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

«УТВЕРЖДАЮ»
Проректор по учебной работе _____ Г.Ю. Нагорная
«30» 03 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы алгоритмов криптографии

Уровень образовательной программы бакалавриат

Направление подготовки 09.03.04 Программная инженерия

Направленность (профиль) Программная инженерия

Форма обучения очная

Срок освоения ОП 4 года

Институт Прикладной математики и информационных технологий

Кафедра разработчик РПД Общая информатика

Выпускающая кафедра Прикладная информатика

Начальник
учебно-методического управления _____ Семенова Л.У.

Директор института ПМ и ИТ _____ Тебуев Д.Б.

Заведующий выпускающей кафедрой _____ Хапаева Л.Х.

г. Черкесск, 2022 г.

СОДЕРЖАНИЕ

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Основы алгоритмов криптографии» 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 практические методы разработки собственных электронных ключей

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2.1. Дисциплина «Основы алгоритмов криптографии» относится к к дисциплинам по выбору 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.	Опирается на знания, сформированные дисциплинами предыдущего уровня образования	Алгоритмизация и программирование

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Планируемые результаты освоения образовательной программы (ОП) – компетенции обучающихся определяются требованиями стандарта по направлению подготовки 01.03.04 Прикладная математика 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.	УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК–1.1. Определяет, интерпретирует и ранжирует информацию, требуемую для решения поставленной задачи УК–1.2. Осуществляет поиск информации для решения поставленной задачи по различным типам запросов УК-1.3. При обработке информации отличает факты от мнений, интерпретаций, оценок, формирует собственные мнения и суждения, аргументирует свои выводы и точку зрения
2.	ПК-1	Способен использовать методы и инструментальные средства исследования объектов профессиональной деятельности	ПК-1.2. Обрабатывает полученные результаты исследований с использованием стандартных методов (методик) ПК-1.3. Осуществляет поиск, хранение обработку и анализ информации из различных источников, представляет в требуемом формате с использованием информационных технологий ПК-1.7. Составляет формализованные описания решений, поставленных задач, применяя стандартные алгоритмы решения типовых задач.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Вид учебной работы		**Всего часов**	**Семестр**
			№ 1
			Часов
1		2	3
Аудиторная контактная работа (всего)		**90**	**90**
В том числе:			
Лекции (Л)		18	18
Лабораторные занятия (ЛЗ),		36	36
Практические занятия (ПЗ)		36	36
Контактная внеаудиторная работа, в том числе:		**2**	**2**
индивидуальные и групповые консультации		2	2
Самостоятельная работа обучающегося (СРС) (всего)**		**16**	**16**
Работа с книжными источниками		4	4
Работа с электронными источниками		4	4
Подготовка к коллоквиуму		4	4
Подготовка к тестированию		2	2
Реферат		2	2
Промежуточная аттестация	Экзамен (Э) **в том числе:**	**Э (36)**	**Э(36)**
	Прием экз., час.	0,5	0,5
	Консультация, час.	2	2
	СРО, час.	33,5	33,5
ИТОГО: Общая трудоемкость	**Часов**	**144**	**144**
	зач. ед.	**4**	**4**

4.2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

№ 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 1							
1.	Раздел 1. Введение в криптографию и шифрование	2	6	6	4	18	Коллоквиум, реферат, тестирование
2.	Раздел 2. Простейшие методы шифрования с открытым и закрытыми ключами.	4	10	10	4	28	Коллоквиум, практические индивидуальные задания. Реферат, тестирование
3.	Раздел 3. Принципы построения блочных шифров с закрытым ключом	6	10	10	4	30	Коллоквиум, практические индивидуальные задания. Реферат, тестирование
4.	Раздел 4. Платформа Ethereum.	6	10	10	4	30	Коллоквиум, практические индивидуальные задания. Реферат, тестирование
	Контактная внеаудиторная работа					2	Индивидуальные и групповые консультации
	Промежуточная аттестация					36	экзамен
Итого часов в 1 семестре:		**18**	**36**	**36**	**16**	**144**	

