

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДЕН
на заседании кафедры
«19» марта 2024 г., протокол № 8
И.О. заведующего кафедрой



Осипов Г.С.

**ФОНД
ОЦЕНОЧНЫХ СРЕДСТВ
ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

Б1.О.24 Методы и средства криптографической защиты информации

Направление подготовки
10.03.01 Информационная безопасность

профиль
Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)

**Уровень высшего образования
БАКАЛАВРИАТ**

Южно-Сахалинск
2024 г.

1. Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.1 Знает основные понятия криптографии и криптографические методы защиты информации; ОПК-9.2 Умеет определять наличие типовых технических каналов утечки информации, а также применять методики расчета и инструментального контроля показателей технической защиты информации на объектах информатизации ПК-9.3. Владеет практическими навыками обоснованного выбора и использования СКЗИ при решении задач профессиональной деятельности..
ОПК 4.3	Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3.1 - Знает основные меры по защите информации в автоматизированных системах, а также содержание эксплуатационной документации автоматизированной системы; ОПК-4.3.2 - Умеет устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств; ОПК-4.3.3 - Владеет навыками осуществления автономной наладки технических и программных средств системы защиты информации автоматизированной системы.

2. Паспорт фонда оценочных средств по дисциплине (модулю)

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Тема 1. Математические основы криптографии.	ОПК-9, ОПК 4.3	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
2.	Тема 2. Основные цели и задачи криптографии	ОПК-9, ОПК 4.3	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
3.	Тема 3. Историческая криптография.	ОПК-9, ОПК 4.3	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
4.	Тема 4. Симметричное шифрование	ОПК-9, ОПК 4.3	Задания к лабораторным работам,

			контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
5.	Тема 5. Хеширование	ОПК-9, ОПК 4.3	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
6.	Тема 6. Поточное шифрование	ОПК-9, ОПК 4.3	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
7.	Тема 7. ГСПЧ и проверка их качества	ОПК-9, ОПК 4.3	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
8.	Тема 8. Криптография с открытым ключом	ОПК-9, ОПК 4.3	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
9.	Тема 9. Электронная подпись	ОПК-9, ОПК 4.3	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
10.	Тема 10 Протоколы	ОПК-9, ОПК 4.3	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
	экзамен	ОПК-9, ОПК 4.3	Вопросы к экзамену

Лабораторное занятие №1 (4 ч.)

Тема Математические основы криптографии

Вопросы для обсуждения:

1. Криптографические методы защиты информации.
2. Шифрование.
3. Хеширование.
4. Электронная подпись.

Задания:

1. Перечислите и кратко охарактеризуйте основные задачи обеспечения информационной безопасности, решаемые с помощью криптографических методов.
2. Раскройте определения: шифрование, зашифрование, расшифрование, дешифрование.
3. Зашифровать слово CRYPTOGRAPHY подстановочным шифром, самостоятельно выбрав ключ шифрования из симметрической группы S26.
4. Зашифровать слово CRYPTOGRAPHY перестановочным шифром, самостоятельно выбрав ключ шифрования из симметрической группы
 - 4.1. S3.
 - 4.2. S4.
 - 4.3. S6.

Лабораторное занятие №2 (2 ч.)

Тема Основные цели и задачи криптографии

Вопросы для обсуждения:

1. Сравнение первой степени с одним неизвестным.
2. Китайская теорема об остатках.
3. Генерация простых чисел.
4. Тест на простоту.
5. Алгоритмы работы с большими числами.

Задания:

1. Чем шифрование отличается от кодирования?
2. Приведите известные вам классификации криптосистем.
3. Укажите основные отличия между современной и классической криптографией.

Зашифровать слово CRYPTOGRAPHY аффинным рекуррентным шифром, самостоятельно выбрав ключ шифрования. Указать, какие преимуществами обладает аффинный рекуррентный шифр по сравнению с аффинным.

4. Зашифровать слово CRYPTOGRAPHY шифром Хилла, самостоятельно выбрав ключевую матрицу размерности

4.1. 2x2.

4.2. 3x3.

4.4. 4x4.

Лабораторное занятие №3 (4 ч.)

Тема Историческая криптография

Вопросы для обсуждения:

1. Математическая модель шифра.
2. Классические шифры: подстановочный, перестановочный.
3. Шифр Хилла.
4. Шифры гаммирования.

Лабораторное занятие №4 (2 ч.)

Тема Симметричное шифрование.

Вопросы для обсуждения:

ГОСТ 28147-89.

1. ГОСТ Р 34.12-2015.
2. ГОСТ Р 34.13-2015.
3. Режимы шифрования.

Задания:

1. Сравните аффинный шифр и шифр Хилла с точки зрения криптостойкости.
2. Опишите способы криптоанализа:
3. аффинного шифра;
4. шифра Хилла;
5. шифра гаммирования.
6. Зашифровать слово CRYPTOGRAPHY табличным шифром гаммирования, самостоятельно выбрав ключ шифрования.
7. Зашифровать слово CRYPTOGRAPHY шифром Вижинера, самостоятельно выбрав
- 7.1. циклический ключ шифрования.
- 7.2. самоключ по открытому тексту.
- 7.3. самоключ по шифртексту.

Лабораторное занятие №5 (4 ч.)

Тема Хеширование

Вопросы для обсуждения:

1. Криптографические хеш-функции.
2. ГОСТ Р 34.11- 2012.
3. SHA-3.

