Приложение 1

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
«_15_» ____июня_____ 2023 г.

Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине
(Оценочные средства по дисциплине)

Введение в компьютерную безопасность

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Интеллектуальный анализ больших данных

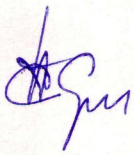
Томск–2023

ОС составил:
канд. физ.-мат. наук,
старший преподаватель кафедры компьютерной безопасности  А.С. Твардовский

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

Оценочные средства одобрены на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН).

Протокол от 08.06.2023 г. № 2

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

Оценочные средства (ОС) являются элементом системы оценивания сформированности компетенций у обучающихся в целом или на определенном этапе ее формирования.

ОС разрабатывается в соответствии с рабочей программой (РП) дисциплины.

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

2.

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения, характеризующие этапы формирования компетенций)	**Критерии оценивания результатов обучения**	
			Зачтено	Не зачтено
ОПК-2. Способен совершенствовать и реализовывать новые математические методы решения прикладных задач.	ИОПК-2.1. Использует результаты прикладной математики для освоения, адаптации новых методов решения задач в области своих профессиональных интересов.	ОР-2.1.1 обучающийся сможет - использовать современные информационно-коммуникационные технологии для решения задач в области прикладной математики с учетом требований информационной безопасности; ОР-2.1.2 обучающийся сможет - использовать известные криптографические системы для обеспечения безопасности компьютерных систем; ОР-2.1.3 обучающийся сможет - использовать основные виды политик контроля доступа и соответствующие модели безопасности для разработки и анализа механизмов контроля доступа компьютерных систем;	Достижение обучающимся необходимого уровня знаний в области политик и моделей контроля доступа, а также криптографических систем, понимание математических основ данных областей; способность использовать современные информационно-коммуникационные технологии, криптографические системы и механизмы контроля доступа для решения задач в области прикладной математики с учетом требований информационной безопасности.	Обучающийся не имеет четкого представления об изучаемом материале, допускает грубые ошибки при использовании математического аппарата в области политик и моделей контроля доступа, а также криптографических систем; не способен обосновать использование современных информационно-коммуникационных технологий, криптографических систем и механизмов контроля доступа для решения задач в области прикладной математики с учетом требований информационной безопасности.

ОПК-4. Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.	ИОПК-4.2. Учитывает основные требования информационной безопасности.	ОР-4.2.1 обучающийся сможет - учитывать основные требования информационной безопасности к политикам контроля доступа и криптографическим протоколам защиты данных; ОР-4.2.2 обучающийся сможет - учитывать основные направления атак на распространённые телекоммуникационный протоколы для организации мер по противодействию таким атакам;	Обучающийся ориентируется в основных направлениях атак на распространённые телекоммуникационный протоколы и знаком с мерами по противодействию таким атакам; способен учитывать основные требования информационной безопасности к политикам контроля доступа и криптографическим протоколам защиты данных.	Обучающийся не ориентируется в основных направлениях атак на распространённые телекоммуникационный протоколы и не может сформулировать меры по противодействию таким атакам; плохо представляет основные требования информационной безопасности к политикам контроля доступа и криптографическим протоколам защиты данных.
ПК-1. Способен разрабатывать и применять математические методы, алгоритмы, программное обеспечение для решения задач научно-исследовательской и проектной деятельности.	ИПК-1.2. Применяет существующие математические методы, алгоритмы и программное обеспечение для решения задач в области профессиональной деятельности	ОР-1.2.1 обучающийся сможет - применять существующие примитивы разработки систем контроля доступа и механизмы их реализации для разработки безопасных компьютерных систем; ОР-1.2.2 обучающийся сможет - применять навыки обеспечения безопасного функционирования телекоммуникационных протоколов; ОР-1.2.3 обучающийся сможет - применять знания математических основ криптографических алгоритмов для их программной реализации и внедрения в компьютерные системы;	Обучающийся демонстрирует способность применять существующие примитивы разработки систем контроля доступа и механизмы их реализации для разработки безопасных компьютерных систем; в состоянии спроектировать и внедрить программную реализацию криптографического алгоритма в компьютерную систему; способен организовать безопасное функционирование телекоммуникационных протоколов.	Обучающийся не знаком с принципами разработки систем контроля доступа и механизмами их реализации для обеспечения безопасности компьютерных систем; не способен спроектировать и внедрить программную реализацию криптографического алгоритма в компьютерную систему; не понимает основ организации безопасного функционирования телекоммуникационных протоколов.

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.	Общие понятия компьютерной безопасности	ОР-2.1.1, ОР-4.2.1	зачёт (билет и дополнительные вопросы), тест в системе moodle
2.	Основы сетевой безопасности	ОР-4.2.2, ОР-1.2.2, ОР-1.2.1-3	зачёт (билет и дополнительные вопросы), отчёт по проекту, тест в системе moodle
3	Криптографическая защита информации	ОР-2.1.2, ОР-1.2.3, ОР-1.2.1-3	зачёт (билет и дополнительные вопросы), отчёт по проекту, тест в системе moodle
4	Управление доступом	ОР-2.1.3, ОР-1.2.1, ОР-1.2.1-3	зачёт (билет и дополнительные вопросы), отчёт по проекту, тест в системе moodle

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

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине

Проектное задание:

Проект предназначен для группы от одного до трёх человек и заключается в реализации сервиса по хранению ключей пользователей и подписыванию ими электронной документации.