4.2.2. Лекционный курс

№ п/п	Наименование раздела дисциплины	Наименование темы лекции	Содержание лекции	Всего часов
1	2	3	4	5
Семестр 1				
1.	Раздел 1. Введение в криптографию и шифрование	Тема 1.1Основные понятия	Основы криптографической теории, ключи безопасности.	2
2.	Раздел 2. Простейшие методы шифрования с открытым и закрытыми ключами	Тема 2.1 Различные методы шифрования	Требования к криптографическим системам, защита информации. Примеры простейших шифров	4
3.	Раздел 3. Принципы построения блочных шифров с закрытым ключом	Тема 3.1 Принципы построения блочных шифров. Криптографические хеш – функции. Разработка собственного ПО шифра с хэш – функцией.	Хеш-функции. Proof of work. Проблема двойных трат. Блоки и цепочки блоков. Дерево Меркла. Сложность майнинга. Награда за создание блока. Комиссии за транзакции.	6
4.	Раздел 4. Платформа Ethereum.	Тема 4.1 Начальные сведения о платформе Ethereum.	Основные различия Эфириума и Биткоина. Отличие системы utxo от балансов. Базовая теория Эфириума. Виды узлов. Транзакции. Газ. Пользовательский аккаунт. Metamask. Основная сеть, тестовые сети. Faucet. Теория смарт-контрактов. Аккаунт смарт-контракта.	2
5.		Тема 4.2 Работа в платформе Ethereum.	Газ в смарт-контрактах. Создание контракта. Языки для написания смарт-контрактов (Solidity). Oracles. Bytecode, OPcode, ABI. Виртуальная машина Эфириума (EVM). Различные способы хранения данных. Stack-machine. Разработка и техническая собственного ПО на платформе проверка Ethereum.	4
ИТОГО часов в 1 семестре:				**18**

4.2.2 Практические занятия

№ п/п	Наименование раздела дисциплины	Наименование практического занятия	Содержание практического занятия	Всего часов
1	2	3	4	5
Семестр 1				
2	Раздел 1. Введение в криптографию и шифрование	Тема 1.1Основные понятия	Основы криптографической теории, ключи безопасности.	6
3	Раздел 2. Простейшие методы шифрования с открытым и закрытыми ключами	Тема 2.1 Различные методы шифрования	Требования к криптографическим системам, защита информации. Примеры простейших шифров	10
4	Раздел 3. Принципы построения блочных шифров с закрытым ключом	Тема 3.1 Принципы построения блочных шифров. Криптографические хеш – функции. Разработка собственного ПО шифра с хэш – функцией.	Хеш-функции. Proof of work. Проблема двойных трат. Блоки и цепочки блоков. Дерево Меркла. Сложность майнинга. Награда за создание блока. Комиссии за транзакции.	10
5	Раздел 4. Платформа Ethereum.	Тема 4.1 Начальные сведения о платформе Ethereum.	Основные различия Эфириума и Биткоина. Отличие системы utxo от балансов. Базовая теория Эфириума. Виды узлов. Транзакции. Газ. Пользовательский аккаунт. Metamask. Основная сеть, тестовые сети. Faucet. Теория смарт-контрактов. Аккаунт смарт-контракта.	**4**
		Тема 4.2 Работа в платформе Ethereum.	Газ в смарт-контрактах. Создание контракта. Языки для написания смарт-контрактов (Solidity). Oracles. Bytecode, OPcode, ABI. Виртуальная машина Эфириума (EVM). Различные способы хранения данных. Stack-machine. Разработка и техническая собственного ПО на платформе проверка Ethereum.	**6**
ИТОГО часов в 1 семестре:				**36**

4.2.3 Лабораторные занятия

№ п/п	Наименование раздела дисциплины	Наименование лабораторные занятия	Содержание лабораторного занятия	Всего часов
1	2	3	4	5
Семестр 1				
2	Раздел 1. Введение в криптографию и шифрование	Тема 1.1Основные понятия	Основы криптографической теории.	6
3	Раздел 2. Простейшие методы шифрования с открытым и закрытыми ключами	Тема 2.1 Различные методы шифрования	Требования к криптографическим системам.	10
4	Раздел 3. Принципы построения блочных шифров с закрытым ключом	Тема 3.1 Принципы построения блочных шифров. Криптографические хеш – функции. Разработка собственного ПО шифра с хэш – функцией.	Сложность майнинга. Награда за создание блока. Комиссии за транзакции.	10
5	Раздел 4. Платформа Ethereum.	Тема 4.1 Работа в платформе Ethereum.	Теория смарт-контрактов. Аккаунт смарт-контракта. Различные способы хранения данных. Stack-machine. Разработка и техническая собственного ПО на платформе проверка Ethereum.	10
ИТОГО часов в 1 семестре:				**36**

