КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)
АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОБРАЗОВАТЕЛЬНОЙ
ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 2 з.е.
в академических часах: 72 ак.ч.

Форма промежуточной аттестации: зачет

2025

Оценочные материалы по дисциплине **Криптографические протоколы**

обсуждены и рекомендованы к утверждению решением кафедры естественных дисциплин, сервиса и туризма от 25 марта 2025 г., протокол № 6

одобрены Научно-методическим советом Казанского кооперативного института (филиала) от 2 апреля 2025 г., протокол № 3

СОДЕРЖАНИЕ

Целью оценочных материалов по дисциплине (модулю) (далее –ОМ) является комплексная оценка результатов обучения по дисциплине Криптографические протоколы и установление уровня сформированности компетенций обучающегося.

ОМ предназначен для проведения текущего контроля успеваемости и промежуточной аттестации.

ОМ включает оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации.

Оценочные материалы разработаны в соответствии с рабочей программой дисциплины Криптографические протоколы.

1. Паспорт оценочных матриалов по дисциплине «Криптографические протоколы»

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения	Контролируемые разделы, темы дисциплины	Наименование оценочного средства	
				Текущий контроль	Промежуточная аттестация
1	2	3	4	5	6
ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1. Применяет в профессиональной деятельности знания об основных алгоритмах, используемых в криптографии, а также методы оценивания сложности таких алгоритмов	Знать: основные алгоритмы, используемые в криптографии, их принципы работы и области применения, а также методы оценки их сложности и стойкости. Уметь: применять эти знания для анализа и выбора оптимальных алгоритмов в зависимости от конкретных задач и условий профессиональной деятельности. Владеть: навыками практического использования криптографических алгоритмов и методами их адаптации к различным информационным системам.	Тема 1. Поля объектов и проблема защиты информации Тема 2. Криптоалгоритмы	Опрос (Тема 1-2) Доклад /Презентация (Тема 1-2) Тест (Тема 1-2)	Тест (П 1-4 тестового задания)
	ОПК-10.2. Демонстрирует при решении задач профессиональной деятельности умение использовать основные преобразования	Знать: основные принципы и алгоритмы симметричного и асимметричного шифрования, методы их применения, принципы построения криптосистем, а также типичные уязвимости и известные атаки на криптографические алгоритмы. Уметь: анализировать текущее состояние ИБ на предприятии с целью разработки требований к средствам	Тема 3. Криптопротоколы	Опрос (Тема 1-3) Доклад /Презентация (Тема 1-3) Тест (Тема 1-3)	Тест (П 5-9 тестового задания)

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения	Контролируемые разделы, темы дисциплины	Наименование оценочного средства	
				Текущий контроль	Промежуточная аттестация
1	2	3	4	5	6
	симметричной и асимметричной криптографии и анализировать их криптостойкость к возможным компьютерным атака	криптографической защиты информации (СКЗИ) Владеть: практическим опытом использования распространенных криптографических алгоритмов и методов, такими как DES, AES, RSA, ECC; способностями оценивать эффективность выбранных криптографических методов и адаптировать их к требованиям информационной безопасности конкретной профессиональной деятельности.			

2. Оценочные материалы по дисциплине Криптографические протоколы

2.1 Оценочные материалы для проведения текущего контроля успеваемости

Тема 1. Поля объектов и проблема защиты информации.

Системы вычетов. НОД, функция Эйлера, основная теорема арифметики. Мультипликативная инверсия, расширенный алгоритм Евклида. М алая теорема Ферма, формула Эйлера, примитивный элемент поля. Решение сравнений первой степени. Китайская теорема об остатках. Алгоритмы проверки на простоту. Тест Миллера- Рабина. Задача факторизации числа. Эллиптические кривые.

Цель опроса – закрепить полученные знания и развить профессиональные навыки и умения, актуальные для будущих специальстов.