Сервис должен быть реализован как клиент-серверное приложение и поддерживать следующие функции.

a) Система аутентификации и авторизации пользователей.
b) Генерация, приём от клиента и хранение пары из открытого (public) и закрытого (private) ключей.
c) Генерация цифровой подписи, при помощи хранимого сервером закрытого ключа, для загружаемого пользователем документа.

Для реализации цифровой подписи могут быть использованы криптосистемы RSA, DSA, ECDSA, и др. Для генерации хеш-значения рекомендуются алгоритмы семейства SHA.

Результатом выполнения проекта является письменный отчёт.

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине

Список билетов к зачёту:

Билет 1

1. Информационная безопасность. Свойства безопасности информации.
2. AES (Advanced Encryption Standard). Режимы шифрования.

Билет 2

1. Уязвимость, угроза, атака. Классификация атак/угроз
2. MAC (message authentication code).

Билет 3

1. Межсетевые экраны (шлюзы сетевого и прикладного уровней).
2. Передача сеансового ключа (RSA и алгоритм Диффи-Хелмана). Perfect forward secrecy.

Билет 4

1. Канальный уровень. MAC flooding и spoofing.
2. Криптографическая система. Шифрование и расшифрование.

Билет 5

1. Межсетевые экраны (пакетные фильтры).
2. Симметричные и асимметричные шифры. Принципы криптографической защиты Кергкхоффса

Билет 6

1. DDoS атаки (DNS, HTTP, TCP, MAC-flooding).
2. Data Encryption Standard (DES)

Билет 7

1. Протокол DNS и атаки на него.
2. Шифры подстановки и перестановки.

Билет 8

1. Отличия TLS 1.3 и 1.2
2. Поточные и блочные шифры. RC4 и Salsa20

Билет 9

1. Дискреционная и мандатная политики контроля доступа (основные признаки и отличия)
2. Цифровая подпись

Билет 10

1. Терминология в области управления доступом
2. TLS Handshake 1.2

Билет 11

1. Методы реализации политик контроля доступа (IBAC, LBAC, RBAC, ABAC)
2. TLS Records, Alerts, История TLS

Дополнительные вопросы к зачёту:

1. Конфиденциальность, целостность и доступность информации.
2. Уязвимость, угроза, атака.
3. Активная атака (пример)
4. Пассивная атака (пример)
5. Пакетные фильтры
6. Шлюзы сетевого уровня
7. Канальный уровень
8. Коммутатор и маршрутизатор. Отличия.
9. Сетевой уровень TCP/IP
10. Транспортный уровень TCP/IP

11. Прикладной уровень TCP/IP
12. Стек TCP/IP инкапсуляция и декапсуляция данных
13. MAC-spoofing
14. IP-spoofing
15. DDoS-атака
16. Zero window stress
17. SYN-атака
18. HTTP Slow GET/POST
19. Шлюзы прикладного уровня
20. Отравление кэша DNS
21. DNS Amplification
22. Криптографическая система
23. Может ли сумма по модулю 2 (XOR) ключа с открытым тестом быть стойким шифром
24. Шифры подстановки
25. Шифры перестановки
26. Симметричный шифр
27. Ассиметричный шифр
28. Потоковый шифр
29. Блочный шифр
30. Раундовая функция в DES
31. Сеть Фейстеля
32. Triple DES
33. State в AES
34. Основные преобразования в AES
35. MAC (message authentication code)
36. RSA
37. Perfect forward secrecy
38. Протокол Диффи-Хеллмана
39. Цифровая подпись
40. Сертификаты
41. Типы записей в TLS
42. Client/Server Hello в TLS
43. TLS Records
44. Отличия TLS 1.2 и 1.3 (не менее двух)
45. Политика, механизм и модель контроля доступа
46. Граф доступов
47. Информационный поток
48. Дискреционная политика
49. Мандатная политика
50. Списки доступа
51. Ролевая модель
52. Атрибутная модель

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

4.1. Методические материалы для оценки текущего контроля успеваемости по дисциплине «Введение в компьютерную безопасность».

Текущий контроль осуществляется при помощи тестов в системе Moodle (moodle.tsu.ru). Для успешного прохождения текущего контроля необходимо набрать не менее 70% от максимальной оценки.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине «Введение в компьютерную безопасность».

Для получения зачёта необходимо выполнить все вышеперечисленные условия.

1. Набрать не менее 70% от максимальной оценки по каждому из тестов в системе Moodle.
2. Предоставить отчёт о выполнении проектного задания, реализация которого соответствует техническому заданию из раздела 3.3.
3. Набрать не менее 7 баллов на устном зачёте, в соответствии со следующими критериями.

Условия	Баллы
Корректный ответ на 1 вопрос из билета	4
Неполный ответ на 1 вопрос из билета	2
Корректный ответ на доп. вопрос (всего не более трёх)	1