4.3. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ

№ п/п	Наименование раздела (темы) дисциплины	№ п/п	Виды СРО	Всего часов
1	2	3	4	4
Семестр 1				
1.	Раздел 1. Введение в криптографию и шифрование	1.1.	Работа с книжными источниками. Работа с электронными учебниками. Подготовка к коллоквиуму. Реферат.	4
2.	Раздел 2. Простейшие методы шифрования с открытым и закрытыми ключами	2.1.	Работа с книжными источниками. Работа с электронными учебниками. Подготовка к коллоквиуму. Реферат. Тестирование	4
3.	Раздел 3. Принципы построения блочных шифров с закрытым ключом	3.1	Работа с книжными источниками. Работа с электронными учебниками. Подготовка к коллоквиуму. Реферат. Тестирование	4

4.	Раздел 4. Платформа Ethereum.	4.1	Работа с книжными источниками. Работа с электронными учебниками. Подготовка к коллоквиуму. Реферат. Тестирование	4
ИТОГО часов в 1 семестре:				**16**

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. Студенты 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.

5.3 Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обучающегося предполагает различные формы индивидуальной учебной деятельности: конспектирование научной литературы, сбор и анализ практического материала в СМИ, проектирование, выполнение тематических и творческих заданий и пр. Выбор форм и видов самостоятельной работы определяется индивидуально-личностным подходом к обучению совместно преподавателем и обучающимся. Формы текущего контроля успеваемости и промежуточной аттестации обучающихся.

В процессе подготовки к практическим занятиям, обучающимся необходимо 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.

Тестирование

Тестирование представляет собой средство контроля усвоения учебного материала темы или раздела дисциплины. При самостоятельной подготовке к тестированию обучающемуся необходимо:

а) проработать информационный материал по дисциплине, проконсультироваться с преподавателем по вопросу выбора учебной литературы;

б) выяснить все условия тестирования заранее, узнать, сколько тестов будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.

в) приступая к работе с тестами, внимательно и до конца прочитать вопрос и предлагаемые варианты ответов, выбрать правильные (их может быть несколько).

г) в процессе решения желательно применять несколько подходов в решении задания, это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант.

д) если встретился чрезвычайно трудный вопрос, не тратить много времени на него, перейти к другим тестам, вернутся к трудному вопросу в конце.

е) обязательно оставить время для проверки ответов, чтобы избежать механических ошибок.

Работа с книжными и электронными источниками

- В процессе подготовки к практическим занятиям, студентам 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 студентам проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

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

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

№ п/п	Виды учебной работы	Образовательные технологии	Всего часов
1	2	3	4
1	Тема 1.1Основные понятия	Технологии развития критического мышления. Обзорная лекция.	2
2	Тема 2.1 Различные методы шифрования	Лекция – презентация с использованием Power Point.	2
3	Тема 3.1 Принципы построения блочных шифров. Криптографические хеш - функции	Использование компьютерных технологий при выполнении индивидуальных практических заданий по созданию собственного ПО.	2
4	Тема 4.1 начальные сведения о платформе Ethereum.	Лекция – презентация с использованием Power Point.	2
5	Тема 4.2 Работа в платформе Ethereum.	Использование компьютерных технологий при выполнении индивидуальных практических заданий	2
Итого часов в 1 семестре:			**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 c. — 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 c. — 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 c. — 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 c. — 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 c. — 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	Реквизиты лицензий/ договоров
Microsoft Azure Dev Tools for Teaching 1. Windows 7, 8, 8.1, 10 2. Visual Studio 2008, 2010, 2013, 2019 5. Visio 2007, 2010, 2013 6. Project 2008, 2010, 2013 7. Access 2007, 2010, 2013 и т. д.	Идентификатор подписчика: 1203743421 Срок действия: 30.06.2022 (продление подписки)
MS Office 2003, 2007, 2010, 2013	Сведения об Open Office: 63143487, 63321452, 64026734, 6416302, 64344172, 64394739, 64468661, 64489816, 64537893, 64563149, 64990070, 65615073 Лицензия бессрочная
Антивирус Dr.Web Desktop Security Suite	Лицензионный сертификат Серийный № 8DVG-V96F-H8S7-NRBC Срок действия: с 20.10.2022 до 22.10.2023
Цифровой образовательный ресурс IPRsmart	Лицензионный договор № 10423/23П от 30.06.2023 г. Срок действия: с 01.07.2022 г. до 01.07.2023г.
Лицензионное программное обеспечение	Реквизиты лицензий/ договоров

Бесплатное ПО: Lazarus, Firebird, IBE Expert, Pascal ABC, Python, VBA, Virtual box, Sumatra PDF, 7-Zip

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 студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде, и т.п.

