор по учебной работе _____ Т.Ю. Нагорная
«27» 03 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптография

Уровень образовательной программы бакалавриат

Направление подготовки 01.03.02 Прикладная математика и информатика

Направленность (профиль) Прикладная математика и информатика

Форма обучения очная

Срок освоения ОП 4 года

Институт Цифровых технологий

Кафедра разработчик РПД Математика

Выпускающая кафедра Математика

Начальник
учебно-методического управления _____ Семенова Л.У.

Директор института ЦТ _____ Кумратова А.М.

Заведующий выпускающей кафедрой _____ Кочкаров А.М.

г. Черкесск, 2026 г.

СОДЕРЖАНИЕ

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Криптография» является: получение теоретических знаний в области цифровой безопасности. Познакомить обучающихся основам шифрования с открытым и закрытыми ключами, научить разрабатывать программные приложения с собственными шифрами.

Задачи дисциплины:

- дать основы теоретической составляющей криптографии;
- изучить фундаментальные идеи и отличия блокчейнов Биткоина и Эфириума;
- изучить практические методы разработки собственных электронных ключей

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2.1. Дисциплина «Криптография» относится к части, формируемой участниками образовательных отношений Блока1. Дисциплины (модули), имеет тесную связь с другими дисциплинами.

2.2. В таблице приведены предшествующие и последующие дисциплины, направленные на формирование компетенций дисциплины в соответствии с матрицей компетенций ОП.

Предшествующие и последующие дисциплины, направленные на формирование компетенций

№ п/п	Предшествующие дисциплины	Последующие дисциплины
1.	Объектно – ориентированное программирование Численные методы Системы программирования Мобильные сети и технологии Теория вероятностей и математическая статистика Методы оптимизации	Интеллектуальные системы Искусственный интеллект Научно – исследовательская работа (получение первичных навыков научно – исследовательской деятельности) Выполнение и защита выпускной квалификационной работы

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Планируемые результаты освоения образовательной программы (ОП) – компетенции обучающихся определяются требованиями стандарта по направлению подготовки 01.03.02 Прикладная математика и информатика и формируются в соответствии с матрицей компетенций ОП

№ п/п	Номер/ индекс компетенции	Наименование компетенции (или ее части)	Индикаторы достижений компетенций
1	2	3	4
1.	ПК-2	Способен применять современные информационные и коммуникационные сервисы и программные комплексы в различных сферах деятельности	ПК-2.1 Работает с современными информационными и коммуникационными сервисами при создании программных комплексов ПК-2.2 Знает основные этапы и их содержание при установке и настройке операционных систем и сетевых устройств, при создании программных комплексов ПК-2.3 Способен программировать на современных прикладных платформах, настраивать и тестировать создаваемые программные комплексы

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ
Очная форма обучения

Вид учебной работы		**Всего часов**	**Семестры**
			№ 6
			Часов
1		2	3
Аудиторная контактная работа (всего)		54	54
В том числе:			
Лекции		18	18
Лабораторные занятия В том числе, практическая подготовка		36 4	36 4
Контактная внеаудиторная работа в том числе:			
индивидуальные и групповые консультации		1,7	1,7
Самостоятельная работа обучающегося (СР) (всего)		52	52
Работа с книжными источниками		10	10
Работа с электронными источниками		10	10
Подготовка к коллоквиуму		10	10
Подготовка к тестированию		12	12
Реферат		10	10
Промежуточная аттестация	Зачет (З) В том числе	З	З
	Прием зачета, час	0,3	0,3
ИТОГО: Общая трудоемкость	**Часов**	108	108
	зач. ед.	3	3

4.2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.2.1. Разделы (темы) дисциплины, виды учебной деятельности и формы контроля
Очная форма обучения

№ п/п	Наименование раздела (темы) дисциплины	Виды учебной деятельности, включая самостоятельную работу обучающихся (в часах)					Формы текущей и промежуточной аттестации
		Л	ЛР (ПП)	ПЗ (ПП)	СРО	всего	
1	2	3	4	5	6	7	8
Семестр 6							
1.	Раздел 1. Введение в криптографию. Исторические шифры	4	8		10	22	Коллоквиум, реферат, тестирование
2.	Раздел 2. Математические основы криптографии	4	8		10	22	Коллоквиум, контрольные вопросы. Проверка практических индивидуальных заданий. Реферат, тестирование
3.	Раздел 3. Симметричное шифрование (криптография с секретным ключом)	4	8		10	22	Коллоквиум, контрольные вопросы. Проверка практических индивидуальных заданий. Реферат, тестирование
4.	Раздел 4. Криптография с открытым ключом (асимметричное шифрование)	4	8		12	24	Коллоквиум, контрольные вопросы. Проверка практических индивидуальных заданий. Реферат, тестирование
5.	Раздел 5. Цифровые подписи и управление ключами	2	4		10	16	
	Контактная внеаудиторная работа					1,7	индивидуальные и групповые консультации
	Промежуточная аттестация					**0,3**	**Зачет**
Итого часов в 8 семестре:		**18**	**36**		**52**	**108**	
ВСЕГО:		**18**	**36**		**52**	**108**	

4.2.2. Лекционный курс

№ п/п	Наименование раздела дисциплины	Наименование темы лекции	Содержание лекции	Всего часов
1	2	3	4	5
Семестр 6				
1.	Раздел 1. Введение в криптографию. Исторические шифры	Тема 1.1Основные понятия криптографии	Введение в криптографию. Конфиденциальность, целостность, аутентификация, неотрекаемость. Модель К. Шеннона: источник, шифровальщик, канал, дешифровальщик, противник.	2
		Тема 1.2 Классические шифры и их криптоанализ. Математическая формализация	Шифры замены (Цезарь, Афинский, многоалфавитные — шифр Виженера). Шифры перестановки (скитала, маршрутное шифрование). Криптоанализ на основе частотного анализа. Понятие криптосистемы, пространства ключей, открытых и шифрованных текстов.	2
	Раздел 2. Раздел 2. Математические основы криптографии	Тема 2.1 Теория чисел. Теория вероятностей и информация	Алгоритм Евклида (расширенный), сравнения по модулю, китайская теорема об остатках. Функция Эйлера, теоремы Эйлера и Ферма. Алгоритмы быстрого возведения в степень, вычисления обратного элемента. Основы теории информации К. Шеннона: энтропия, избыточность языка, единственность ключа. Совершенная секретность. Теорема Шеннона о единственности ключа и ее следствия.	2
		Тема 2.2 Теория сложности вычислений	Классы сложности P, NP, co-NP, NP-полные задачи. Понятие однонаправленной функции и функции с секретом (лазейкой).	2
	Раздел 3. Симметричное шифрование (криптография с секретным ключом)	Тема 3.1 Блочные шифры	Принципы построения: сеть Фейстеля (DES), SP-сеть (AES). Режимы работы блочных шифров (ECB, CBC, CFB, OFB, CTR, GCM). Методы криптоанализа: дифференциальный и линейный криптоанализ (основные идеи).	2

		Тема 3.2 Поточные шифры	Синхронные и самосинхронизирующиеся. Генераторы псевдослучайных последовательностей (РСЛОС, нелинейные комбинаторы).	2
	Раздел 4. Криптография с открытым ключом (асимметричное шифрование)	Тема 4.1 Основные концепции	Проблема распределения ключей, однонаправленные функции с секретом.	2
		Тема 4.2 Криптосистема RSA	Построение, шифрование, расшифрование. Оценка стойкости: факторизация больших чисел, атаки (на малый модуль, малые экспоненты).	2
	Раздел 5. Цифровые подписи и управление ключами	Тема 5.1 Понятие и свойства цифровой подписи	Схемы RSA-PSS, ECDSA, EdDSA.Стандарты и протоколы: PKI (Инфраструктура открытых ключей), сертификаты X.509, протоколы SSL/TLS (базовые принципы).	2
ИТОГО часов в 8 семестре:				**18**
ВСЕГО часов:				**18**

4.2.2 Лабораторные занятия

№ п/п	Наименование раздела дисциплины	Наименование практического занятия	Содержание практического занятия	Всего часов
1	2	3	4	5
Семестр 6				
2	Раздел 1. Введение в криптографию. Исторические шифры	Лабораторная работа №1 Классические шифры и их криптоанализ. Математическая формализация	Основы криптографической теории. Принципы работы классических шифров, криптоаналитическое вскрытие на основе математических моделей.	8
3	Раздел 2. Математические основы криптографии	Лабораторная работа №1 Классические шифры и их криптоанализ. Математическая формализация	Основные типы классических шифров (подстановочные, перестановочные, составные). Математическую формализация процессов шифрования и дешифрования. Криптоанализ классических шифров с использованием частотного анализа и	4

			методов оптимизации.	
			(Администрация Усть-Джегутинского муниципального района, Отдел информатизации и информационной безопасности)	
		Лабораторная работа №2 Теория сложности вычислений	Класс P сложности задач. NP – полные задачи. Понятие полиномиальной сводимости (Karp-сводимости). Псевдополиномиальные алгоритмы.	4
4	Раздел 3. Симметричное шифрование (криптография с секретным ключом)	Лабораторная работа №3 Блочные шифры	Принципы построения и анализ симметричных блочных шифров, изучение современных алгоритмов и режимов их работы. Базовые понятия и структуры блочных шифров Основные алгоритмы (DES, AES, ГОСТ 28147-89)	4
		Лабораторная работа №4 Поточные шифры	Принципы построения, методы анализа и реализации поточных шифров, их криптографические свойства и области применения.	4
5	Раздел 4. Криптография с открытым ключом (асимметричное шифрование)	Лабораторная работа №5 Криптосистема RSA	Криптосистема RSA (Rivest-Shamir-Adleman) - асимметричная криптографическая система, основанная на вычислительной сложности задачи факторизации больших чисел. Алгоритм работы	**8**
	Раздел 5. Цифровые подписи и управление ключами	Лабораторная работа №6 Понятие и свойства цифровой подписи	Систематизированные знания о цифровой подписи (ЭЦП), её математические основы, свойства, области применения и права регулирования.	**4**
ИТОГО часов в 8 семестре:				**36**
Всего часов:				**36**

