МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ
Директор института прикладной
математики и компьютерных наук
_____А.В. Замятин
«_02_» ____мая_____ 2021 г.

Фонд оценочных средств по дисциплине

Методы и средства криптографической защиты информации

Специальность
10.05.01 Компьютерная безопасность
код и наименование специальности

Анализ безопасности компьютерных систем
наименование специализации

Томск–2021

ФОС составил:
канд. техн. наук,
доцент кафедры компьютерной безопасности  В.Н. Тренькаев

Рецензент:
канд. техн. наук,
заведующий кафедрой компьютерной безопасности  С.А. Останин

Фонд оценочных средств одобрен на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 17 июня 2021 г. № 05

Председатель УМК ИПМКН,
д-р техн. наук, профессор  С.П. Сущенко

Фонд оценочных средств (ФОС) является элементом системы оценивания сформированности компетенций у обучающихся в целом или на определенном этапе ее формирования.

ФОС разрабатывается в соответствии с рабочей программой (РП) дисциплины и включает в себя набор оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине.

1. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения, характеризующие этапы формирования компетенций)	**Критерии оценивания результатов обучения**			
			Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.	ИОПК-2.2 Определяет порядок настройки и эксплуатации программных средств системного и прикладного назначений, в том числе отечественного производства, используемых для решения задач профессиональной деятельности; ИОПК-2.3 Формулирует предложения по применению программных средств системного и прикладного назначений, в том числе	ОР-2.2.1 Уметь: формулировать предложения по применению программных средств, реализующих криптографические алгоритмы	Отлично сформированное умение формулировать предложения по применению программных средств, реализующих криптографические алгоритмы	Хорошее умение формулировать предложения по применению программных средств, реализующих криптографические алгоритмы	Удовлетворительное умение формулировать предложения по применению программных средств, реализующих криптографические алгоритмы .	Неудовлетворительное умение формулировать предложения по применению программных средств, реализующих криптографические алгоритмы

	отечественного производства, используемых для решения задач профессиональной деятельности.					
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.	ИОПК-10.1 Осуществляет анализ тенденций развития методов и средств криптографической защиты информации; ИОПК-10.2 Применяет средства криптографической защиты информации при решении задач профессиональной деятельности.	ОР-10.1.1 Знать: типовые криптографические алгоритмы, используемые в компьютерных системах и сетях	Высокий уровень знаний; способность самостоятельного анализа проблем предметной области.	В целом успешные, но содержащие отдельные пробелы знания.	Фрагментарные, неполные знания без грубых ошибок.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки.
ОПК-13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.	ИОПК-13.1 Предпринимает необходимые действия по сбору и анализу исходных данных для проектирования компонент программных и программно-аппаратных средств защиты информации в компьютерных системах; ИОПК-13.2 Определяет параметры функционирования, архитектуру и	ОР-13.1.1 Уметь: разрабатывать компоненты программных средств защиты информации, реализующих криптографические алгоритмы	Отлично сформированное умение разрабатывать компоненты программных средств защиты информации, реализующих криптографические алгоритмы	Хорошее умение разрабатывать разрабатывать компоненты программных средств защиты информации, реализующих криптографические алгоритмы	Удовлетворительное умение разрабатывать компоненты программных средств защиты информации, реализующих криптографические алгоритмы .	Неудовлетворительное умение разрабатывать компоненты программных средств защиты информации, реализующих криптографические алгоритмы

	интерфейсы компонент программных и программно-аппаратных средств защиты информации в компьютерных системах; ИОПК-13.3 Проводит анализ компонент программных и программно-аппаратных средств защиты информации в компьютерных системах с целью определения уровня обеспечиваемой ими защищенности и доверия.					
ПК-2 Способен разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей	ИПК-2.1 Определяет угрозы безопасности и их возможные источники, каналы утечки информации ИПК-2.2 Разрабатывает математические модели, реализуемые в средствах защиты информации ИПК-2.3 Проводит исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации	ОР-2.1.1 Знать: математические методы исследования криптографических алгоритмов.	Высокий уровень знаний; способность самостоятельного анализа проблем предметной области.	В целом успешные, но содержащие отдельные пробелы знания.	Фрагментарные, неполные знания без грубых ошибок.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки.