Критерии оценки:

«отлично» - ставится обучающемуся, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;

«хорошо» - ставится обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

«удовлетворительно» - ставится обучающемуся, показавшему фрагментарный, разрозненный характер знаний и может применять полученные знания по образцу в стандартной ситуации;

«неудовлетворительно» - ставится студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении практических задач

Тематика докладов/презентаций:

1. Расширенный алгоритм Евклида: теория и применение в криптографии (на примере RSA).
2. Функция Эйлера: свойства, вычисление и роль в асимметричных криптосистемах.
3. Малая теорема Ферма и теорема Эйлера как основа корректности RSA.
4. Китайская теорема об остатках: математический аппарат и использование для ускорения RSA.
5. Тест Миллера–Рабина: принцип работы, вероятностная природа и практическое применение.
6. Проблема факторизации больших чисел и её влияние на стойкость RSA.
7. Примитивные элементы конечных полей и их значение в построении криптосистем.

8. Эллиптические кривые в криптографии: основные понятия и преимущества перед RSA.
9. Сравнение методов генерации простых чисел: детерминированные и вероятностные подходы.
10. Математические основы построения безопасных криптосистем: от теории чисел к практике.

Критерии оценки докладов:

– оценка *«отлично»* выставляется студенту, если выполнены все требования к написанию и защите доклада: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

– оценка *«хорошо»,* если основные требования к докладу и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём доклада; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

– оценка *«удовлетворительно»,* если имеются существенные отступления от требований. В частности, тема освещена лишь частично; допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.

– оценка *«неудовлетворительно»* тема доклада не раскрыта, обнаруживается существенное непонимание проблемы.

Тесты по теме:

Какой алгоритм используется в криптографии для нахождения такого числа, при умножении на которое по модулю получается единица?

a) Алгоритм быстрого возведения в степень

b) Расширенный алгоритм Евклида

c) Алгоритм Эратосфена

d) Тест Миллера–Рабина

Что позволяет определить функция Эйлера при работе с криптосистемами на основе модульной арифметики?

a) Количество простых чисел до заданного

b) Количество целых чисел, взаимно простых с заданным модулем

c) Минимальное количество бит для представления числа

d) Степень защищённости шифра

Какая теорема лежит в основе корректной работы шифрования и расшифрования в алгоритме RSA?

a) Малая теорема Ферма

b) Теорема Пифагора

c) Основная теорема арифметики

d) Теорема Эйлера

Какой метод позволяет эффективно выполнять вычисления с большими числами, разбивая задачу на несколько подзадач с меньшими модулями?

a) Расширенный алгоритм Евклида

b) Китайская теорема об остатках

c) Метод последовательного перебора

d) Алгоритм двоичного возведения в степень

Какой из перечисленных тестов используется для проверки числа на простоту с высокой вероятностью, но не даёт стопроцентной гарантии?

a) Алгоритм решета Эратосфена

b) Тест Миллера–Рабина

c) Метод полного перебора делителей

d) Алгоритм Евклида

Что является основной вычислительной задачей, обеспечивающей стойкость классического алгоритма RSA?

a) Поиск примитивного корня

b) Решение дискретного логарифма

c) Разложение большого числа на простые множители

d) Генерация случайных чисел

Как называется элемент конечного поля, степени которого позволяют получить все ненулевые элементы этого поля?

a) Нейтральный элемент

b) Инверсный элемент

c) Примитивный элемент

d) Обратный элемент

Какая современная криптографическая технология обеспечивает высокий уровень защиты при значительно меньшей длине ключа по сравнению с RSA?

a) Симметричное шифрование

b) Криптография на эллиптических кривых

c) Хэширование по ГОСТ

d) Коды исправления ошибок

Согласно какой теореме любое составное число можно единственным образом представить в виде произведения простых множителей?

a) Малая теорема Ферма

b) Основная теорема арифметики

c) Теорема Эйлера

d) Теорема о делении с остатком

Какая из перечисленных задач лежит в основе криптосистем, построенных на эллиптических кривых?

a) Факторизация больших чисел

b) Решение квадратных уравнений

c) Дискретное логарифмирование на эллиптической кривой

d) Поиск наибольшего общего делителя

Критерии оценки тестов:
85% – 100% правильных ответов – «отлично»;
75% – 84% правильных ответов – «хорошо»;
50% – 75% правильных ответов – «удовлетворительно»;
менее 50 % правильных ответов – «неудовлетворительно».

Тема 2. Криптоалгоритмы.