4.3. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ

№ п/п	Наименование раздела (темы) дисциплины	№ п/п	Виды СРО	Всего часов
1	2	3	4	4
Семестр 8				
1.	Раздел 1. Введение в криптографию. Исторические шифры	1.1.	Работа с книжными источниками. Работа с электронными учебниками. Подготовка к коллоквиуму. Реферат.	5
		1.2	Работа с книжными источниками. Работа с электронными учебниками. Подготовка к коллоквиуму. Реферат.	5
2.	Раздел 2. Раздел 2. Математические основы криптографии	2.1.	Работа с книжными источниками. Работа с электронными учебниками. Подготовка к коллоквиуму. Реферат. Тестирование	5
		2.2	Работа с книжными источниками. Работа с электронными учебниками. Подготовка к коллоквиуму. Реферат. Тестирование	5
3.	Раздел 3. Симметричное шифрование (криптография с секретным ключом)	3.1	Работа с книжными источниками. Работа с электронными учебниками. Подготовка к коллоквиуму. Реферат. Тестирование	5
		3.2	Работа с книжными источниками. Работа с электронными учебниками. Подготовка к коллоквиуму. Реферат. Тестирование	5
4.	Раздел 4. Криптография с открытым ключом (асимметричное шифрование)	4.1	Работа с книжными источниками. Работа с электронными учебниками. Подготовка к коллоквиуму. Реферат. Тестирование	6
		4.2	Работа с книжными источниками. Работа с электронными учебниками. Подготовка к коллоквиуму. Реферат. Тестирование	6
5.	Раздел 5. Цифровые подписи и управление ключами	5.1	Работа с книжными источниками. Работа с электронными учебниками. Подготовка к коллоквиуму. Реферат. Тестирование	10
ИТОГО часов в 8 семестре:				**52**
Всего часов:				**52**

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

5.1. Методические указания для обучающихся к лекционным занятиям

Какими бы замечательными качествами в области методики ни обладал лектор, какое бы большое значение на занятиях ни уделял лекции слушатель, глубокое понимание материала достигается только путем самостоятельной работы над ним.

Работа над конспектом лекции осуществляется по этапам:

• повторить изученный материал по конспекту;

• непонятные положения отметить на полях и уточнить;

• неоконченные фразы, пропущенные слова и другие недочеты в записях устранить, пользуясь материалами из учебника и других источников;

• завершить техническое оформление конспекта (подчеркивания, выделение главного, выделение разделов, подразделов и т.п.).

Самостоятельную работу следует начинать с доработки конспекта, желательно в тот же день, пока время не стерло содержание лекции из памяти (через 10 ч после лекции в памяти остается не более 30-40 % материала). Работа над конспектом не должна заканчиваться с прослушивания лекции. После лекции, в процессе самостоятельной работы, перед тем, как открыть тетрадь с конспектом, полезно мысленно восстановить в памяти содержание лекции, вспомнив ее структуру, основные положения и выводы.

С целью доработки необходимо прочитать записи, восстановить текст в памяти, а также исправить описки, расшифровать не принятые ранее сокращения, заполнить пропущенные места, понять текст, вникнуть в его смысл. Далее прочитать материал по рекомендуемой литературе, разрешая в ходе чтения, возникшие ранее затруднения, вопросы, а также дополнения и исправляя свои записи. Записи должны быть наглядными, для чего следует применять различные способы выделений. В ходе доработки конспекта углубляются, расширяются и закрепляются знания, а также дополняется, исправляется и совершенствуется конспект. Еще лучше, если вы переработаете конспект, дадите его в новой систематизации записей. Это, несомненно, займет некоторое время, но материал вами будет хорошо проработан, а конспективная запись его приведена в удобный для запоминания вид. Введение заголовков, скобок, обобщающих знаков может значительно повысить качество записи. Этому может служить также подчеркивание отдельных мест конспекта красным карандашом, приведение на полях или на обратной стороне листа краткой схемы конспекта и др.

Подготовленный конспект и рекомендуемая литература используется при подготовке к практическому (семинарскому) занятию. Подготовка сводится к внимательному прочтению учебного материала, к выводу с карандашом в руках всех утверждений и формул, к решению примеров, задач, к ответам на вопросы, предложенные в конце лекции преподавателем или помещенные в рекомендуемой литературе. Примеры, задачи, вопросы по теме являются средством самоконтроля.

Непременным условием глубокого усвоения учебного материала является знание основ, на которых строится изложение материала. Обычно преподаватель напоминает, какой ранее изученный материал и в какой степени требуется подготовить к очередному занятию. Эта рекомендация, как и требование систематической и серьезной работы над всем лекционным курсом, подлежит безусловному выполнению. Потери логической связи как внутри темы, так и между ними приводит к негативным последствиям: материал учебной дисциплины перестает основательно восприниматься, а творческий труд подменяется утомленным переписыванием. Обращение к ранее изученному материалу не только помогает восстановить в памяти известные положения, выводы, но и приводит разрозненные знания в систему, углубляет и расширяет их. Каждый возврат к старому материалу позволяет найти в нем что-то новое, переосмыслить его с иных позиций, определить для него наиболее подходящее место в уже имеющейся системе знаний. Неоднократное обращение к пройденному материалу является наиболее рациональной формой приобретения и закрепления знаний. Очень полезным, но, к сожалению, еще мало используемым в практике самостоятельной работы, является предварительное ознакомление с учебным материалом. Даже краткое, беглое знакомство с материалом очередной лекции дает многое. Обучающиеся получают общее представление о ее содержании и структуре, о главных и второстепенных вопросах, о терминах и определениях. Все это облегчает работу на лекции и делает ее целеустремленной.

5.2. Методические указания для подготовки обучающихся к практическим занятиям

В процессе подготовки и проведения практических занятий обучающиеся закрепляют полученные ранее теоретические знания, приобретают навыки их практического применения, опыт рациональной организации учебной работы.

Поскольку активность на практических занятиях является предметом внутрисеместрового контроля его продвижения в освоении курса, подготовка к таким занятиям требует ответственного отношения.

При подготовке к занятию в первую очередь должны использовать материал лекций и соответствующих литературных источников. Самоконтроль качества подготовки к каждому занятию осуществляют, проверяя свои знания и отвечая на вопросы для самопроверки по соответствующей теме.

Входной контроль осуществляется преподавателем в виде проверки и актуализации знаний обучающихся по соответствующей теме.

Выходной контроль осуществляется преподавателем проверкой качества и полноты выполнения задания.

Подготовку к практическому занятию каждый обучающийся должен начать с ознакомления с планом практического занятия, который отражает содержание предложенной темы. Тщательное продумывание и изучение вопросов плана основывается на проработке текущего материала, а затем изучение обязательной и дополнительной литературы, рекомендованной к данной теме.

Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса. Результат такой работы должен проявиться в способности обучающегося свободно ответить на теоретические вопросы, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий. Предлагается следующая опорная схема подготовки к практическим занятиям.

Обучающийся при подготовке к практическому занятию может консультироваться с преподавателем и получать от него наводящие разъяснения, задания для самостоятельной работы.

1. Ознакомление с темой практического занятия. Выделение главного (основной темы) и второстепенного (подразделы, частные вопросы темы).
2. Освоение теоретического материала по теме с опорой на лекционный материал, учебник и другие учебные ресурсы. Самопроверка: постановка вопросов, затрагивающих основные термины, определения и положения по теме, и ответы на них.
3. Выполнение практического задания. Обнаружение основных трудностей, их решение с помощью дополнительных интеллектуальных усилий и/или подключения дополнительных источников информации.
4. Решение типовых заданий расчетно-графической работы.

5.4 Методические рекомендации прохождения тестирования

Подготовку к итоговому тестированию необходимо осуществлять поэтапно.

На первом этапе необходимо повторить основные положения всех тем, детально разбирая наиболее сложные моменты. Непонятные вопросы необходимо выписывать, чтобы по ним можно было проконсультироваться с преподавателем перед прохождением итогового тестирования. Подготовку по темам каждой дидактической единицы целесообразно производить отдельно. На этом этапе необходимо использовать материалы лекционного курса, материалы семинарских занятий, тестовые задания для текущего контроля знаний, а также презентации лекционного курса.

На втором этапе подготовки предлагается без повторения теоретического материала дать ответы тестовые задания для рубежного контроля знаний. Если ответы на какие-то вопросы вызвали затруднение, необходимо еще раз повторить соответствующий теоретический материал.

Наконец, третий этап подготовки необходимо осуществить непосредственно накануне теста. На данном этапе необходимо аккуратно просмотреть весь лекционный курс.

В случае, если результаты выполнения тестового задания оказались неудовлетворительными, необходимо зафиксировать темы, на вопросы по которым были даны неверные ответы, и еще раз углубленно повторить соответствующие темы в соответствии с указанными выше тремя этапами подготовки к тестированию.

5.3 Методические рекомендации прохождения коллоквиума

Коллоквиумом называется собеседование преподавателя и студента по заранее определенным контрольным вопросам. Целью коллоквиума является формирование у студента навыков анализа теоретических проблем на основе самостоятельного изучения учебной и научной литературы. На коллоквиум выносятся крупные, проблемные, нередко спорные теоретические вопросы. Упор делается на монографические работы профессора-автора данного спецкурса. От студента требуется:

- владение изученным в ходе учебного процесса материалом, относящимся к рассматриваемой проблеме;
- знание разных точек зрения, высказанных в научной литературе по соответствующей проблеме, умение сопоставлять их между собой;
- наличие собственного мнения по обсуждаемым вопросам и умение его аргументировать.

Коллоквиум – это не только форма контроля, но и метод углубления, закрепления знаний студентов, так как в ходе собеседования преподаватель разъясняет сложные вопросы, возникающие у студента в процессе изучения данного источника. Однако коллоквиум не консультация и не экзамен. Его задача добиться глубокого изучения отобранного материала, пробудить у студента стремление к чтению дополнительной социологической литературы.

Подготовка к коллоквиуму.

Подготовка к коллоквиуму начинается с установочной консультации преподавателя, на которой он разъясняет развернутую тематику проблемы, рекомендует литературу для изучения и объясняет процедуру проведения коллоквиума. Как правило, на самостоятельную подготовку к коллоквиуму студенту отводится 3 – 4 недели. Методические указания состоят из рекомендаций по изучению источников и литературы, вопросов для самопроверки и кратких конспектов ответа с перечислением основных фактов и событий, относящихся к пунктам плана каждой темы. Это должно помочь студентам целенаправленно организовать работу по овладению материалом и его запоминанию. При подготовке к коллоквиуму следует, прежде всего, просмотреть конспекты лекций и практических занятий и отметить в них имеющиеся вопросы коллоквиума. Если какие-то вопросы вынесены преподавателем на самостоятельное изучение, следует обратиться к учебной литературе, рекомендованной преподавателем в качестве источника сведений.