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

Основы алгоритмов криптографии

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Основы алгоритмов криптографии

Компетенции, формируемые в процессе изучения дисциплины

Индекс	Формулировка компетенции
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
ПК-1	Способен использовать методы и инструментальные средства исследования объектов профессиональной 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	УК-1	ПК_1
Раздел 1. Введение в криптографию и шифрование	+	+
Раздел 2. Простейшие методы шифрования с открытым и закрытыми ключами.	+	+
Раздел 3. Принципы построения блочных шифров с закрытым ключом	+	+
Раздел 4. Платформа Ethereum.	+	+

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

УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

Индикаторы достижения компетенции	Критерии оценивания результатов обучения				Средства оценивания результатов обучения	
	неудовлетв	удовлетв	хорошо	отлично	Текущий контроль	Промежуточная аттестация
УК–1.1. Определяет, интерпретирует и ранжирует информацию, требуемую для решения поставленной задачи	Не знает основные концепции, принципы, теории и факты, связанными с информатикой	Демонстрирует частичные знания в области концепций, принципов, теорий и фактов, связанными с информатикой	Хорошие знания основных концепций, принципов, теорий и фактов, связанными с информатикой	Демонстрирует отличные знания в области концепций, принципов, теорий и фактов, связанными с информатикой	Коллоквиум, контрольная работа, итоговый тестовый контроль, практические индивидуальные задания	Экзамен
УК–1.2. Осуществляет поиск информации для решения, поставленной задачи по различным типам запросов	Не умеет и не готов использовать основные концепции, принципы, теории и факты, связанные с информатикой	Не уверено использует основные концепции, принципы, теории и факты, связанные с информатикой	Уверено использует основные концепции, принципы, теории и факты, связанные с информатикой	Готов и умеет использовать основные концепции, принципы, теории и факты, связанные с информатикой		Экзамен
УК-1.3. При обработке информации отличает факты от мнений, интерпретаций, оценок, формирует собственные мнения и суждения, аргументирует свои выводы и точку зрения	Не владеет основными концепциями, принципами, теориями и фактами, связанными с информатикой	Частично владеет основными концепциями, принципами, теориями и фактами, связанными с информатикой	Владеет основными концепциями, принципами, теориями и фактами, связанными с информатикой	Отличное владение основными концепциями, принципами, теориями и фактами, связанными с информатикой		Экзамен

ПК-1 владением и навыками использования различных технологий разработки программного обеспечения

Индикаторы достижения компетенции	Критерии оценивания результатов обучения				Средства оценивания результатов обучения	
	неудовлетв	удовлетв	хорошо	отлично	Текущий контроль	Промежуточная аттестация
ПК-1.3. Осуществляет поиск, хранение обработку и анализ информации из различных источников, представляет в требуемом формате с использованием информационных технологий	Не знает методы поиска, хранения, обработки и анализа информации, не умеет представлять информацию в требуемом формате с использованием информационных технологий	Демонстрирует частичные знания методов поиска, хранения, обработки и анализа информации, допускает ошибки в представлении информации в требуемом формате.	Демонстрирует знания основных методов поиска, хранения, обработки и анализа информации, умеет представлять информацию в требуемом формате.	Владеет методами поиска, хранения, обработки и анализа информации, представляет информацию в требуемом формате с использованием информационных технологий	Коллоквиум, тестирование, практические индивидуальные задания, реферат	Экзамен
ПК-1.4. Применяет прикладные аспекты и инструментальные средства, и методы в современных программных комплексах	Не умеет и не готов применять прикладные аспекты и инструментальные средства, и методы в современных программных комплексах	Неуверенно владеет навыками применения прикладных аспектов и инструментальных средств, и методов в современных программных комплексах	Умеет применять прикладные аспекты и инструментальные средства, и методы в современных программных комплексах	Готов и умеет применять прикладные аспекты и инструментальные средства, и методы в современных программных комплексах		Экзамен
ПК-1.7. Составляет формализованные описания решений, поставленных задач, применяя стандартные алгоритмы решения типовых задач.	Решение поставленной задачи описано неверной моделью; ошибки в описании и применении стандартных алгоритмов решения типовых задач.	В описании модели решения поставленной задачи допущены ошибки; неточности в описании и применении стандартных алгоритмов решения типовых задач.	Строит формализованные модели решения поставленной задачи, применяя стандартные алгоритмы решения типовых задач	Свободно владеет навыками построения формализованных моделей решения поставленной задачи, применяя стандартные алгоритмы решения типовых задач		Экзамен