ПК-3 Способен проектировать программно-аппаратные средств защиты информации компьютерных систем и сетей	ИПК-3.2 Разработка проектов программных и аппаратных средств защиты информации в соответствии с техническим заданием	ОР-3.2.1 Уметь: корректно использовать криптографические алгоритмы при решении задач защиты информации	Отлично сформированное умение корректно использовать криптографические алгоритмы при решении задач защиты информации	Хорошее умение корректно использовать криптографические алгоритмы при решении задач защиты информации	Удовлетворительное умение корректно использовать криптографические алгоритмы при решении задач защиты информации .	Неудовлетворительное умение корректно использовать криптографические алгоритмы при решении задач защиты информации

2. Этапы формирования компетенций и виды оценочных средств

№	Этапы формирования компетенций (разделы дисциплины)	Код и наименование результатов обучения	Вид оценочного средства (тесты, задания, кейсы, вопросы и др.)
1.	Введение в криптографию	ОР-10.1.1, ОР-2.1.1 ОР-10.1.1 Знать: типовые криптографические алгоритмы, используемые в компьютерных системах и сетях ОР-2.1.1 Знать: математические методы исследования криптографических алгоритмов	контрольные задания, опросы на занятиях
2.	Шифры замены и перестановки	ОР-10.1.1, ОР-2.1.1 ОР-10.1.1 Знать: типовые криптографические алгоритмы, используемые в компьютерных системах и сетях ОР-2.1.1 Знать: математические методы исследования криптографических алгоритмов	контрольные задания, опросы на занятиях
3.	Абсолютно стойкие шифры	ОР-2.1.1 ОР-2.1.1 Знать: математические методы исследования криптографических алгоритмов	контрольные задания, опросы на занятиях
4.	Блочные шифры	ОР-10.1.1, ОР-2.1.1 ОР-3.2.1 ОР-10.1.1 Знать: типовые криптографические алгоритмы, используемые в компьютерных системах и сетях ОР-2.1.1 Знать: математические методы исследования криптографических алгоритмов ОР-3.2.1 Уметь: корректно использовать криптографические алгоритмы при решении задач защиты информации	контрольные задания, опросы на занятиях
5.	Поточные шифры	ОР-10.1.1, ОР-2.1.1 ОР-3.2.1 ОР-10.1.1 Знать: типовые криптографические алгоритмы, используемые в компьютерных системах и сетях ОР-2.1.1 Знать: математические методы исследования криптографических алгоритмов ОР-3.2.1 Уметь: корректно использовать криптографические алгоритмы при решении задач защиты информации	контрольные задания, опросы на занятиях

6.	Ассиметричные шифры	ОР-10.1.1, ОР-2.1.1 ОР-3.2.1 ОР-10.1.1 Знать: типовые криптографические алгоритмы, используемые в компьютерных системах и сетях ОР-2.1.1 Знать: математические методы исследования криптографических алгоритмов ОР-3.2.1 Уметь: корректно использовать криптографические алгоритмы при решении задач защиты информации	контрольные задания, опросы на занятиях
7.	Цифровая подпись	ОР-10.1.1, ОР-2.1.1 ОР-3.2.1 ОР-10.1.1 Знать: типовые криптографические алгоритмы, используемые в компьютерных системах и сетях ОР-2.1.1 Знать: математические методы исследования криптографических алгоритмов ОР-3.2.1 Уметь: корректно использовать криптографические алгоритмы при решении задач защиты информации	контрольные задания, опросы на занятиях
8.	Криптографические функции хеширования.	ОР-10.1.1, ОР-2.1.1 ОР-3.2.1 ОР-10.1.1 Знать: типовые криптографические алгоритмы, используемые в компьютерных системах и сетях ОР-2.1.1 Знать: математические методы исследования криптографических алгоритмов ОР-3.2.1 Уметь: корректно использовать криптографические алгоритмы при решении задач защиты информации	контрольные задания, опросы на занятиях
9.	Теория секретных систем Шеннона.	ОР-2.1.1 ОР-2.1.1 Знать: математические методы исследования криптографических алгоритмов	контрольные задания, опросы на занятиях
10.	Методы криптоанализа.	ОР-2.1.1, ОР-13.1.1, ОР-3.2.1 ОР-2.1.1 Знать: математические методы исследования криптографических алгоритмов ОР-13.1.1 Уметь: разрабатывать компоненты программных средств защиты информации, реализующих криптографические алгоритмы	лабораторные работы, контрольные задания, опросы на занятиях