Коллоквиум проводится в форме индивидуальной беседы преподавателя с каждым студентом или беседы в небольших группах (2 – 3 человека). Обычно преподаватель задает несколько кратких конкретных вопросов, позволяющих выяснить степень добросовестности работы с литературой, проверяет конспект. Далее более подробно обсуждается какая-либо сторона проблемы, что позволяет оценить уровень понимания. По итогам коллоквиума выставляется дифференцированная оценка по пятибалльной системе.

5.5 Работа с литературными источниками и интернет ресурсами

В процессе подготовки к практическим занятиям, обучающимся необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме семинарского или практического занятия, что позволяет обучающимся проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

5.6 Подготовка презентации и реферата

Для подготовки презентации рекомендуется использовать: PowerPoint, MS Word, Acrobat Reader, LaTeX-овский пакет beamer. Самая простая программа для создания презентаций – Microsoft PowerPoint. Для подготовки презентации необходимо собрать и обработать начальную информацию.

Последовательность подготовки презентации:

1. Четко сформулировать цель презентации: вы хотите свою аудиторию мотивировать, убедить, заразить какой-то идеей или просто формально отчитаться.
2. Определить каков будет формат презентации: живое выступление (тогда, сколько будет его продолжительность) или электронная рассылка (каков будет контекст презентации).
3. Отобрать всю содержательную часть для презентации и выстроить логическую цепочку представления.
4. Определить ключевые моменты в содержании текста и выделить их.
5. Определить виды визуализации (картинки) для отображения их на слайдах в соответствии с логикой, целью и спецификой материала.
6. Подобрать дизайн и форматировать слайды (количество картинок и текста, их расположение, цвет и размер).
7. Проверить визуальное восприятие презентации.

К видам визуализации относятся иллюстрации, образы, диаграммы, таблицы. Иллюстрация - представление реально существующего зрительного ряда. Образы – в отличие от иллюстраций - метафора. Их назначение - вызвать эмоцию и создать отношение к ней, воздействовать на аудиторию. С помощью хорошо продуманных и представляемых образов, информация может надолго остаться в памяти человека. Диаграмма - визуализация количественных и качественных связей. Их используют для убедительной демонстрации данных, для пространственного мышления в дополнение к логическому. Таблица - конкретный, наглядный и точный показ данных. Ее основное назначение - структурировать информацию, что порой облегчает восприятие данных аудиторией.

Практические советы по подготовке презентации готовьте отдельно:

- печатный текст + слайды + раздаточный материал;
- слайды - визуальная подача информации, которая должна содержать минимум текста, максимум изображений, несущих смысловую нагрузку, выглядеть наглядно и

просто;

- текстовое содержание презентации – устная речь или чтение, которая должна включать аргументы, факты, доказательства и эмоции;
- рекомендуемое число слайдов 17-22;
- обязательная информация для презентации: тема, фамилия и инициалы выступающего; план сообщения; краткие выводы из всего сказанного; список использованных источников;
- раздаточный материал – должен обеспечивать ту же глубину и охват, что и живое выступление: люди больше доверяют тому, что они могут унести с собой, чем исчезающим изображениям, слова и слайды забываются, а раздаточный материал остается постоянным осязаемым напоминанием; раздаточный материал важно раздавать в конце презентации; раздаточный материалы должны отличаться от слайдов, должны быть более информативными.

Тема доклада должна быть согласованна с преподавателем и соответствовать теме учебного занятия. Материалы при его подготовке, должны соответствовать научно-методическим требованиям вуза и быть указаны в докладе. Необходимо соблюдать регламент, оговоренный при получении задания. Иллюстрации должны быть достаточными, но не чрезмерными.

Работа обучающегося над докладом-презентацией включает отработку умения самостоятельно обобщать материал и делать выводы в заключении, умения ориентироваться в материале и отвечать на дополнительные вопросы слушателей, отработку навыков ораторства, умения проводить диспут.

Докладчики должны знать и уметь: сообщать новую информацию; использовать технические средства; хорошо ориентироваться в теме всего семинарского занятия; дискутировать и быстро отвечать на заданные вопросы; четко выполнять установленный регламент (не более 10 минут); иметь представление о композиционной структуре доклада и др.

Структура выступления

Вступление помогает обеспечить успех выступления по любой тематике. Вступление должно содержать: название, сообщение основной идеи, современную оценку предмета изложения, краткое перечисление рассматриваемых вопросов, живую интересную форму изложения, акцентирование внимания на важных моментах, оригинальность подхода.

Основная часть, в которой выступающий должен глубоко раскрыть суть затронутой темы, обычно строится по принципу отчета. Задача основной части – представить достаточно данных для того, чтобы слушатели заинтересовались темой и захотели ознакомиться с материалами. При этом логическая структура теоретического блока не должны даваться без наглядных пособий, аудио-визуальных и визуальных материалов.

Заключение – ясное, четкое обобщение и краткие выводы, которых всегда ждут слушатели

5.7 Методические указания по подготовке к опросу (контрольные вопросы)

Самостоятельная работа обучающихся включает подготовку к опросу на практическом занятии. Опрос представляет собой форму текущего контроля успеваемости обучающегося по изучаемой дисциплине. При подготовке к опросу необходимо изучить материалы лекции, основную и дополнительную литературу, а также информацию с использованием Интернет-ресурсов по заявленной теме. Темы практических занятий,

вопросы для обсуждения, а также контрольные вопросы даются в методических указаниях по соответствующим темам дисциплины. Обучающийся должен обратить внимание на основные термины и понятия по теме, на проблемные вопросы, подобрать дополнительную литературу для их освещения, составить тезисы выступления. Ответ обучающегося должен быть развернутым, аргументированным, логически выстроенным. При выставлении оценки учитывается правильность ответа по содержанию, самостоятельность суждений и выводов, умение анализировать и связывать теоретические положения с практикой.

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

№ п/п	Виды учебной работы	Образовательные технологии	Всего часов
1	2	3	4
1	Тема 1.1Основные понятия криптографии	Технологии развития критического мышления. Обзорная лекция.	2
2	Тема 2.1 Теория чисел. Теория вероятностей и информация	Лекция – презентация с использованием Power Point.	2
3	Тема 3.1 Блочные шифры	Использование компьютерных технологий при выполнении индивидуальных практических заданий по созданию собственного ПО.	2
4	Тема 4.2 Криптосистема RSA	Лекция – презентация с использованием Power Point.	2
5	Тема 5.1 Понятие и свойства цифровой подписи.	Использование компьютерных технологий при выполнении индивидуальных практических заданий	2
Итого часов в 8 семестре:			**10**
Всего часов:			**10**

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Перечень основной и дополнительной учебной литературы

Список основной литературы

1. Бескид П.П. Криптографические методы защиты информации. Часть 1. Основы криптографии : учебное пособие / Бескид П.П., Тагарникова Т.М.. — Санкт-Петербург : Российский государственный гидрометеорологический университет, 2010. — 95 с. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/17925.html — Режим

доступа: для авторизир. пользователей

2. Майстренко Н.В. Основы теории информации и криптографии : учебное пособие / Майстренко Н.В., Майстренко А.В.. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2018. — 81 с. — ISBN 978-5-8265-1950-9. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/94362.html — Режим доступа: для авторизир. пользователей
3. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / Лапонина О.Р.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 605 с. — ISBN 978-5-4497-0684-3. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/97571.html — Режим доступа: для авторизир. пользователей

Список дополнительной литературы

4. Гультяева Т.А. Основы теории информации и криптографии : конспект лекций / Гультяева Т.А.. — Новосибирск : Новосибирский государственный технический университет, 2010. — 88 с. — ISBN 978-5-7782-1425-5. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/44987.html — Режим доступа: для авторизир. пользователей
5. Басалова Г.В. Основы криптографии : учебное пособие / Басалова Г.В.. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 282 с. — ISBN 978-5-4497-0340-8. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89455.html — Режим доступа: для авторизир. пользователей

7.2 Интернет-ресурсы, справочные систем

1. ООО «Ай Пи Ар Медиа». Доступ с к ЭБС IPRbooks

7.3. Информационные технологии, лицензионное программное обеспечение

Лицензионное программное обеспечение	Реквизиты лицензий/ договоров
Антивирус Dr.Web Desktop Security Suite	Лицензионный договор № 621 Срок действия: с 25.09.2025 до 24.09.2026
Консультант Плюс	Договор № 7 от 15.01.2026 г.
Цифровой образовательный ресурс IPR SMART	Лицензионный договор № 12873/25П от 02.07.2025 г. Срок действия: с 01.07.2025 г. до 30.06.2026 г.
ЛИРА	Сублицензионный договор № 2066/А от 21.01.2014 г.
MATLAB	Гос. контракт № 0379100003114000018 от 16 мая 2014 г.
Кодекс	Лицензионное соглашение № 5/4072 от 29.03.2026 г.
Бесплатное ПО	
LibreOffice, OpenOffice, МойОфис, Sumatra PDF, 7-Zip, Adobe Acrobat Reader, Lazarus, Firebird, IBE Expert, VBA, MySQL, Virtual box, Visual Studio Code, StarUML – унифицированный язык моделирования, PostgreSQL. Учебная версия, Project, STDU Viewer	

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Требования к аудиториям (помещениям, местам) для проведения занятий

1. Учебная аудитория для проведения занятий лекционного типа:

Учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнение курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации

2. Учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Специализированная мебель:
Стол преподавательский - 1шт., компьютерные столы - 10шт., парты -7шт., стулья - 24шт., доска меловая - 1шт.
Лабораторное оборудование, технические средства обучения, служащие для предоставления учебной информации большой аудитории:
Персональный компьютер – 10 шт.
Экран настенный рулонный – 1 шт.