4. Комплект контрольно-оценочных средств по дисциплине

Вопросы к экзамену

по дисциплине «Основы алгоритмов криптографии»

1. Централизованный реестр.
2. Цифровые подписи.
3. Временные отметки. Система utxo.
4. Децентрализованный реестр. P2P-сети
5. Как достичь консенсуса. Хеш-функции.
6. Proof of work. Проблема двойных трат.
7. Блоки и цепочки блоков.
8. Дерево Меркла.
9. Сложность майнинга. Награда за создание блока.
10. Основные различия Эфириума и Биткоина.
11. Отличие системы utxo от балансов.
12. Аналоговые цифровые технологии.
13. Пользовательский аккаунт. Metamask.
14. Языки для написания смарт-контрактов (Solidity)
15. Oracles. Bytecode, OPcode, ABI.
16. Виртуальная машина Эфириума (EVM)
17. Различные способы хранения данных.
18. Remix - онлайн среда разработки для Solidity.
19. Основы Solidity.
20. Version pragma, import, комментарии.
21. Переменные состояния. Основные типы. Конструкторы.
22. Функции, типы функций. Настройки Remix.
23. Подробности Solidity. Типы (struct, enum, mapping).
24. Модификаторы view и pure. Видимость функций. Модификатор payable, fallback функции.
25. Продвинутые смарт-контракты.
26. Модификаторы функций. Наследование, интерфейсы.
27. События. Библиотеки. Calls, delegated calls.

СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ

Кафедра «Общая информатика»

20__- 20__ учебный год

Экзаменационный билет № ____

по дисциплине Основы алгоритмов криптографии

для обучающихся 1 курса направления подготовки

09.03.04. Программная инженерия

1. Различные способы хранения данных.
2. Remix - онлайн среда разработки для Solidity.
3. Задача

Зав. кафедрой Эльканова Л.М.

Задачи к экзамену

Рассмотрим модель шифра для цифрового текста, в котором каждая цифра заменяется остатком от деления значения многочлена

f(x) = b(x3 + 7x7 + 3x + a) на число 10, где a, b — фиксированные натуральные числа. Выяснить, при каких значениях a и b возможно однозначное расшифрование.

А-00000 З-01000 Р-10000 Ш-11000

Б-00001 И-01001 С-10001 Щ-11001

В-00010 К-01010 Т-10010 Ъ-11010

Г-00011 Л-01011 У-10011 Ы-11011

Д-00100 М-01100 Ф-10100 Ь-11100

Е-00101 Н-01101 Х-10101 Э-11101

Ё-00110 О-01110 Ц-10110 Ю-11110

Ж-00111 П-01111 Ч-10111 Я-11111

Вопросы к коллоквиуму

по дисциплине «Основы алгоритмов криптографии»

Вопросы к разделу 1.

1. Централизованный реестр.
2. Цифровые подписи.
3. Временные отметки. Система utxo.
4. Децентрализованный реестр. P2P-сети
5. Как достичь консенсуса. Хеш-функции.
6. Proof of work. Проблема двойных трат.
7. Блоки и цепочки блоков.
8. Дерево Меркла.

Вопросы к разделу 2.

1. Сложность майнинга. Награда за создание блока.
2. Основные различия Эфириума и Биткоина.
3. Отличие системы utxo от балансов.
4. Аналоговые цифровые технологии.
5. Пользовательский аккаунт. Metamask.
6. Языки для написания смарт-контрактов (Solidity)
7. Oracles. Bytecode, OPcode, ABI.

Вопросы к разделу 3.

1. Oracles. Bytecode, OPcode, ABI.
2. Виртуальная машина Эфириума (EVM)
3. Различные способы хранения данных.
4. Remix - онлайн среда разработки для Solidity.
5. Основы Solidity.
6. Version pragma, import, комментарии.
7. Переменные состояния. Основные типы. Конструктор

Темы рефератов

по дисциплине «Основы алгоритмов криптографии»

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.