		ОР-3.2.1 Уметь: корректно использовать криптографические алгоритмы при решении задач защиты информации	
11.	Автоматная криптография.	ОР-2.1.1 ОР-2.1.1 Знать: математические методы исследования криптографических алгоритмов	контрольные задания, опросы на занятиях
12.	Средства криптографической защиты информации.	ОР-2.2.1, ОР-3.2.1 ОР-2.2.1 Уметь: формулировать предложения по применению программных средств, реализующих криптографические алгоритмы ОР-3.2.1 Уметь: корректно использовать криптографические алгоритмы при решении задач защиты информации	лабораторные работы, контрольные задания, опросы на занятиях

3. Типовые контрольные задания или иные материалы, необходимые для оценки образовательных результатов обучения

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине.

Примеры типовых вариантов контрольных заданий:

- Задание по теме “Шифры замены”. Зашифровать свою фамилию аффинным шифром, шифром Виженера, шифром Хилла, показывая корректность выбранных ключей, т.е. существование обратного элемента.
- Используя CrypTool-Online (https://www.cryptool.org) подсчитать частные характеристики произвольного большого открытого текста, зашифровать любой текст с помощью сдвигового шифра и подсчитать частные характеристики зашифрованного текста. Далее сравнить с таковыми, полученными для произвольного отрытого текста, выдвинуть гипотезу о таблице замены, проверить гипотезу, сравнив с истинной таблицей замены.
- Построить таблицу шифрования произвольного шифра, когда множество открытых(шифрованных) текстов X=Y={0,1,2}, множество ключей K={0,1,2}. Реализовать атаку на основе шифртекста, при условии, что все ключи равновероятны, но среди открытых текстов есть сильно вероятный текст. Определить при перехвате какого шифротекста получается наилучший вариант восстановления открытого текста.
- Сгенерировать произвольный открытый текст (8 бит) и ключ (10 бит). Вычислить шифрованный текст (8 бит), который получается после первого раунда упрощенного варианта DES (Simplified DES). При этом представить все промежуточные результаты вычислений как при генерации раундовых ключей, так и при вычислении значений раундовой функции, т.е. после каждого P-блока, S-блока, XOR.

- Сгенерировать произвольный открытый текст (16 бит) и раундовый ключ (16 бит). Вычислить шифрованный текст (16 бит), который получается после первого раунда упрощенного варианта шифра AES (Simplified AES). При этом представить все промежуточные результаты вычислений, т.е. после каждого преобразования SubNibbles, ShiftRows, MixColumns, AddRoundKey.
- Построить псевдослучайную последовательность небольшой длины, выбрав малые произвольные параметры генератора (модуль, начальные значение и т.п.) и используя алгоритм середины квадрата, линейный конгруэнтный генератор, аддитивный генератор Фибоначчи, инверсный конгруэнтный генератор, регистр сдвига с линейной обратной связью, генератор с квадратичным остатком.
- Вычислить несколько элементов псевдослучайной последовательности при произвольно выбранном ключе, когда в качестве генератора используется упрощенный вариант RC4 (4 или 8 ячеек вместо 256). В решении представить все промежуточные результаты вычислений.
- Реализовать атаку на подпись RSA по выбранному шифротексту, когда при подписывании и шифровании используется одинаковый ключ, перехвачен шифротекст и известен открытый ключ отправителя сообщения, а требуется найти исходный открытый текст без знания закрытого ключа: выбрать параметры шифра, вычислить открытую и закрытую экспоненты, зашифровать произвольный открытый текст, провести необходимые вычисления со стороны атакующего, подписать замаскированное сообщение атакующего, провести финальные вычисления со стороны атакующего и восстановить открытый текст.
- Реализовать атаку на шифр Эль-Гамаля на основе шифртекста, когда при шифровании различных сообщений используется одно и тоже значение случайной величины: определить, что надо знать атакующему, выбрать параметры шифра, вычислить открытый и закрытый ключи, зашифровать необходимое количество произвольных открытых текстов, провести вычисления со стороны атакующего, убедится в правильности результатов атаки.