3. Помещение для самостоятельной работы

Отдел обслуживания печатными изданиями
Специализированная мебель:Рабочие столы на 1 место – 21 шт.Стулья – 55 шт. Набор демонстрационного оборудования и учебно-наглядных пособий, обеспечивающих тематические иллюстрации: экран настенный – 1 шт.
Проектор – 1шт. Ноутбук – 1шт.
Информационно-библиографический отдел.
Специализированная мебель:
Рабочие столы на 1 место - 6 шт. Стулья - 6 шт.
Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением

доступа в электронную информационно-образовательную среду ФГБОУ ВО «СевКавГА»: Персональный компьютер – 1шт. Сканер – 1 шт. МФУ – 1 шт. Отдел обслуживания электронными изданиями Специализированная мебель:

Рабочие столы на 1 место – 24 шт. Стулья – 24 шт.
Набор демонстрационного оборудования и учебно-наглядных пособий, обеспечивающих тематические иллюстрации:
Интерактивная система - 1 шт. Монитор – 21 шт. Сетевой терминал -18 шт. Персональный компьютер -3 шт. МФУ – 2 шт. Принтер –1шт.

4. Помещение для хранения и профилактического обслуживания учебного оборудования
Специализированная мебель: Шкаф – 1 шт., стул -2 шт., кресло компьютерное – 2 шт., стол угловой компьютерный – 2 шт., тумбочки с ключом – 2 шт. Учебное пособие (персональный компьютер в комплекте) – 2 шт.

8.2. Требования к оборудованию рабочих мест преподавателя и обучающихся
Рабочее место преподавателя, оснащенное компьютером с доступом в Интернет.
Рабочие места обучающихся, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в цифровой образовательной среде.

8.3. Требования к специализированному оборудованию нет

9. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Для обеспечения образования инвалидов и обучающихся с ограниченными возможностями здоровья разрабатывается (в случае необходимости) адаптированная образовательная программа, индивидуальный учебный план с учетом особенностей их психофизического развития и состояния здоровья, в частности применяется индивидуальный подход к освоению дисциплины, индивидуальные задания: рефераты, письменные работы и, наоборот, только устные ответы и диалоги, индивидуальные консультации, использование диктофона и других записывающих средств для воспроизведения лекционного и семинарского материала.

В целях обеспечения обучающихся инвалидов и лиц с ограниченными возможностями здоровья комплектуется фонд основной учебной литературой, адаптированной к ограничению электронных образовательных ресурсов, доступ к которым организован в БИЦ Академии. В библиотеке проводятся индивидуальные консультации для данной категории пользователей, оказывается помощь в регистрации и использовании сетевых и локальных электронных образовательных ресурсов, предоставляются места в читальном зале.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
ПО ДИСЦИПЛИНЕ

Криптография

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Основы алгоритмов криптографии

Компетенции, формируемые в процессе изучения дисциплины

Индекс	Формулировка компетенции
ПК-2	Способен применять современные информационные и коммуникационные сервисы и программные комплексы в различных сферах деятельности

2. Этапы формирования компетенции в процессе освоения дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой разделов (тем) учебных занятий. Изучение каждого раздела (темы) предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций обучающимися.

Этапность формирования компетенций прямо связана с местом дисциплины в образовательной программе.

Разделы (темы) дисциплины	ПК-2
Тема 1.1Основные понятия криптографии	+
Тема1.2 Классические шифры и их криптоанализ. Математическая формализация	+
Тема 2.1 Теория чисел. Теория вероятностей и информация	+
Тема 2.2 Теория сложности вычислений	+
Тема 3.1 Блочные шифры	+
Тема 3.2 Поточные шифры	+
Тема 4.1 Основные концепции	+
Тема 4.2 Криптосистема RSA	+
Тема 5.1 Понятие и свойства цифровой подписи	+

3. Показатели, критерии и средства оценивания компетенций, формируемых в процессе изучения дисциплины

ПК-2 Способен применять современные информационные и коммуникационные сервисы и программные комплексы в различных сферах деятельности

Индикаторы достижений	**Критерии оценивания результатов обучения**				**Средства оценивания результатов обучения**	
	неудовлетв	**удовлетв**	**хорошо**	**отлично**	**Текущий контроль**	**Промежуточная аттестация**
ПК-2.1 Работает с современными информационными и коммуникационными сервисами при создании программных комплексов	Не может работать с современными информационными и коммуникационными сервисами при создании программных комплексов	Частично может работать с современными информационными и коммуникационными сервисами при создании программных комплексов	Может работать с современными информационными и коммуникационными сервисами при создании программных комплексов	Разбирается на отлично в работе с современных информационных и коммуникационных сервисов при создании программных комплексов	Коллоквиум, контрольные вопросы. Проверка практических индивидуальных заданий. Реферат, тестирование	Зачет
ПК-2.2 Знает основные этапы и их содержание при установке и настройке операционных систем и сетевых устройств, при создании программных комплексов	Не знает основные этапы и их содержание при установке и настройке операционных систем и сетевых устройств, при создании программных комплексов	Частично знает основные этапы и их содержание при установке и настройке операционных систем и сетевых устройств, при создании программных комплексов	Знает основные этапы и их содержание при установке и настройке операционных систем и сетевых устройств, при создании программных комплексов	Отлично знает основные этапы и их содержание при установке и настройке операционных систем и сетевых устройств, при создании программных комплексов	Коллоквиум, контрольные вопросы. Проверка практических индивидуальных заданий. Реферат, тестирование	Зачет
ПК-2.3 Способен программировать на современных прикладных платформах, настраивать и тестировать создаваемые программные комплексы	Не способен программировать на современных прикладных платформах, настраивать и тестировать создаваемые программные комплексы	Частично способен программировать на современных прикладных платформах, настраивать и тестировать создаваемые программные комплексы	Способен программировать на современных прикладных платформах, настраивать и тестировать создаваемые программные комплексы	Отлично может программировать на современных прикладных платформах, настраивать и тестировать создаваемые программные комплексы	Коллоквиум, контрольные вопросы. Проверка практических индивидуальных заданий. Реферат, тестирование	Зачет

4. Комплект контрольно-оценочных средств по дисциплине

Вопросы к зачету

по дисциплине «Криптография»

1. Главное отличие шифра перестановки от шифра замены
2. Дайте математическое определение аффинному шифру. При каких условиях он корректно определен?
3. Опишите алгоритм частотного криптоанализа шифра простой замены.
4. Объясните, как с помощью индекса совпадений можно определить длину ключа в шифре Виженера.
5. Криптографическая слабость шифра Цезаря и аффинного шифра
6. Дайте определение класса сложности P. Приведите примеры задач, принадлежащих этому классу.
7. Что такое NP-полные задачи? Почему они занимают особое место в теории сложности?
8. Объясните понятие полиномиальной сводимости (Karp-сводимости).
9. В чем заключается проблема P vs NP? Каковы ее практические последствия?
10. Опишите алгоритм верификатора для NP-задач.
11. Что такое класс co-NP? Приведите пример co-NP-полной задачи.
12. Объясните различия между классами сложности P, NP и EXP.
13. Что такое псевдополиномиальные алгоритмы? Приведите пример.
14. Опишите метод сведения для доказательства NP-полноты задачи.
15. Что такое параметризованная сложность и класс FPT?
16. Дайте определение блочному шифру. Чем он отличается от поточного?
17. Опишите структуру сети Фейстеля. Какие ее преимущества?
18. Объясните принцип работы SP-сети на примере AES.
19. Что такое S-блоки и каким требованиям они должны удовлетворять?
20. Перечислите и охарактеризуйте основные режимы работы блочных шифров.
21. В чем заключаются основные уязвимости режима ECB?
22. Опишите алгоритм DES. Почему он считается устаревшим?
23. Каковы основные особенности алгоритма ГОСТ 28147-89?
24. Объясните процедуру расширения ключа в AES.
25. Что такое атаки "встреча посередине" и дифференциальный криптоанализ?
26. Дайте определение поточного шифра. Чем он отличается от блочного?
27. Опишите принцип работы синхронного поточного шифра.
28. Что такое самосинхронизирующийся поточный шифр?
29. Перечислите основные требования к ключевому потоку.
30. Опишите структуру генератора ключевого потока на основе регистров сдвига с линейной обратной связью (РСЛОС).
31. Что такое нелинейный комбинированный генератор? Приведите пример.
32. Объясните уязвимости, связанные с использованием линейной обратной связи в РСЛОС.
33. Что такое корреляционная атака на поточные шифры?
34. Опишите алгоритм RC4. Какие у него есть преимущества и недостатки?
35. Где применяются поточные шифры в современных информационных системах?
36. На чем основана криптографическая стойкость RSA?

37. Объясните, почему в RSA выбирают простые числа p и q примерно одинаковой длины.
38. Что такое функция Эйлера и как она вычисляется для n = p×q?
39. Почему необходимо выбирать e взаимно простым с φ(n)?
40. Как вычисляется секретная экспонента d?
41. Какие атаки возможны на RSA и как от них защищаться?
42. Что такое схема дополнения OAEP и зачем она нужна?
43. Объясните китайскую теорему об остатках и ее применение в RSA.
44. Чем отличается практическое применение RSA от теоретического описания?
45. Какие современные рекомендации по длине ключей RSA существуют?
46. Дайте определение цифровой подписи. Чем она отличается от простой электронной подписи?
47. Опишите принцип работы асимметричной криптографии в контексте ЭЦП.
48. Каковы основные цели использования цифровой подписи?
49. Объясните, почему для создания ЭЦП обычно используется связка «хэш-функция + шифрование закрытым ключом».
50. Перечислите основные свойства цифровой подписи и дайте краткую характеристику каждому.
51. Что такое «неотказуемость» и почему это важнейшее свойство ЭЦП?
52. Объясните разницу между присоединённой и отсоединённой цифровой подписью.
53. Какие угрозы безопасности предотвращает корректно реализованная система ЭЦП?
54. Опишите типовой алгоритм формирования цифровой подписи.
55. Опишите типовой алгоритм проверки цифровой подписи.
56. Что такое сертификат открытого ключа и какова его роль в инфраструктуре ЭЦП?
57. Назовите распространённые алгоритмы цифровой подписи (RSA, DSA, ECDSA).
58. Какие виды ЭЦП установлены в законодательстве РФ (ФЗ-63 «Об электронной подписи»)?
59. В каких сферах деятельности наиболее востребована квалифицированная электронная подпись?
60. Какие юридические последствия влечёт использование ЭЦП?

Вопросы к коллоквиуму

по дисциплине «Криптография»

Вопросы к разделу 1.