Индивидуальные задания при разработке собственных ПО

по дисциплине «Основы алгоритмов криптографии»

Разработать проект на языке объектно – ориентированного программирования:

Вариант 1. Для передачи сообщений по телеграфу каждая буква русского алфавита (Е и Ё отождествлены) представляется в виде пятизначной комбинации из нулей и единиц, соответствующих двоичной записи номера данной буквы в алфавите (нумерация букв начинается с нуля). Например, буква А представляется в виде 00000, буква Б - 00001, буква Ч - 10111, буква Я - 11111. Передача пятизначной комбинации производится по кабелю, содержащему пять проводов. Каждый двоичный разряд передается по отдельному проводу. При приеме сообщения перепутали провода, поэтому вместо переданного слова получен набор букв ЭАВЬЩО. Найдите переданное слово. «ПАРОЛЬ»

Вариант 2. При шифровании открытый текст разбивается на блоки одинаковой длины и в каждом блоке осуществляется перестановка букв по одной и той же схеме. Восстановите исходное сообщение по криптограмме.

ПЬОКМ РХТЮЕ ШИРОО МОПЙО ККНЩИ ТОИРП ФАРГА

(45213) (45213) ….

КОМПЬЮТЕР ХОРОШИЙ ПОМОЩНИК КРИПТОГРАФА

Вариант 3. Коммерсант для передачи цифровой информации с целью контроля передачи разбивает строчку передаваемых цифр на пятерки и после каждых двух пятерок приписывает две последние цифры от суммы чисел, изображенных этими пятерками. Затем процесс шифрования осуществляется путем прибавления к шифруемым цифрам членов арифметической прогрессии с последующей заменой сумм цифр остатками от деления на 10. Прочитайте зашифрованное сообщение:

4 2 3 4 6 1 4 0 5 3 1 3.

Вариант 4. Буквы русского алфавита занумерованы в соответствии с таблицей: Для зашифровки сообщения, состоящего из n букв, выбирается ключ K - некоторая последовательность из n букв приведенного выше алфавита. Шифрование каждой буквы сообщения состоит в сложении ее номера в таблице с номером соответствующей буквы ключевой последовательности и замене полученной суммы на букву алфавита, номер которой имеет тот же остаток от деления на 30, что и эта сумма. Прочтите шифрованное сообщение: РБЬНПТСИТСРРЕЗОХ, если известно, что шифрующая последовательность не содержала никаких букв, кроме А, Б и В.

Вариант 5. Тридцати двум буквам русского алфавита А, Б, В, ..Э, Ю, Я приписаны соответственно числа 1, 2, 3, ..30, 31, 0 (буквы Е и Ё отождествляются). Выбрано некоторое нечетное число k (секретный ключ). Шифрование текста осуществляется побуквенно следующим образом:

1) число a, соответствующее данной букве, умножается на k,

2) вычисляется остаток r от деления a*k на 32

3) выписывается буква, соответствующая числу r.

Расшифруйте криптограммы:

1. ЕЦВ РФЗФЧНЙОЯ ЗМСФЦМ АМХХЛЭ
2. ЦОДШФДЮ ПКЫМЙМЯ
3. ЁРЪЫШРЫЪЩДБ ПЪДЛЪКООВЪДАКЩВБ

Разработать программный модуль по следующим заданиям:

Задание 1.

1. Расшифровать предлагаемый текст и определить ключ зашифрования. Известно, что использован шифр простой замены в русском 30-буквенном алфавите. (Разбиение на группы букв не несет никакой смысловой нагрузки).

```
ЕКЫЬЦ ЕЦЕКШ ИКТЦЕ ИХМКИ ШЩКМ
ЭНШИЬ РШООК ШХКСР ЭЬКЩЦ ИЭРЗ
ОКСИШ ДЛКЯЦ ЕРУНЭ ОШШКО ОЭШЯ
ЧЭЮОК ЧДЬЭИ ЯЦЕРУ НЦИЗЩ СЭЧЭ
ОЭЕКЭ ШОКЭИ КРЕКЩ ЦОШЭ
```

2. Составить программу для криптоанализа шифра Цезаря просмотром всех вариантов. Ввести возможные усовершенствования в алгоритм. Прочитать криптотекст (исходный текст на английском языке).

```
PXPXK XENVD RUXVT NLXHY MXGMA XYKXJN
XGVRF XMAHW GXXWL EHGZX KVBIA XKMXQM
```

3. Произвести выборку текстов (худ. литература, тех. литература и т.д.; на русском или англ. языке) объемом 5-100 Мбайт и
а) составить таблицу частот встречаемости букв;
б) составить таблицу (матрицу) частот встречаемости биграмм (в процентах);
в) определить запретные биграммы.