Типы атак на криптосистемы. Понятие стойкости шифра по Шеннону. Совершенные шифры. Алгоритм Блюм-Блюм-Шуба. Регистр сдвига. М-последовательность, нелинейный усложнитель. Вихрь Мерсена. Тесты NIST. Тесты DIE HARD. Общие подходы к построению блочных симметричных шифров. Обратимые и необратимые операции, классификация блочных шифров. Шифры Фейстеля. Шифр DES. Шифр AES. SubBytes, AddRoundKey. Криптография в эллиптических кривых

Цель опроса – закрепить полученные знания и развить профессиональные навыки и умения, актуальные для будущих специальстов.

Критерии оценки:

«отлично» - ставится обучающемуся, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;

«хорошо» - ставится обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

«удовлетворительно» - ставится обучающемуся, показавшему фрагментарный, разрозненный характер знаний и может применять полученные знания по образцу в стандартной ситуации;

«неудовлетворительно» - ставится студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении практических задач

Тематика докладов/презентаций:

1. Типы атак на криптосистемы: от пассивного перехвата до атаки с выбранным шифротекстом.
2. Совершенная секретность по Шеннону: теория и практическая реализуемость (шифр Вернама).
3. Генераторы псевдослучайных чисел: сравнительный анализ Блюм–Блюм–Шуба, регистра сдвига и вихря Мерсена.
4. Статистические тесты NIST и DIEHARD: цели, методы и значение для криптографии.
5. Архитектура шифров Фейстеля: принцип работы и применение в DES,

ГОСТ, Blowfish.

6. Алгоритм DES: история, структура, причины устаревания и замена на AES.
7. AES (Rijndael): этапы раунда, обратимость операций, безопасность и производительность.
8. Операции SubBytes и AddRoundKey в AES: роль в обеспечении диффузии и конфузии.
9. Преимущества криптографии на эллиптических кривых по сравнению с классическими системами (RSA, DSA).
10. Почему DES больше не используется, а AES стал стандартом? Анализ криптостойкости и аппаратной реализации.

Критерии оценки докладов:

– оценка *«отлично»* выставляется студенту, если выполнены все требования к написанию и защите доклада: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

– оценка *«хорошо»,* если основные требования к докладу и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём доклада; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

– оценка *«удовлетворительно»,* если имеются существенные отступления от требований. В частности, тема освещена лишь частично; допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.

– оценка *«неудовлетворительно»* тема доклада не раскрыта, обнаруживается существенное непонимание проблемы.

Тесты по теме:

Какой тип атаки предполагает, что криптоаналитик имеет доступ только к зашифрованным сообщениям?

a) Атака на основе известного открытого текста
b) Атака на основе выбранного шифротекста
c) Атака на основе только шифротекста
d) Атака методом грубой силы

Какой шифр считается «совершенным» по определению Шеннона?

a) DES
b) AES
c) Шифр Вернама

d) RSA

Какой генератор псевдослучайных чисел основан на трудности факторизации больших чисел?

a) Вихрь Мерсена

b) Регистр сдвига

c) Блюм–Блюм–Шуб

d) RANDU

Какой стандарт включает набор статистических тестов для оценки качества случайных последовательностей?

a) ISO/IEC 27001

b) NIST SP 800-22

c) GOST R 34.12-2015

d) RFC 2827

Какая из перечисленных операций входит в один раунд алгоритма AES?

a) SubBytes

b) XOR с ключом сессии

c) Расширение ключа

d) Все перечисленные

Что является основной причиной отказа от использования DES в современных системах?

a) Сложность реализации

b) Малая длина ключа (56 бит)

c) Отсутствие поддержки в ОС

d) Несовместимость с AES

Какая структура лежит в основе шифра DES?

a) SP-сеть

b) Архитектура Фейстеля

c) Регистр сдвига

d) Эллиптическая кривая

Какой из перечисленных компонентов НЕ входит в раундовую функцию AES?

a) SubBytes

b) ShiftRows

c) MixColumns

d) FeistelRound

Какая криптосистема обеспечивает сравнимую стойкость с RSA при значительно меньшей длине ключа?

a) DES

b) SHA-256

c) ECC (криптография на эллиптических кривых)

d) Blowfish

Какой из алгоритмов НЕ является блочным симметричным шифром?

a) AES

b) DES

c) RSA
d) ГОСТ 28147-89

Критерии оценки тестов:
85% – 100% правильных ответов – «отлично»;
75% – 84% правильных ответов – «хорошо»;
50% – 75% правильных ответов – «удовлетворительно»;
менее 50 % правильных ответов – «неудовлетворительно».