1. Главное отличие шифра перестановки от шифра замены
2. Дайте математическое определение аффинному шифру. При каких условиях он корректно определен?
3. Опишите алгоритм частотного криптоанализа шифра простой замены.
4. Объясните, как с помощью индекса совпадений можно определить длину ключа в шифре Виженера.
5. Криптографическая слабость шифра Цезаря и аффинного шифра
6. Дайте определение класса сложности P. Приведите примеры задач, принадлежащих этому классу.

Вопросы к разделу 2.

1. Что такое NP-полные задачи? Почему они занимают особое место в теории сложности?
2. Объясните понятие полиномиальной сводимости (Karp-сводимости).
3. В чем заключается проблема P vs NP? Каковы ее практические последствия?

4. Опишите алгоритм верификатора для NP-задач.
5. Что такое класс co-NP? Приведите пример co-NP-полной задачи.
6. Объясните различия между классами сложности P, NP и EXP.
7. Что такое псевдополиномиальные алгоритмы? Приведите пример.
8. Опишите метод сведения для доказательства NP-полноты задачи.
9. Что такое параметризованная сложность и класс FPT?

Вопросы к разделу 3.

1. Дайте определение блочному шифру. Чем он отличается от поточного?
2. Опишите структуру сети Фейстеля. Какие ее преимущества?
3. Объясните принцип работы SP-сети на примере AES.
4. Что такое S-блоки и каким требованиям они должны удовлетворять?
5. Перечислите и охарактеризуйте основные режимы работы блочных шифров.
6. В чем заключаются основные уязвимости режима ECB?
7. Опишите алгоритм DES. Почему он считается устаревшим?
8. Каковы основные особенности алгоритма ГОСТ 28147-89?
9. Объясните процедуру расширения ключа в AES.
10. Что такое атаки "встреча посередине" и дифференциальный криптоанализ?
11. Дайте определение поточного шифра. Чем он отличается от блочного?
12. Опишите принцип работы синхронного поточного шифра.
13. Что такое самосинхронизирующийся поточный шифр?
14. Перечислите основные требования к ключевому потоку.
15. Опишите структуру генератора ключевого потока на основе регистров сдвига с линейной обратной связью (РСЛОС).

Вопросы к разделу 4

1. Опишите алгоритм RC4. Какие у него есть преимущества и недостатки?
2. Где применяются поточные шифры в современных информационных системах?
3. На чем основана криптографическая стойкость RSA?
4. Объясните, почему в RSA выбирают простые числа p и q примерно одинаковой длины.
5. Что такое функция Эйлера и как она вычисляется для $n = p \times q$?
6. Почему необходимо выбирать e взаимно простым с $\varphi(n)$?
7. Как вычисляется секретная экспонента d?
8. Какие атаки возможны на RSA и как от них защищаться?
9. Что такое схема дополнения OAEP и зачем она нужна?
10. Объясните китайскую теорему об остатках и ее применение в RSA.
11. Чем отличается практическое применение RSA от теоретического описания?
    Какие современные рекомендации по длине ключей RSA существуют

Вопросы к разделу 5

1. Дайте определение цифровой подписи. Чем она отличается от простой электронной подписи?
2. Опишите принцип работы асимметричной криптографии в контексте ЭЦП.
3. Каковы основные цели использования цифровой подписи?
4. Объясните, почему для создания ЭЦП обычно используется связка «хэш-функция + шифрование закрытым ключом».
5. Перечислите основные свойства цифровой подписи и дайте краткую характеристику каждому.

6. Что такое «неотказуемость» и почему это важнейшее свойство ЭЦП?
7. Объясните разницу между присоединённой и отсоединённой цифровой подписью.
8. Какие угрозы безопасности предотвращает корректно реализованная система ЭЦП?
9. Опишите типовой алгоритм формирования цифровой подписи.
10. Опишите типовой алгоритм проверки цифровой подписи.
11. Что такое сертификат открытого ключа и какова его роль в инфраструктуре ЭЦП?
12. Назовите распространённые алгоритмы цифровой подписи (RSA, DSA, ECDSA).
13. Какие виды ЭЦП установлены в законодательстве РФ (ФЗ-63 «Об электронной подписи»)?
14. В каких сферах деятельности наиболее востребована квалифицированная электронная подпись?
15. Какие юридические последствия влечёт использование ЭЦП

Контрольные вопросы
по дисциплине «Криптография»

Вопросы к коллоквиуму

по дисциплине «Криптография»

Вопросы к разделу 1.

7. Главное отличие шифра перестановки от шифра замены
8. Дайте математическое определение аффинному шифру. При каких условиях он корректно определен?
9. Опишите алгоритм частотного криптоанализа шифра простой замены.
10. Объясните, как с помощью индекса совпадений можно определить длину ключа в шифре Виженера.
11. Криптографическая слабость шифра Цезаря и аффинного шифра
12. Дайте определение класса сложности P. Приведите примеры задач, принадлежащих этому классу.

Вопросы к разделу 2.

10. Что такое NP-полные задачи? Почему они занимают особое место в теории сложности?
11. Объясните понятие полиномиальной сводимости (Karp-сводимости).
12. В чем заключается проблема P vs NP? Каковы ее практические последствия?
13. Опишите алгоритм верификатора для NP-задач.

Вопросы к разделу 3.

16. Дайте определение блочному шифру. Чем он отличается от поточного?
17. Опишите структуру сети Фейстеля. Какие ее преимущества?
18. Объясните принцип работы SP-сети на примере AES.
19. Что такое S-блоки и каким требованиям они должны удовлетворять?
20. Перечислите и охарактеризуйте основные режимы работы блочных шифров.
21. В чем заключаются основные уязвимости режима ECB?
22. Опишите алгоритм DES. Почему он считается устаревшим?
23. Каковы основные особенности алгоритма ГОСТ 28147-89?
24. Перечислите основные требования к ключевому потоку.
25. Опишите структуру генератора ключевого потока на основе регистров сдвига с линейной обратной связью (РСЛОС).

Вопросы к разделу 4

12. Опишите алгоритм RC4. Какие у него есть преимущества и недостатки?
13. Где применяются поточные шифры в современных информационных системах?
14. На чем основана криптографическая стойкость RSA?
15. Объясните, почему в RSA выбирают простые числа p и q примерно одинаковой длины.
16. Что такое функция Эйлера и как она вычисляется для $n = p \times q$?
17. Почему необходимо выбирать e взаимно простым с $\varphi(n)$?
18. Как вычисляется секретная экспонента d?

Вопросы к разделу 5

16. Дайте определение цифровой подписи. Чем она отличается от простой электронной подписи?
17. Опишите принцип работы асимметричной криптографии в контексте ЭЦП.
18. Каковы основные цели использования цифровой подписи?
19. Объясните, почему для создания ЭЦП обычно используется связка «хэш-функция + шифрование закрытым ключом».
20. Перечислите основные свойства цифровой подписи и дайте краткую характеристику каждому.
21. Что такое «неотказуемость» и почему это важнейшее свойство ЭЦП?
22. Объясните разницу между присоединённой и отсоединённой цифровой подписью.
23. Какие угрозы безопасности предотвращает корректно реализованная система ЭЦП?

Темы рефератов

по дисциплине «Криптография»

1. Криптографические системы защиты данных
2. Разработка алгоритмов криптографических примитивов
3. Криптографические методы
4. Различные алгоритмы шифрования
5. Криптографические методы
6. Актуальные виды тестирования для блокчейн – приложений
7. Функциональное тестирование для блокчейн – приложений
8. Особенности блокчейн тестирования
9. Области применения технологии блокчейна
10. Цифровые технологии в образовании
11. Цифровые технологии в промышленности
12. Преимущества и недостатки технологии блокчейна
13. Принципы функционирования технологии блокчейна на примере биткоина.
14. Постквантовая криптография (PQC) — самое востребованное направление
15. Криптографические примитивы нового поколения
16. Криптография и блокчейн / Криптовалют
17. Криптография и конфиденциальность данных

Индивидуальные задания к лабораторным работам
по дисциплине «Криптография»

Лабораторная работа №1 Классические шифры и их криптоанализ. Математическая формализация

Индивидуальные задания:

Общая структура задания для каждого варианта:

1. Теоретическая задача на математическую формализацию.
2. Практическая задача на шифрование/дешифрование.
3. Задача на криптоанализ (вскрытие шифртекста без ключа).

Вариант 1

1. **Теория:** Дайте формальное определение шифру перестановки с ключом в виде квадратной таблицы n×n и маршрута заполнения/чтения. Запишите функции E и D.
2. **Шифрование:** Зашифруйте фразу "КРИПТОГРАФИЯ" шифром Цезаря со сдвигом b=5 (русский алфавит, 33 буквы, "А"=0).
3. **Криптоанализ:** Вскройте методом частотного анализа (используйте таблицы частот букв русского языка). Известно, что использован шифр простой замены. **Шифртекст:** "ЮООЖТЁ СЖТБЁВФЁЗ Р ФТИУФТДФВУФЗ ЖТИВФТС".

Вариант 2

1. **Теория:** Выведите формулу для функции дешифрования D(y) в аффинном шифре E(x) = (a*x + b) mod N. Укажите условие существования обратной функции.
2. **Шифрование:** Зашифруйте слово "ЗАЩИТА", используя аффинный шифр с параметрами a=5, b=8 (алфавит 33 буквы).
3. **Криптоанализ:** Определите длину ключа для шифра Виженера, используя метод Касиски/индекс совпадений. **Шифртекст:** "ЬЛХВУЧЁТДХ ЬСШПРЁТДХ Л ДХЛОТПРЛН Р ЬСШУМХЙЛВ".

(Варианты 3-10 имеют аналогичную структуру с разными шифрами, параметрами и текстами для анализа. Примеры других заданий: анализ шифра "железнодорожной изгороди", взлом аффинного шифра перебором, формализация шифра Виженера, полиалфавитный шифр с автоключом и т.д.)

Вариант 3

1. **Теория:** Опишите формальную модель шифра Вернама (одноразового блокнота) и докажите его абсолютную стойкость при выполнении условий.
2. **Шифрование:** Выполните перестановку биграмм для слова "ПАРОЛЬ", используя ключевую перестановку (2,1) (разбить на биграммы ПА РО ЛЬ, переставить в каждой биграмме символы согласно ключу).
3. **Криптоанализ:** Перед вами шифртекст, полученный с помощью шифра перестановки (таблица 4x4, чтение по столбцам в порядке, заданном ключевым словом). Восстановите открытый текст. **Шифртекст:** "ЕШЁНР_ИАСЕ_КЗ_ВТ".