Задания:

1. Зашифровать слово CRYPTOGRAPHY шифром простой замены над конечным полем, самостоятельно выбрав ключ шифрования и неприводимый многочлен.
2. Перечислите режимы работы ГОСТ 28147-89. Для чего служит каждый из данных режимов?
3. Сравните DES и ГОСТ 28147-89

Лабораторное занятие №6 (2 ч.)

Тема Поточное шифрование

Вопросы для обсуждения:

1. Принципы поточного шифрования.
2. Типы поточного шифрования.
3. Синхронные и самосинхронизирующиеся шифры.
4. Шифр RC-4 как пример поточного алгоритма шифрования

Задания:

1. Сравните AES и ГОСТ 28147-89.
2. Перечислите основные свойства хеш-функций.
3. Выработать общий секретный элемент данных по протоколу Диффи-Хеллмана, взяв значения $p = 127$, $g = 12$, а x и y выбрав самостоятельно.

Лабораторное занятие №7 (4 ч.)

Тема ГСПЧ и проверка их качества

Вопросы для обсуждения:

1. Генерация случайных чисел.
2. Псевдослучайные числа и их отличия от истинно случайных чисел.
3. Подходы к получению псевдослучайных чисел.
4. Критерии качества псевдослучайных чисел.
5. Виды тестов псевдослучайных последовательностей.
6. Тесты NIST.

Задания:

1. Зашифровать слово CRYPTOGRAPHY по алгоритму Эль-Гамала, самостоятельно выбрав ключевую пару.
2. Сравните DES и ГОСТ 28147-89.
3. Сравните AES и ГОСТ 28147-8

Лабораторное занятие №8 (2 ч.)

Тема. Криптография с открытым ключом

Вопросы для обсуждения:

1. Концепция криптографии с открытым ключом.
2. Протокол Диффи-Хеллмана.
3. Криптосистема RSA.
4. Криптосистема Эль-Гамала.
5. Криптосистема Рабина

Индивидуальные задания (15 вариантов)

Лабораторное занятие №9 (4 ч.)

Тема Электронная подпись

Вопросы для обсуждения:

1. Коды аутентичности сообщений.
2. Электронная подпись.
3. ГОСТ Р 34.10-2012.
4. Инфраструктура открытого ключа

Индивидуальные задания (15 вариантов)

Лабораторное занятие №10 (2 ч.)

Тема Протоколы

Вопросы для обсуждения:

1. Протокол раздельного вручения бита.
2. Протоколы доказательства знания с нулевым разглашением.
3. Протоколы простановки "слепых" подписей.

4. Протоколы голосования.
5. Протоколы безопасных вычислений

Задания:

1. Что такое эллиптическая криптография?
2. Дайте понятие криптографического протокола.
3. Определить (с вероятностью не менее 0,99609375), является ли простым число
 - 3.1. 353.
 - 3.2. 489.
 - 3.3. 1213.

Форма контроля – *экзамен*

Примерные вопросы к экзамену

1. Алгебраические структуры. Свойства алгебраических структур. Группы, подгруппы.
2. Циклические группы.
3. Кольца. Кольца классов вычетов.
4. Поля. Поля Галуа.
5. Цели и задачи криптографии. Основные понятия.
6. Простейшие шифры: простой замены, перестановочный, аффинный.
7. Шифр Хилла.
8. Генерация простых чисел.
9. Шифры гаммирования. Шифр Вернама (одноразовый блокнот).
10. ГОСТ Р 34.12-2015. Шифр «Магма».
11. ГОСТ Р 34.12-2015. Шифр «Кузнечик».
12. Генерация псевдослучайных последовательностей и их тесты.
13. Поточное шифрование.
14. Стандарт шифрования DES.
15. Стандарт шифрования AES.
16. Криптография с открытым ключом.
17. Ранцевая криптосистема.
18. Криптосистема RSA.
19. Криптосистема Эль-Гамала.
20. Протокол Диффи-Хеллмана.
21. Алгоритмы работы с большими числами.
22. Хеш-функции. Свойства хеш-функций.
23. Коды аутентичности сообщений. Электронная подпись.
24. ГОСТ Р 34.10-2012.
25. Протокол передачи бита.
26. Слепые подписи.
27. Протоколы доказательств знания с нулевым разглашением.
28. Протоколы электронного голосования.
29. Протоколы безопасных вычислений.

Критерии оценивания

Оценка «отлично» выставляется студенту, глубоко и прочно усвоившему программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающему, в ответе которого увязывается теория с практикой, он показывает знакомство с литературой, правильно обосновывает и использует рациональные и современные средства решения поставленной проблемы.

Оценка «хорошо» выставляется студенту, твердо знающему программный материал, грамотно и по существу излагающему его, который не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при

решении поставленной задачи.

Оценка «удовлетворительно» выставляется студенту, который знает только основной программный материал, но не усвоил особенностей, допускает в ответе неточности, некорректно формулирует основные законы и правила, затрудняется в выполнении практических задач.

Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает в ответе существенные ошибки, с затруднениями выполняет практические задания.

Форма контроля	За одну работу		Всего	
	Мин. баллов	Макс. баллов	Мин. баллов	Макс. баллов
Текущий контроль:				
Активная работа на занятии	0,25	0,5	9	18
Выполнение домашнего задания	0,75	0,75	27	27
Выполнение заданий самостоятельной работы	1	3	1	3
коллоквиум	1	3	3	9
Промежуточная аттестация (экзамен)			20	43
Итого за семестр			60	100

Составитель _____

Осипов Г.С., профессор кафедры информатики

«19» марта 2024 г.