Тема 3. Криптопротоколы

Понятие хэш-функции. Понятие коллизий. Понятие криптографически стойкой хэш функции, классификация. MD5. Sha-2 . Стрибог. Построение хэш функций на симметричных алгоритмах. Протоколы построения. Whirpool. ЭЦП. ГОСТ 34.10-2018.

Цель опроса – закрепить полученные знания и развить профессиональные навыки и умения, актуальные для будущих специалистов.

Критерии оценки:

«отлично» - ставится обучающемуся, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;

«хорошо» - ставится обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

«удовлетворительно» - ставится обучающемуся, показавшему фрагментарный, разрозненный характер знаний и может применять полученные знания по образцу в стандартной ситуации;

«неудовлетворительно» - ставится студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении практических задач

Тематика докладов/презентаций:

1. Криптографические хэш-функции: требования, свойства и классификация.
2. Почему MD5 больше не используется: анализ уязвимостей и реальных атак.
3. Семейство SHA-2: структура, безопасность и применение в современных системах.
4. ГОСТ Р 34.11-2012 (Стрибог): особенности алгоритма и сравнение с SHA-2.
5. Построение хэш-функций на основе симметричных шифров: конструкция Дэвиса–Мейера и другие подходы.
6. Алгоритм Whirlpool: принцип работы и использование в стандартах

ISO/IEC.

7. Электронная цифровая подпись: цели, свойства и основные схемы (RSA, DSA, ECDSA).
8. ГОСТ Р 34.10-2018: математические основы, параметры эллиптических кривых и процедуры работы.
9. Сравнение ГОСТ Р 34.10-2018 и ECDSA: безопасность, эффективность и совместимость.
10. Роль хэш-функций в обеспечении целостности и аутентичности данных в защищённых протоколах (TLS, IPsec, S/MIME).

Критерии оценки докладов:

– оценка *«отлично»* выставляется студенту, если выполнены все требования к написанию и защите доклада: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

– оценка *«хорошо»,* если основные требования к докладу и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём доклада; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

– оценка *«удовлетворительно»,* если имеются существенные отступления от требований. В частности, тема освещена лишь частично; допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.

– оценка *«неудовлетворительно»* тема доклада не раскрыта, обнаруживается существенное непонимание проблемы.

Тесты по теме:

Какое из перечисленных требований НЕ предъявляется к криптографически стойкой хэш-функции?

a) Устойчивость к поиску прообраза

b) Устойчивость к поиску коллизий

c) Возможность обратного восстановления входных данных

d) Устойчивость к подбору второго прообраза

Какой из перечисленных алгоритмов считается небезопасным и не рекомендуется к использованию в новых системах?

a) SHA-256

b) Стрибог

c) MD5

d) Whirlpool

Какой российский стандарт определяет требования к криптографическим хэш-функциям?

a) ГОСТ Р 34.10-2018

b) ГОСТ Р 34.11-2012

c) ГОСТ 28147-89

d) ГОСТ Р 34.13-2015

На какой математической основе строится алгоритм ЭЦП по стандарту ГОСТ Р 34.10-2018?

a) Факторизация больших чисел

b) Дискретное логарифмирование в конечных полях

c) Дискретное логарифмирование на эллиптических кривых

d) Решение систем линейных уравнений

Какой из перечисленных алгоритмов входит в семейство SHA-2?

a) SHA-1

b) MD5

c) SHA-256

d) RIPEMD-160

Что такое «коллизия» в контексте хэш-функций?

a) Совпадение хэш-значений для двух различных входных сообщений

b) Ошибка при вычислении хэша

c) Повторное использование одного и того же ключа

d) Несовпадение контрольной суммы

Какой стандарт определяет процедуру формирования и проверки электронной цифровой подписи в Российской Федерации?

a) ГОСТ Р 34.11-2012

b) ГОСТ Р 34.10-2018

c) ГОСТ Р 34.13-2015

d) ГОСТ 28147-89

Какой из перечисленных алгоритмов основан на итеративной структуре с использованием симметричного шифра?

a) SHA-256

b) Whirlpool

c) MD5

d) Стрибог

Для чего в протоколах ЭЦП используется хэш-функция?

a) Для ускорения шифрования

b) Для сжатия сообщения перед подписью

c) Для обеспечения фиксированной длины подписываемых данных и защиты от подделки

d) Для генерации случайного ключа

Какой из перечисленных алгоритмов является международным стандартом хэш-функции, разработанным совместно с Vincent Rijmen?

a) SHA-1

b) MD5

c) Whirlpool

d) Стрибог

Критерии оценки тестов:
85% – 100% правильных ответов – «отлично»;
75% – 84% правильных ответов – «хорошо»;
50% – 75% правильных ответов – «удовлетворительно»;
менее 50 % правильных ответов – «неудовлетворительно».