Вариант 4

1. **Теория:** Формально опишите **шифр Гронсфельда** (числовой вариант шифра Виженера). Запишите функцию шифрования E(k, p), где ключ k — числовая последовательность из цифр 0-9, а p — буква открытого текста.
2. **Шифрование:** Зашифруйте слово **"КОД"** с помощью шифра Гронсфельда с ключом 4215. Используйте русский алфавит (33 буквы, А=0). Процедуру повтора ключа применить.
3. **Криптоанализ:** Вам дан шифртекст, полученный с помощью **шифра Цезаря** (простой сдвиг). Определите ключ (сдвиг) и расшифруйте сообщение. Известно, что в тексте есть слово **"шифр"**.
   Шифртекст: "ЁЛЗПТЩЙЗ ЙЛО ЫРЛЕПЗ ДЩЙПТСФР".

Вариант 5

1. **Теория:** Дайте математическое определение **шифру "двойной квадрат" (шифр Плейфейра для кириллицы)**. Опишите алгоритм шифрования биграммы (p1, p2) с помощью двух заранее составленных таблиц 5x6.
2. **Шифрование:** Зашифруйте биграмму **"ТО"**, используя следующие таблицы (чтение по строкам). Если буквы в строке/столбце, сдвиг вправо/вниз.
   Таблица 1 (ключ "АЛГОРИТМ"): А Л Г О Р / И Т М Б В / В Г Д Е Ё / Ж З И Й К / ... (остальные буквы по порядку)
   Таблица 2 (ключ "ШИФР"): Ш И Ф Р А / Б В Г Д Е / Ё Ж З И Й / ...
   Примечание: Для полноты задания студентам должны быть предоставлены полностью заполненные таблицы.
3. **Криптоанализ:** Проведите **частотный анализ первого порядка** (частоты букв) для приведённого шифртекста. Сделайте предположение о типе шифра (моно- или полиалфавитный), обоснуйте ответ. **Шифртекст:** "ЦВФЗЬЦ ЫЖИЁЖЦ ЧСЁДЦБ Ц СЁЗФЁДШЗФД" (текст короткий, специально составлен для демонстрации неровности частот).

Вариант 6

1. **Теория:** Постройте математическую модель **шифра простой перестановки с фиксированным периодом** d. Ключ — перестановка чисел {1, 2, ..., d}. Запишите функцию шифрования блока (p1, p2, ..., pd).
2. **Шифрование:** Зашифруйте фразу **"СЕКРЕТНЫЙ ДОКУМЕНТ"**, используя шифр перестановки с периодом d=5 и ключом (3, 1, 4, 5, 2). Незначащие символы (для выравнивания) заменяйте буквой "Х".
3. **Криптоанализ:** Перед вами шифртекст, зашифрованный с помощью **аффинного шифра** на русском алфавите (33 буквы). Ключ неизвестен. Найдите все возможные ключи (a, b), для которых существует обратная функция дешифрования. Сколько их? Если известно, что самая частая буква шифртекста "Щ" соответствует самой частой букве русского языка, предложите гипотезу для ключа.
   Шифртекст (очень короткий, для перебора): "ЩРЁХ".

Вариант 7

1. **Теория:** Опишите алгоритм и формализуйте **шифр "железнодорожная изгородь" (Rail Fence Cipher)**. Запишите функцию E(k, P), где k — количество "рельсов" (строк), P — последовательность символов.
2. **Шифрование:** Зашифруйте текст **"КРИПТОАНАЛИЗ"** с помощью "железнодорожной изгороди" с k=3 рельсами.
3. **Криптоанализ:** Вскройте шифртекст, полученный с помощью **моноалфавитной замены** (шифр простой подстановки). Используйте не только частоты отдельных букв, но и знание о самых частых биграммах и триграммах русского языка (**"СТ"**, **"НО"**, **"ТО"**, **"НА"**, **"ЕН"**).

   Шифртекст: "П ФЯМЁИХЯФЮМ МЯЖЮ ЬР ФЯМЁИХЯФЮЬР ЖФЮВРМРМШЯФ".

   Подсказка: Обратите внимание на повторяющиеся длинные фрагменты (например, "ФЯМЁИХЯФЮ"), что характерно для шифра простой замены.

Вариант 8

1. **Теория:** Формализуйте понятие **взлома шифра по известному открытому тексту (Known-plaintext attack)**. Для шифра Виженера опишите, как, зная пару (P, C), можно восстановить ключ или его фрагмент. Выведите формулу для нахождения i-го символа ключа.
2. **Шифрование:** Реализуйте шифр **атбаш** для русского алфавита (зеркальное отображение: А↔Я, Б↔Ю и т.д.). Зашифруйте слово **"АБВГД"**.
3. **Криптоанализ: Задача на интуицию и логику.** Вам дан шифртекст, который, как известно, является результатом применения двух классических шифров **последовательно**: сначала перестановка, затем простая замена. Предложите общий план атаки на такую композицию. Каким этапом нужно заниматься в первую очередь? Почему?

   Шифртекст (для размышления): "ЬИРАП ЫД ЕНРЁНСВЕИ В ЫЩЗЁН".

   Ответ студента должен содержать рассуждение о том, что атаку следует начинать с вскрытия перестановки (которая не меняет частотный профиль), а затем применять частотный анализ к промежуточному тексту.

Лабораторная работа №2 Теория сложности вычислений

Индивидуальные задания:

Вариант 1

Задание: Докажите, что задача о клике является NP-полной, используя сведение от задачи о вершинном покрытии.

Указания:

1. Дайте формальное определение задачи о клике
2. Напомните определение задачи о вершинном покрытии и ее NP-полноту

3. Постройте преобразование экземпляра задачи о вершинном покрытии в экземпляр задачи о клике
4. Докажите эквивалентность решений
5. Покажите, что преобразование выполняется за полиномиальное время

Вариант 2

Задание: Проанализируйте задачу разбиения (Partition) и докажите, что она является NP-полной.

Указания:

1. Сформулируйте задачу разбиения
2. Сведите к ней задачу о рюкзаке (Knapsack)
3. Определите преобразование экземпляров
4. Докажите корректность сведения
5. Оцените временную сложность преобразования

Вариант 3

Задание: Исследуйте задачу о гамильтоновом цикле в направленном графе. Докажите ее NP-полноту через сведение от задачи о вершинном покрытии.

Указания:

1. Опишите конструкцию гаджетов для вершин и ребер
2. Определите правила построения графа-примера
3. Докажите, что гамильтонов цикл существует тогда и только тогда, когда существует вершинное покрытие определенного размера
4. Проанализируйте размер построенного графа

Вариант 4

Задание: Рассмотрите задачу 3-раскраски графа. Докажите ее NP-полноту, используя сведение от задачи 3-выполнимости (3-SAT).

Указания:

1. Постройте гаджеты для переменных и клозов
2. Определите соединения между гаджетами
3. Докажите эквивалентность выполнимости формулы и раскрашиваемости графа
4. Покажите, что граф может быть 3-раскрашен тогда и только тогда, когда формула выполнима

Вариант 5

Задание: Исследуйте задачу о сумме подмножества (Subset Sum). Разработайте псевдополиномиальный алгоритм решения этой задачи.

Указания:

1. Сформулируйте задачу о сумме подмножества
2. Разработайте алгоритм на основе динамического программирования
3. Проанализируйте временную сложность алгоритма
4. Объясните, почему алгоритм является псевдополиномиальным
5. Приведите пример работы алгоритма

Вариант 6

Задание: Докажите, что задача о раскраске графа в 2 цвета принадлежит классу P.

Указания:

1. Сформулируйте задачу 2-раскраски (задачу о двудольности)
2. Предложите алгоритм проверки двудольности графа
3. Докажите корректность алгоритма
4. Проанализируйте временную сложность
5. Приведите пример работы алгоритма

Вариант 7

Задание: Исследуйте связь между классами P, NP и co-NP. Докажите, что если P = NP, то P = NP = co-NP.

Указания:

1. Дайте определения классов P, NP и co-NP
2. Докажите, что $P \subseteq NP \cap co\text{-}NP$
3. Покажите, что если P = NP, то $NP \subseteq co\text{-}NP$
4. Докажите, что из этого следует $co\text{-}NP \subseteq NP$
5. Сделайте вывод о равенстве классов

Вариант 8

Задание: Рассмотрите задачу коммивояжера (TSP). Проанализируйте ее принадлежность классу NP и докажите NP-полноту ее варианта принятия решения.

Указания:

1. Сформулируйте задачу коммивояжера в варианте принятия решения
2. Докажите принадлежность задачи классу NP
3. Сведите к ней задачу о гамильтоновом цикле
4. Докажите корректность сведения
5. Обсудите метрический вариант задачи

Вариант 9

Задание: Исследуйте класс PSPACE. Докажите, что задача проверки истинности формул логики предикатов в пропозициональной логике (TQBF) является PSPACE-полной.

Указания:

1. Дайте определение класса PSPACE
2. Сформулируйте задачу TQBF
3. Докажите принадлежность TQBF классу PSPACE
4. Выберите подходящую PSPACE-полную задачу для сведения
5. Постройте сведение и докажите его корректность

Вариант 10

Задание: Проанализируйте параметризованную сложность задачи о вершинном покрытии. Докажите, что она принадлежит классу FPT.

Указания:

1. Дайте определение параметризованной задачи и класса FPT
2. Сформулируйте параметризованную задачу о вершинном покрытии
3. Разработайте алгоритм с ветвлением (branching algorithm)
4. Проанализируйте время работы алгоритма: O(2^k * n)
5. Докажите корректность алгоритма

Лабораторная работа №3 Блочные шифры

Индивидуальные задания :

Вариант 1

1. Зашифруйте текст "CRYPTO" с помощью алгоритма DES в режиме ECB (используйте учебный пример с ключом 0x133457799BBCDFF1).
2. Проанализируйте уязвимости режима ECB на примере шифрования bitmap-изображения.
3. Реализуйте один раунд упрощенного шифра Фейстеля с 4-битными блоками.

Вариант 2

1. Выполните процедуру расширения ключа для AES-128 для ключа: 0x2b7e151628aed2a6abf7158809cf4f3c (первые 3 раунда).
2. Сравните структуры сетей Фейстеля и SP-сети.
3. Зашифруйте сообщение "HELLO" в режиме CBC с использованием упрощенного DES.