Пример типового варианта лабораторной работы:

- Выполнить линейный криптоанализ учебного блочного шифра. Учебный шифр и методика выполнения лабораторной работы представлены в книге Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. – М: Гелиос АРВ, 2006. – 376с. Глава 9. Лабораторно-практические работы (стр.206-280).

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине.

Примерный перечень билетов к экзамену (7 семестр):

Билет 1.
1. Криптографическая стойкость шифра. Основные криптоаналитические атаки.
2. Шифр DES: общая схема шифра, функция шифрования.

Билет 2.
1. Конфиденциальность, целостность, доступность, аутентификация, невозможность отказа от авторства.
2. Шифр DES: общая схема шифра, генерация раундовых ключей.

Билет 3.
1. Организация секретной связи с использованием симметричного, асимметричного, гибридного шифрования.
2. Шифр ГОСТ 28147-89 (Магма): общая схема шифра, функция шифрования.

Билет 4.
1. Задача аутентификации сообщения (имитовставка и цифровая подпись).
2. Шифр ГОСТ 28147-89 (Магма): общая схема шифра, генерация раундовых ключей.

Билет 5.
1. Шифры простой замены. Шифр Цезаря. Сдвиговый шифр.
2. Режим использования блочных шифров (ECB).

Билет 6.
1. Частотный криптоанализ шифров простой замены.
2. Сравнение блочных шифров ГОСТ 28147-89 и DES.

Билет 7.
1. Шифры многоалфавитной замены. Шифры гаммирования.
2. Режим использования блочных шифров (CBC).

Билет 8.
1. Криптоанализ шифров многоалфавитной замены.
2. Режим использования блочных шифров (CFB).

Билет 9.
1. Шифры многозначной замены. Шифр пропорциональной замены.
2. Режим использования блочных шифров (OFB).

Билет 10.
1. Маршрутные перестановки. Шифр вертикальной перестановки.
2. Шифр AES: требования к стандарту, архитектура “квадрат”, поле AES

Билет 11.
1. Криптоанализ шифров вертикальной перестановки на основе запретных биграмм.
2. Комбинирующий и фильтрующий генераторы.

Билет 12.
1. Модель шифра по К.Шеннону.
2. Шифр AES: общая схема, базовые операции.

Билет 13.
1. Необходимые и достаточные условия абсолютно стойкого шифра.
2. Поточные шифры на базе регистров сдвига с линейной обратной связью.

Билет 14.
1. Принципы построения блочных шифров. Сеть Фейстеля.
2. Схема поточного шифра. Требования к элементам схемы.

Билет 15.
1. Линейные рекуррентные последовательности
(линейная сложность, теорема о максимальном периоде).
2. Шифр Эль-Гамаля.

Билет 16.
1. Поточные шифры. Генератор Геффе.
2. Шифр RSA. Атаки на шифр RSA.

Билет 17.
1. Поточные шифры. RC4.
2. Свойства шифра Эль-Гамаля.

Билет 18.
1. Поточные шифры. Генератор на базе функции мажорирования.
2. Шифр RSA. Корректность RSA.

Билет 19.
1. Поточные шифры. Чередующий генератор «Старт-Стоп».
2. Ассиметричные шифры. Атака подмены открытого ключа.

Билет 20.
1. Поточные шифры. A5.
2. Ассиметричные шифры. Односторонняя функция с лазейкой.

Билет 21.
1. Код аутентификации сообщения (имитовставка).
Атаки на ключевые хэш-функции (имитация, подмена).
2. Цифровая подпись RSA.