2.2 Оценочные материалы для проведения промежуточной аттестации

Вопросы к зачету:

ОПК-10.1. Применяет в профессиональной деятельности знания об основных алгоритмах, используемых в криптографии, а также методы оценивания сложности таких алгоритмов

1. Понятие криптографической защиты информации. Основные цели и задачи.
2. Встроенные средства обеспечения безопасности в операционных системах Windows и Linux. Архитектура подсистемы безопасности Windows (LSASS, SAM, SRM).
3. Модели управления доступом: DAC, MAC, RBAC. Сравнительная характеристика.
4. Встроенные механизмы защиты сетевых протоколов: TLS/SSL, SSH, IPsec. Принципы их работы.
5. Основные компоненты инфраструктуры открытых ключей (PKI). Роль сертификатов и центров сертификации.
6. Жизненный цикл криптографического ключа. Принципы управления ключами.
7. Причины ненадёжности криптосистем: человеческий фактор, ошибки реализации, использование нестойких алгоритмов.
8. Отличие криптографии как математической науки и как инженерной дисциплины.
9. Понятие совершенного шифра. Шифр Вернама и его свойства.
10. Типы атак на криптосистемы: от атаки на основе только шифротекста до атаки с выбранным ключом.
11. Принципы построения блочных симметричных шифров. Архитектура Фейстеля.
12. Особенности алгоритмов DES и AES. Причины замены DES на AES.
13. Основные операции в раунде AES: SubBytes, ShiftRows, MixColumns, AddRoundKey.
14. Генераторы псевдослучайных чисел в криптографии: Блюм–Блюм–Шуб, вихрь Мерсена, регистры сдвига.

15. Тесты NIST и DIEHARD: назначение и применение для оценки качества случайных последовательностей.
16. Понятие хэш-функции. Требования к криптографически стойкой хэш-функции.
17. Коллизии в хэш-функциях: определение, виды, последствия.
18. Сравнительная характеристика хэш-алгоритмов: MD5, SHA-2, Стрибог, Whirlpool.
19. Построение хэш-функций на основе симметричных шифров (конструкция Дэвиса–Мейера).
20. Принципы работы электронной цифровой подписи (ЭЦП). Стандарт ГОСТ Р 34.10-2018: основные этапы и особенности.
21. Математические основы криптографии на эллиптических кривых. Преимущества перед RSA.
22. Роль хэш-функций в обеспечении целостности и аутентичности данных.
23. Проблема факторизации больших чисел и её связь со стойкостью RSA.
24. Китайская теорема об остатках и её применение в криптографии (например, в RSA-CRT).
25. Тест Миллера–Рабина: принцип работы и вероятностная природа.

ОПК-10.2. Демонстрирует при решении задач профессиональной деятельности умение использовать основные преобразования симметричной и асимметричной криптографии и анализировать их криптостойкость к возможным компьютерным атака

1. Основные принципы построения систем криптографической защиты информации.
2. Роль встроенных средств безопасности операционных систем в обеспечении защиты данных.
3. Сравнительный анализ встроенных механизмов безопасности в Windows и Linux.
4. Проблемы управления криптографическими ключами в распределённых и облачных средах.

5. Особенности жизненного цикла ключевой информации: генерация, распределение, хранение, отзыв и уничтожение.
6. Типичные ошибки при реализации и использовании криптографических алгоритмов.
7. Различие между «доказуемой» и «практической» безопасностью криптосистем.
8. Принципы работы и структура блочного шифра AES.
9. Особенности построения и применения хэш-функций в криптографических протоколах.
10. Этапы формирования и проверки электронной цифровой подписи по стандарту ГОСТ Р 34.10-2018.

Тестовые задания для проведения промежуточной аттестации.