Вариант 3

1. Проанализируйте S-блоки алгоритма ГОСТ 28147-89 и их криптографические свойства.
2. Реализуйте режим CTR для блочного шифра с 8-битными блоками.
3. Объясните принцип атаки "встреча посередине" на двойной DES.

Вариант 4

1. Выполните операцию MixColumns для AES для заданного столбца.
2. Исследуйте проблему дополнения данных в режимах CBC и ECB.
3. Разработайте учебный пример дифференциального криптоанализа для 3-раундового упрощенного DES.

Вариант 5

1. Сравните производительность аппаратных реализаций AES и ГОСТ 28147-89.
2. Реализуйте процедуру генерации раундовых ключей для ГОСТ 28147-89.
3. Проанализируйте устойчивость различных режимов работы к ошибкам передачи данных.

Вариант 6

1. Выполните операцию SubBytes для AES для заданного состояния.
2. Исследуйте влияние размера блока на безопасность шифра.
3. Разработайте схему блочного шифра на основе сети Фейстеля с 64-битными блоками.

Вариант 7

1. Проанализируйте эволюцию блочных шифров от DES к AES.
2. Реализуйте режим OFB для учебного блочного шифра.
3. Исследуйте концепцию побитового распространения ошибок в различных режимах.

Вариант 8

1. Выполните процедуру KeyExpansion для AES-192.
2. Сравните требования к S-блокам в DES и AES.
3. Разработайте учебный пример линейного криптоанализа для упрощенного шифра.

Вариант 9

1. Проанализируйте особенности российского стандарта ГОСТ 28147-89.
2. Реализуйте процедуру добавления раундового ключа в AES.

3. Исследуйте проблему инициализации векторов в режимах CBC и CFB.

Вариант 10

1. Выполните полный раунд AES для заданного состояния и ключа.
2. Сравните аппаратную и программную эффективность современных блочных шифров.
3. Разработайте протокол использования блочного шифра с аутентификацией данных.

Лабораторная работа №4 Поточные шифры

Индивидуальные задания:

Вариант 1

1. Даны РСЛОС длиной 5 бит с полиномом обратной связи f(x) = x^5 + x^2 + 1. Начальное состояние: 10011. Вычислите 10 бит выходной последовательности.
2. Проанализируйте стойкость шифра Vernam при использовании действительно случайного ключа и псевдослучайного ключа.
3. Разработайте схему нелинейного комбинированного генератора на основе трех РСЛОС и нелинейной функции мажоритарности.

Вариант 2

1. Зашифруйте сообщение "CRYPTO" с помощью поточного шифра, используя ключевой поток 010011100101... (представьте буквы в ASCII/двоичном виде).
2. Вычислить линейную сложность последовательности 010011000111...
3. Опишите атаку на суммирующий генератор с известными фазами регистров.

Вариант 3

1. Постройте нелинейный фильтрующий генератор на основе РСЛОС длины 6 и нелинейной фильтрующей функции f(x1,x2,x3,x4) = x1x2 ⊕ x3x4.
2. Проанализируйте период последовательности РСЛОС с примитивным полиномом x^4 + x + 1.
3. Сравните синхронные и самосинхронизирующиеся поточные шифры по критериям безопасности и эффективности.

Вариант 4

1. Даны два РСЛОС длины L1=3 и L2=4. Постройте генератор с перемежающимся шагом (shrinking generator).
2. Выполните корреляционный анализ для генератора Геффе.
3. Опишите принцип работы шифра A5/1, используемого в GSM.

Вариант 5

1. Реализуйте алгоритм RC4 для ключа "KEY" (представьте первые 10 байт ключевого потока).
2. Проанализируйте уязвимости RC4 и причины его отказа в современных протоколах.
3. Разработайте метод восстановления состояния РСЛОС по известному отрезку выходной последовательности.

Вариант 6

1. Постройте самосинхронизирующийся поточный шифр на основе обратной связи по шифртексту.

2. Вычислите взаимную информацию между входом и выходом нелинейного комбинирующего узла.
3. Опишите атаку "двойного использования" гаммы и методы ее предотвращения.

Вариант 7

1. Спроектируйте поточный шифр на основе блочного в режиме CTR или OFB.
2. Проанализируйте криптостойкость генератора с чередованием (alternating step generator).
3. Дайте сравнительную характеристику поточных шифров SEAL, RC4 и ChaCha20.

Вариант 8

1. Решите систему линейных уравнений для восстановления начального состояния РСЛОС.
2. Постройте схему дифференциального анализа поточного шифра.
3. Опишите методы тестирования статистических свойств ключевых потоков.

Вариант 9

1. Реализуйте алгоритм генерации ключевого потока с использованием хеш-функции в режиме выработки псевдослучайной последовательности.
2. Проанализируйте устойчивость поточного шифра к атакам на основе известного открытого текста.
3. Опишите принцип работы современного поточного шифра ChaCha20.

Вариант 10

1. Разработайте протокол обмена ключами для поточного шифра с использованием асимметричной криптографии.
2. Выполните оценку линейной сложности и периода для заданной последовательности.
3. Проанализируйте преимущества и недостатки аппаратной и программной реализации поточных шифров.

Лабораторная работа №5 Криптосистема RSA

Индивидуальные задания:

Вариант 1

Дано: p = 17, q = 19, e = 5

Задания:

1. Сгенерировать ключи RSA
2. Зашифровать сообщение M = 88
3. Расшифровать полученный шифротекст

Вариант 2

Дано: p = 13, q = 23, e = 7

Задания:

1. Вычислить φ(n) и проверить условие для e
2. Найти секретную экспоненту d
3. Зашифровать M = 123

Вариант 3

Дано: n = 323, e = 5

Задания:

1. Определить p и q (факторизовать n)
2. Найти закрытый ключ
3. Расшифровать C = 101

Вариант 4

Дано: p = 31, q = 37, M = 256

Задания:

1. Выбрать подходящее e из {3, 17, 19}
2. Выполнить шифрование
3. Проверить корректность дешифрования

Вариант 5

Дано: e = 65537, p = 61, q = 53

Задания:

1. Сгенерировать ключи
2. Проанализировать стойкость системы
3. Зашифровать свое ФИО (по таблице ASCII)

Вариант 6

Дано: n = 187, e = 7, C = 11

Задания:

1. Факторизовать n
2. Найти закрытый ключ
3. Расшифровать сообщение

Вариант 7

Дано: p = 41, q = 43, e = 11

Задания:

1. Проверить, является ли e допустимым
2. Зашифровать M = 1000
3. Оценить время факторизации n методом перебора

Вариант 8

Дано: два шифротекста, зашифрованных одним ключом

Задания:

1. Описать атаку на основе общего модуля
2. Показать математически возможность атаки
3. Предложить меры защиты

Вариант 9

Дано: p = 101, q = 103, e = 3

Задания:

1. Объяснить проблему малой экспоненты
2. Зашифровать три разных сообщения
3. Показать уязвимость

Вариант 10

Дано: Реализованная система RSA с малыми параметрами
Задания:

1. Провести атаку временными характеристиками
2. Описать countermeasures
3. Предложить улучшенную реализацию

Лабораторная работа №6 Понятие и свойства цифровой подписи

Индивидуальные задания:

Вариант 1

Тема: Сравнительный анализ симметричной и асимметричной криптографии

Задание:

1. Подготовьте таблицу сравнения симметричной и асимметричной криптографии по 5 параметрам.
2. Объясните, почему для цифровой подписи используется именно асимметричная криптография.
3. Приведите 2 примера реального применения симметричной криптографии в системах с ЭЦП.

Вариант 2

Тема: Хэш-функции в процессе формирования ЭЦП

Задание:

1. Опишите роль хэш-функции в процессе создания цифровой подписи.
2. Перечислите требования к криптографическим хэш-функциям.
3. Сравните алгоритмы SHA-256 и ГОСТ Р 34.11-2012 по 3 параметрам.

Вариант 3

Тема: Алгоритм RSA для цифровой подписи

Задание:

1. Опишите математические основы алгоритма RSA.
2. Приведите пошаговый алгоритм формирования и проверки подписи RSA.
3. Перечислите преимущества и недостатки RSA для ЭЦП.

Вариант 4

Тема: Эллиптические кривые в цифровой подписи (ECDSA)

Задание:

1. Объясните, почему цифровые подписи на эллиптических кривых считаются перспективными.
2. Сравните ECDSA и RSA по размерам ключей при равной криптостойкости.
3. Приведите 2 области, где применение ECDSA наиболее целесообразно.

Вариант 5

Тема: Инфраструктура открытых ключей (PKI)

Задание:

1. Опишите архитектуру PKI и её основные компоненты.

2. Объясните жизненный цикл сертификата открытого ключа.
3. Нарисуйте схему взаимодействия участников PKI при проверке ЭЦП.

Вариант 6

Тема: Юридическая сила цифровой подписи

Задание:

1. Сравните простую, усиленную неквалифицированную и усиленную квалифицированную ЭЦП по юридической силе.
2. Приведите 3 примера документов, которые могут быть подписаны квалифицированной ЭЦП с полной юридической силой.
3. Опишите процедуру судебного оспаривания документа, подписанного ЭЦП.

Вариант 7

Тема: Отечественные стандарты ЭЦП

Задание:

1. Опишите алгоритм цифровой подписи по ГОСТ Р 34.10-2012.
2. Сравните требования к ключам в ГОСТ Р 34.10-2012 и RSA.
3. Приведите примеры госорганов и систем, где обязательна ЭЦП по ГОСТ.

Вариант 8

Тема: Удостоверяющие центры

Задание:

1. Опишите функции удостоверяющего центра в системе ЭЦП.
2. Перечислите требования к аккредитованным УЦ в РФ.
3. Разработайте схему взаимодействия УЦ, владельца сертификата и проверяющего.

Вариант 9

Тема: Смарт-карты и токены для хранения ключей ЭЦП

Задание:

1. Опишите преимущества аппаратного хранения ключей ЭЦП.
2. Сравните смарт-карты, USB-токены и HSM по безопасности хранения ключей.
3. Опишите типовой сценарий использования токена для подписания документа.

Вариант 10

Тема: Области применения цифровой подписи

Задание:

1. Приведите 5 различных областей применения ЭЦП с примерами.
2. Опишите использование ЭЦП в системе электронного документооборота.
3. Проанализируйте перспективы развития ЭЦП в блокчейн-технологиях.