Задание 2.

1. Известно, что в криптотексте (1) использован шифр горизонтальной перестановки. Вскрыть шифр и на том же ключе зашифровать в качестве ответа текст (2).

```
ЕХХ ЗНТ МАН ЕЛЧ ООЕ НЕВ АКА ИЧЕ НДП ТГО
ТНО ЬЯТ АФЫ КТО ПЕД ЮРО ВИТ ЕМО СОО ТЧГ
ЫОТ СБН ООО ТЬИ СТТ ИОЕ ЮРК ФСТ АХМ АХИ
(2)
Способ мышления очень близок и ярок,
но выводы кажутся слишком далеко идущими
и преувеличенными
```

2. Для решетки Кардано 4х4 количество возможных ключей невелико. Подсчитать их. Составить программу, которая перебирает все возможные варианты, и определить решетку Кардано для криптотекста

```
ААКК РОЯЮ ЗГЫГ ДВЛА
```

НОАГ ДЗВА СЧАА ТСАЕ
НЖЛН ОАУЬ ФТЧВ ИЕЕО
ООМВ ННИС РИОО ГГНО
КВЕД ЛГЕО ТГИО ЦЗОА
НТКН ОЦУЕ ЯБГВ ЕОАС

Тестовые вопросы
по дисциплине «Основы алгоритмов криптографии»

№1 Выберите то, что лучше всего описывает цифровую подпись:
1) Это метод переноса собственноручной подписи на электронный документ
2) Это метод шифрования конфиденциальной информации
3) Это метод, обеспечивающий электронную подпись и шифрование
4) Это метод, позволяющий получателю сообщения проверить его источник и убедиться в целостности сообщения

№2 Эффективная длина ключа в DES:
1) 56
2) 64
3) 32
4) 16

№3 Причина, по которой удостоверяющий центр отзывает сертификат:
1) Если открытый ключ пользователя скомпрометирован
2) Если пользователь переходит на использование модели PEM, которая использует сеть доверия
3) Если закрытый ключ пользователя скомпрометирован+
4) Если пользователь переходит работать в другой офис

№4 Расшифруйте аббревиатуру DEA:

_____

№5 Процесс, выполняемый после создания сеансового ключа DES
1) Подписание ключа
2) Передача ключа на хранение третьей стороне (key escrow)
3) Кластеризация ключа
4) Обмен ключом

№6 Количество циклов перестановки и замещения, выполняемый DES

_____

№7 Выберите правильное утверждение в отношении шифрования данных, выполняемого с целью их защиты:
1) Оно обеспечивает проверку целостности и правильности данных
2) Оно требует внимательного отношения к процессу управления ключами
3) Оно не требует большого количества системных ресурсов
4) Оно требует передачи ключа на хранение третьей стороне (escrowed)

№8 Название ситуации, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст:

_____

№9 Определение фактора трудозатрат для алгоритма:
1) Время зашифрования и расшифрования открытого текста
2) Время, которое займет взлом шифрования
3)Время, которое занимает выполнение 16 циклов преобразований
4) Время, которое занимает выполнение функций подстановки

№10 Основная цель использования одностороннего хэширования пароля пользователя:
1) Это снижает требуемый объем дискового пространства для хранения пароля пользователя
2) Это предотвращает ознакомление кого-либо с открытым текстом пароля+
3) Это позволяет избежать избыточной обработки, требуемой асимметричным алгоритмом
4) Это предотвращает атаки повтора (replay attack)

№11 Алгоритм, основанный на сложности разложения больших чисел на два исходных простых сомножителя:

_____

№12 Что является описанием разницы алгоритмов DES и RSA:
1) DES – это симметричный алгоритм, а RSA – асимметричный
2) DES – это асимметричный алгоритм, а RSA – симметричный
3) Они оба являются алгоритмами хэширования, но RSA генерирует 160-битные значения хэша
4) DES генерирует открытый и закрытый ключи, а RSA выполняет шифрование сообщений

№13 Алгоритм, использующий симметричный ключ и алгоритм хэширования:
1) HMAC
2) 3DES
3) ISAKMP-OAKLEY
4) RSA

№14 Количество способов гаммирования:
_____

№15 Метод, который применяют при шифровании с помощью аналитических преобразований:
_____

№16 То, что применяют в качестве ключа при шифровании с помощью аналитических преобразований:

_____

№17 Идентификатор пользователя в блокчейн-сети

1) Публичный ключ алгоритма асимметричного шифрования
2) Ключ симметричного шифрования;
3) Шифр Цезаря;
4) Хэш - функция

№18 Назовите основные характеристики блокчейна.