Какие протоколы относятся к транспортному уровню четырехуровневой модели стека протоколов TCP/IP?
a. ARP
b. TCP
c. UDP
d. IP
e. ICMP

Виртуальные частные сети:
a. Передают частные данные по выделенным сетям
b. Инкапсулируют частные сообщения и передают их по общественной сети
c. Не используются клиентами Windows
d. Могут использоваться с протоколами L2TP или PPTP

Основные отличия протоколов L2TP и PPTP состоят в следующем (выберите все возможные варианты):
a. Протокол L2TP обеспечивает не конфиденциальность, а только туннелирование
b. Протокол PPTP используется только для туннелирования TCP/IP
c. Протокол L2TP может использоваться со службами IPSec, а протокол PPTP используется самостоятельно
d. Протокол PPTP поддерживается крупнейшими производителями, а протокол L2TP является стандартом корпорации Microsoft

Служба, осуществляющая присвоение реальных IP-адресов узлам закрытой приватной сети, называется:
a. NAT

b. PAT
c. Proxy
d. DHCP
e. DNS

На каком из четырех уровней модели стека протоколов TCP/IP к передаваемой информации добавляется заголовок, содержащий поле TTL (time-to-live)?
a. На уровне приложений (application layer)
b. На транспортном уровне (transport layer)
c. На сетевом уровне (internet layer)
d. На канальном уровне (link layer)

На каком уровне четырехуровневой модели стека протоколов TCP/IP работает служба DNS?
a. На уровне приложений (application layer)
b. На транспортном уровне (transport layer)
c. На межсетевом уровне (internet layer)
d. На канальном уровне (link layer)

Какой транспортный протокол используется протоколом Simple Mail Transfer Protocol (SMTP)?
a. TCP
b. UDP
c. ICMP
d. Ни один из перечисленных

Назовите отличия концентраторов (hub) от коммутаторов 2-го уровня (switch).
a. Коммутаторы работают на более высоком уровне модели OSI, чем концентраторы
b. Коммутаторы не могут усиливать сигнал, в отличие от концентраторов
c. Коммутаторы избирательно ретранслируют широковещательные кадры, концентраторы передают широковещательные кадры на все свои порты
d. Коммутаторы анализируют IP-адреса во входящем пакете, а концентраторы анализируют MAC-адреса

Какой из перечисленных компонентов НЕ входит в архитектуру подсистемы безопасности Windows?
a. Security Reference Monitor
b. Local Security Authority
c. NetBIOS
d. Security Accounts Manager

Выберите верное утверждение:
a. Протокол L2TP не имеет встроенных механизмов защиты информации
b. Протокол L2TP не применяется при создании VPN
c. Протокол PPTP более функциональный и гибкий чем L2TP, но требует более сложных настроек
Какой протокол служит, в основном, для передачи мультимедийных данных, где важнее своевременность, а не надежность доставки?
a. TCP
b. UDP
c. TCP, UDP

Протокол передачи команд и сообщений об ошибках:
a. ICMP
b. SMTP
c. TCP

С помощью какой команды можно просмотреть таблицу маршрутизации?
a. Route
b. Ping
c. Tracert

Какой из перечисленных алгоритмов считается нестойким и не рекомендуется к использованию в новых системах?
a. AES-256
b. SHA-3
c. MD5
d. RSA-2048

Что из перечисленного НЕ относится к этапам жизненного цикла криптографического ключа?
a. Генерация
b. Распределение
c. Компиляция
d. Уничтожение

Критерии оценки для проведения промежуточной аттестации по дисциплине (тестирование)

Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок.

Оценка	Уровень сформированности компетенции	Критерии
«Отлично» («зачтено»)	Высокий	Выполнено более 80% заданий предложенного теста
«Хорошо» («зачтено»)	Хороший	Выполнено 60-80% заданий предложенного теста
«Удовлетворительно» («зачтено»)	Достаточный	Выполнено 35-60% заданий предложенного теста
«Неудовлетворительно» («не зачтено»)	Недостаточный	Выполнено менее 35% заданий предложенного теста

Обновление оценочных материалов дисциплины

обсуждено и рекомендовано к утверждению решением кафедры наименование кафедры
от ___ _____ 20_ г., протокол № ___

одобрено Научно-методическим советом _____ от ___ _____ 20__ г., протокол №____