1. **Шифр, в котором буква открытого текста заменяется на одну и ту же букву шифртекста на протяжении всего сообщения, называется:**
    a) Полиалфавитный
    b) Моноалфавитный
    c) Перестановочный
    d) Блочный
2. **Для русского алфавита (33 буквы) количество возможных ключей в шифре Цезаря равно:**
    a) 33
    b) 33! (факториал)
    c) 32
    d) 66
3. **Индекс совпадений для осмысленного русского текста, зашифрованного шифром Виженера с длинным ключом, для всего текста целиком будет:**
    a) Стремиться к 0.065
    b) Стремиться к 0.0385
    c) Равен 1
    d) Не определен

4. **Функция расшифрования для шифра Цезаря** $E(x) = (x+3) \bmod 33$ **имеет вид:**
    _____

5. **Метод Касиски используется для:**

    _____

6. **Какое из следующих утверждений о классе P верно?**
    a) Все задачи в P решаются за полиномиальное время на недетерминированной машине Тьюринга
    b) Если задача принадлежит P, то она обязательно разрешима
    c) Задача коммивояжера принадлежит классу P
    d) Класс P включает все задачи, для которых существует верификатор с полиномиальным временем работы

Ответ: 2 (Если задача принадлежит P, то она обязательно разрешима)

7. Для доказательства NP-полноты задачи необходимо:
a) Показать, что задача принадлежит классу P
b) Показать, что задача принадлежит классу NP и свести к ней некоторую NP-полную задачу
c) Показать, что задача не принадлежит классу P d)Построить для задачи полиномиальный алгоритм

8.Если будет доказано, что P = NP, то:

а) Все NP-задачи станут неразрешимыми

b) Для всех NP-задач будут найдены полиномиальные алгоритмы
c) Все NP-полные задачи останутся практически неразрешимыми
d) Класс P перестанет существовать

9. Задача выполнимости булевых формул (SAT) является:

a) P-
полной
b)NP-полной
c)PSPACE-полной
d)Нераспознаваемой

10. Класс co-NP включает задачи:

a) Дополнения которых принадлежат классу NP
b) Которые решаются за полиномиальное время на квантовых компьютерах
c) Которые являются подмножеством P
d) Которые не могут быть верифицированы за полиномиальное время

11. Размер блока в алгоритме AES составляет:

a) 64 бита
b) 128 бит
c) 256 бит
d) 512 бит

12. Структуру сети Фейстеля используют:

a) только DES
b) DES и ГОСТ 28147-89
c) только AES
d) все современные блочные шифры

13. Режим работы блочного шифра, наиболее уязвимый к анализу шаблонов:

a) CBC
b) ECB
c) CFB
d) OFB

14. Количество раундов в AES-256:

a) 10
b) 12
c) 14
d) 16

15. Размер ключа в ГОСТ 28147-89 составляет:

a) 128 бит

b) 192 бита

c) 256 бит
d) 512 бит

16. Основная операция в функции раунда AES:

_____

17. Режим, позволяющий шифрование данных произвольной длины без дополнения:
a) ECB
b) CBC
c) CFB
d) Все перечисленные

18. Атака, основанная на анализе различий в парах открытых текстов:
a) Линейный криптоанализ
b) Атака по времени
c) Дифференциальный криптоанализ
d) Атака "встреча посередине"

19. Что является основной операцией в большинстве поточных шифров?

A) Перестановка
B) Сложение по модулю 2 (XOR)
C) Арифметические операции
D) Подстановка

20. Какой из перечисленных генераторов является линейным?

A) RC4
B) РСЛОС
C) Генератор Геффе
D) Часы остановки

21. Минимальная длина регистра сдвига, обеспечивающая максимальный период последовательности при правильном выборе полинома обратной связи:

A) N бит, период 2^N
B) N бит, период 2^N – 1
C) N бит, период N^2
D) N бит, период N!

22. Что такое инициализирующий вектор (IV) в поточных шифрах?

A) Дополнительный секретный ключ
B) Открытый параметр, обеспечивающий уникальность ключевого потока
C) Результат шифрования
D) Часть открытого текста

23. Какой атаке подвержены поточные шифры при повторном использовании ключевого потока?

A) Редукции ключа

B) Корреляционной атаке

C) Атаке на основе известного открытого текста

D) Разделению потоков (C1⊕C2 = P1⊕P2)

24. Что такое RSA?_____

25. Какие два основных простых числа используются при генерации ключей RSA?

a) p и q

b)e и d

c) n и φ(n)

d) M и C

26. Что вычисляется как n = p × q в RSA?

a) Открытая

экспонента

b)Секретная экспонента

c)Модуль шифрования

d)Функция Эйлера

27. Как вычисляется функция Эйлера φ(n) для n = p×q, где p и q — простые?

a)φ(n) = n - 1

b)φ(n) = p + q

c)φ(n) = (p-1)(q-1)

d)φ(n) = p×q - p - q

28. Какое условие должно выполняться для открытой экспоненты e?

a) e должно быть простым числом

b) e должно быть больше φ(n)

c) 1 < e < φ(n) и НОД(e, φ(n)) = 1

d) e должно быть степенью двойки

29. Как выполняется шифрование сообщения M в RSA?

a)C = M + e (mod n)

b)C = M^e mod n

c)C = e^M mod n

d)C = M × e mod n

30. Что произойдет, если для шифрования использовать закрытый ключ?

a) Это невозможно математически

b)Получится электронная подпись

c)Сообщение будет уничтожено

d)Получится симметричное шифрование

31. Почему в RSA сообщение M должно быть меньше n?

a) Это требование алгоритма Диффи-Хеллмана

b) Потому что операции выполняются по модулю n

c) Иначе нарушится работа функции Эйлера

d) Это не обязательно, но рекомендуется

32. Что является основной математической основой цифровой подписи?

a) Симметричное

шифрование b)Хэш-функции

c)Асимметричное шифрование

d)Стеганография

33. Какое свойство ЭЦП гарантирует, что подписавший документ не сможет впоследствии отказаться от факта подписания?

a) Конфиденциальн
ость b)Неотказуемость
c)Целостность
d)Аутентичность

34. Какой ключ используется для проверки цифровой подписи?

a) Открытый ключ подписанта
b) Закрытый ключ
подписанта c)Симметричный
ключ d)Сеансовый ключ

35. Что из перечисленного НЕ является свойством цифровой подписи?

a) Установление авторства
b)Обеспечение целостности документа
c)Гарантия конфиденциальности документа
d)Обеспечение неотказуемости

36. Какой элемент инфраструктуры ЭЦП подтверждает принадлежность открытого ключа определённому лицу?

a) Хэш-функция
b) Сертификат открытого ключа+
c) Закрытый ключ
d)Электронный документ

5 Методические материалы, определяющие процедуры оценивания компетенции

5.1 Критерии оценивания качества устного ответа

Оценка **«отлично»** выставляется за глубокое знание предусмотренного программой материала, за умение четко, лаконично и логически последовательно отвечать на поставленные вопросы.
Оценка **«хорошо»** – за твердое знание основного (программного) материала, за грамотные, без существенных неточностей ответы на поставленные вопросы.
Оценка **«удовлетворительно»** – за общее знание только основного материала, за ответы, содержащие неточности или слабо аргументированные, с нарушением последовательности изложения материала.
Оценка **«неудовлетворительно»** – за незнание значительной части программного материала, за существенные ошибки в ответах на вопросы, за неумение ориентироваться в материале, за незнание основных понятий дисциплины.

Критерии оценки:

При тестировании все верные ответы берутся за 100%.
90%-100% отлично
75%-90% хорошо
60%-75% удовлетворительно
менее 60% неудовлетворительно

5.2 Критерии оценивания зачета

Оценка **«зачтено»** выставляется обучающемуся, если обучающийся почти ответил на все вопросы, поставленные преподавателем на защите.
Оценка **«не зачтено»** выставляется обучающемуся, если обучающийся не проявил глубоких теоретических знаний при ответе на вопросы

5.3 Критерии оценивания практического задания

Оценке «зачтено» Данная оценка ставится в том случае, если обучающийся показал полное усвоение программного материала и не допустил каких-либо ошибок, неточностей, своевременно и правильно выполнил задания на занятии, проявил при этом оригинальное мышление, своевременно и без каких-либо ошибок продемонстрировал работу программного приложения.

Оценке «не зачтено». Данная оценка ставится в том случае, если обучающийся не освоил программный материал своевременно не выполнил и не продемонстрировал разработанное программное приложение .

5.4 Критерии оценивания результатов освоения дисциплины

Оценка **«отлично»** выставляется за глубокое знание предусмотренного программой материала, содержащегося в основных и дополнительных рекомендованных литературных источниках, за умение четко, лаконично и логически последовательно отвечать на поставленные вопросы, за умение анализировать изучаемые явления в их взаимосвязи и диалектическом развитии, применять теоретические положения при решении практических задач.
Оценка **«хорошо»** – за твердое знание основного (программного) материала, включая расчеты (при необходимости), за грамотные, без существенных неточностей ответы на поставленные вопросы, за умение применять теоретические положения для решения практических задач.
Оценка **«удовлетворительно»** – за общее знание только основного материала, за ответы, содержащие неточности или слабо аргументированные, с нарушением последовательности изложения материала, за слабое применение теоретических положений при решении практических задач.
Оценка **«неудовлетворительно»** – за незнание значительной части программного материала, за существенные ошибки в ответах на вопросы, за неумение ориентироваться в расчетах, за незнание основных понятий дисциплины.

5.5 Критерии оценивания теста

Критерии оценки:

При тестировании все верные ответы берутся за 100%.
90%-100% отлично
75%-90% хорошо
60%-75% удовлетворительно
менее 60% неудовлетворительно

5.6 Критерии оценивания реферата

Оценка **«отлично»** выставляется за глубокое знание предусмотренного программой материала, за умение четко, лаконично и логически последовательно отвечать на поставленные вопросы.
Оценка **«хорошо»** – за твердое знание основного (программного) материала, за грамотные, без существенных неточностей ответы на поставленные вопросы.
Оценка **«удовлетворительно»** – за общее знание только основного материала, за ответы, содержащие неточности или слабо аргументированные, с нарушением последовательности изложения материала.
Оценка **«неудовлетворительно»** – за незнание значительной части программного материала, за существенные ошибки в ответах на вопросы, за неумение ориентироваться в материале, за незнание основных понятий дисциплины.