Билет 22.
1. Функции хеширования. Конструкция Меркла-Дамгарда.
2. Цифровая подпись Эль-Гамаля.

Билет 23.
1. Требования к безключевым хэш-функциям.
2. Цифровая подпись Фиата-Шамира.

Билет 24.
1. Бесключевые хэш-функции. Атака “дней рождения”.
2. Инфраструктура открытых ключей.

Билет 25.
1. Ключевые хэш-функции на основе блочных шифров.
2. Свойства цифровой подписи. Сравнение с рукописной подписью.

Билет 26.
1. Ключевые хэш-функции на основе безключеых хэш-функций.
2. Генераторы псевдослучайных чисел. Требования к генераторам.

Билет 27.
1. Регистровое представление функции сжатия хэш-функции MD4/5.
2. Атаки на цифровую подпись.

Примерный перечень вопросов к экзамену (8 семестр):

1. Схема секретной системы. Примеры секретных систем.
2. Параметры секретных систем: количество секретности, объем ключа и др.
3. Алгебра секретных систем.
4. Эндоморфная секретная система.
5. Идемпотентная секретная система.
6. Чистые и смешанные секретные системы.
7. Свойства чистых секретных систем.
8. Подобные секретные системы.
9. Ненадежность (условная энтропия) как теоретическая мера секретности.
10. Идеальная секретная система.
11. Автоматы как компоненты криптосистем: генераторы ключевого потока.
12. Автоматы как компоненты криптосистем: комбайнеры.
13. Автоматы как компоненты криптосистем: клеточные автоматы.
14. Автоматы как компоненты криптосистем: пурпурная машина.
15. Шифр Закревского.
16. Равносильность поточных и автоматных шифрсистем.
17. Конечно-автоматная криптосистема с открытым ключом (FAPKC).
18. Криптоанализ. Метод полного/последовательного опробования ключей.
19. Криптоанализ. Метод «встреча посередине».
20. Криптоанализ. Дифференциальный метод.
21. Криптоанализ. Линейный метод.
22. Криптоанализ. Корреляционный метод.
23. Криптоанализ. Алгебраический метод.
24. Атаки по побочным каналам.

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

4.1. Методические материалы для оценки текущего контроля успеваемости по дисциплине.

Текущий контроль подразумевает выполнение лабораторных работ/контрольных заданий. Выполнение лабораторной работы/контрольного задания оценивается в 100 баллов:

0-20 Студент не разбирается в задаче, не знает методов решения, не отвечает, либо отвечает, но с грубыми ошибками на вопросы преподавателя.

21-40 Студент слабо разбирается в задаче, плохо знает методы решения, не отвечает, либо отвечает, но с ошибками на вопросы преподавателя.

41-60 Студент в целом удовлетворительно разбирается в задаче, использует методы решения при подсказке преподавателя, отвечает на вопросы неуверенно, но с негрубыми ошибками. Представляет работу на защите удовлетворительно.

61-80 Студент в целом уверенно разбирается в задаче, знает и использует методы решения практически самостоятельно, отвечает на вопросы с замечаниями. Представляет работу на защите в целом хорошо, с замечаниями.

81-100 Студент отлично разбирается в задаче, знает и использует методы решения самостоятельно, отвечает на вопросы уверенно. Представляет работу на защите отлично, уверенно.

Допуском до экзамена является выполнение 80% лабораторных работ/контрольных заданий, с оценкой за каждую не менее 80 баллов.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Промежуточный контроль знаний по дисциплине осуществляется в форме экзамена, который подразумевает подготовку студента и ответов в устной/письменной форме на несколько контрольных вопросов по всему курсу. Критерии выставления оценок:

Отлично - студент в совершенстве овладел всеми теоретическими вопросами обязательного материала по разделам лекционного курса, показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях.

Хорошо - студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях.

Удовлетворительно - студент имеет недостаточно глубокие знания по теоретическим разделам обязательного материала дисциплины, но показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях.

Неудовлетворительно - студент имеет существенные пробелы по отдельным теоретическим разделам специальной дисциплины или не показал требуемые умения и навыки при выполнении заданий на лабораторных занятиях.