1) технология криптозащиты
2) учетный журнал
3) строго хронологический порядок записей
4) система сбора и хранения данных

№19 Биткоин это

1) криптоключ
2) цифровой актив
3) тип кредитной карты
4) криптовалюта

№20 Случаи использования биткоина

1) для хранения ценностей
2) для совершения электронных оплат
3) для пополнения бумажных счетов
4) для покупки услуг

№21 Блокчейн это

1) глобальная сеть с тысячами компьютеров
2) особо децентрализованный учетный журнал
3) ключевая технология, содержащая децентрализованную запись транзакций
4) централизованная база данных, подтверждающая проведение сделки

№22 Основные задачи майнеров

1) обработка и подтверждение транзакций
2) решение криптографических задач
3) децентрализованное размещение данных по каждой сделке
4) создание цепи записей, которые формируют учетный журнал биткойн

№23 Хэш это

1) криптографически зашифрованная сделка
2) цифровой отпечаток определенного набора данных
3) децентрализованное разрешение криптографических задач
4) объем данных в алфавитно-цифровом формате определенной длины

№24 Периодичность, с которой добавляются новые блоки со всеми новыми транзакциями в блокчейн

1) по мере обработки майнерами
2) каждые десять минут
3) раз в сутки
4) после 100% заполнения нового блока

№25 Вид хеш-функции, которая используется в Биткойн.

№26 Главное отличие между хешированием и шифрованием.

1) уникальный цифровой отпечаток шифра не может быть возвращен к исходному тексту
2) хеш позволяет вернуться к исходному тексту без ключа
3) хеш является односторонней функцией
4) шифр имеет ограничения по обработке объема данных

№27 Перечислите состав блока

1) данные
2) математический шифр
3) криптографический хеш
4) одноразовый номер

№28 Элемент, который является общим для каждого блока.

1) номер
2) объем данных
3) сопутствующий хэш
4) PREV

№29 Когда система высчитывает действующий хэш?

1) при хронологическом выстраивании блоков
2) при создании криптографического хэша
3) во время добычи блока
4) при возврате к исходному количеству символов

№30 Назовите основные составляющие биткоин.

1) программное обеспечение
2) криптографическое испытание
3) майнеры
4) централизованное хранилище

№31 Пусть хеш-функция $y=h(x_1x_2\ldots x_n)$ определяется как результат выполнения побитовой операции «сумма по модулю 2» для всех байтов сообщения, представленного в двоичном виде Длина хеш-кода равна 8 битам Для каждого из шести сообщений, записанных в левом столбце, найдите соответствующий результат вычисления хеш-функции из правого столбца Все сообщения и значения хеш-функции представлены в шестнадцатеричном формате

Сообщения	Значения хеш-функции
а) A3 69 2C;	а) 38;
б) 82 0F B5;	б) 1B;
в) DA 14 90;	в) F9;
г) 32 01 BF;	г) 8C;
д) 9E A6 23;	д) E6;
е) 10 BE 57;	е) 5E

1) а-д, б-а, в-е, г-г, д-б, е-в +
2) а-б, б-е, в-а, г-г, д-д, е-в
3) а-е, б-д, в-г, г-в, д-б, е-а
4) а-д, б-а, в-г, г-е, д-б, е-в

5 Методические материалы, определяющие процедуры оценивания компетенции

5.1 Критерии оценивания коллоквиума

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.

5.2 Критерии оценивания практического задания

Оценка «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 студент не освоил программный материал своевременно не выполнил и не продемонстрировал разработанное программное приложение.

5.3 Критерии оценивания результатов освоения дисциплины на экзамене:

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.

5.4 Критерии оценивания тестирования

Критерии оценки:
При тестировании все верные ответы берутся за 100%.
90%-100% отлично
75%-90% хорошо
60%-75% удовлетворительно

менее 60% неудовлетворительно

5.5 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.