

Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:

Директор института прикладной
математики и компьютерных наук



А. В. Замятин

2022 г.

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

Введение в компьютерную безопасность

по направлению подготовки

02.04.02 Фундаментальная информатика и информационные технологии

Направленность (профиль) подготовки:

Математика беспроводных сетей связи и интернета вещей

ОС составил(и):

канд. физ.-мат. наук

старший преподаватель кафедры компьютерной безопасности

Твардовский

А.С.

Рецензент:

канд. тех. 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 12.05. 2022 г. № 4

Председатель УМК ИПМКН,
д-р техн. наук, профессор

С.П. Сущенко

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

ОС разрабатываются в соответствии с рабочей программой (РП).

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	
			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 Владеть: современными информационно-коммуникационными технологиями для решения задач в области прикладной математики с учетом требований информационной безопасности; ОР-2.1.2 Уметь: использовать известные криптографические системы для обеспечения безопасности компьютерных систем; ОР-2.1.3 Знать: виды политик контроля доступа и соответствующие модели безопасности для разработки и анализа механизмов контроля доступа компьютерных систем;	Понимание обучающимся основных политик и моделей контроля доступа, а также криптографических систем, 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.	Отсутствие у обучающегося четкого представления об изучаемом материале, грубые ошибки при использовании математического аппарата в области политик и моделей контроля доступа, а также криптографических систем; неспособность обосновать использование современных информационно-коммуникационных технологий, криптографических систем и механизмов контроля доступа для решения задач в области прикладной математики с учетом требований информационной безопасности.

<p>ОПК-4. Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности</p>	<p>ИОПК-4.2 Учитывает основные требования информационной безопасности.</p>	<p>ОР-4.2.1 Знать: основные требования информационной безопасности к политикам контроля доступа и криптографическим протоколам защиты данных; ОР-4.2.2 Знать: основные направления атак на распространённые телекоммуникационный протоколы для организации мер по противодействию таким атакам;</p>	<p>Обладание знаниями об основных направлениях атак на распространённые телекоммуникационный протоколы и о мерах по противодействию таким атакам; способность учитывать основные требования информационной безопасности к политикам контроля доступа и криптографическим протоколам защиты данных.</p>	<p>Отсутствие знаний об основных направлениях атак на распространённые телекоммуникационный протоколы и о мерах по противодействию таким атакам; непонимание основных требований информационной безопасности к политикам контроля доступа и криптографическим протоколам защиты данных.</p>
<p>ПК-4. Способен управлять получением, хранением, передачей, обработкой больших данных.</p>	<p>ИПК-4.2 Использует методы и инструменты получения, хранения, передачи, обработки больших данных.</p>	<p>ОР-4.2.3 Владеть: навыками проведения контрольных проверок работоспособности и эффективности примитивов разработки систем контроля доступа; ОР-4.2.4 Уметь: разрабатывать требования к безопасному функционированию телекоммуникационных систем и оценивать их работоспособность и эффективность;</p>	<p>Обладание обучающимся навыками проведения контрольных проверок работоспособности и эффективности примитивов разработки систем контроля доступа и механизмов их реализации для разработки безопасных компьютерных систем; умение разрабатывать требования к безопасному функционированию телекоммуникационных систем.</p>	<p>Отсутствие навыков проведения контрольных проверок работоспособности и эффективности примитивов разработки систем контроля доступа и механизмов их реализации для разработки безопасных компьютерных систем; неспособность разрабатывать требования к безопасному функционированию телекоммуникационных систем.</p>

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	Устный зачёт Тестирование
2.	Основы сетевой безопасности	ОР-4.2.2, ОР-4.2.3, ОР-4.2.4	Групповой проект Устный зачёт Тестирование
3.	Криптографическая защита информации	ОР-4.2.3, ОР-4.2.4, ОР-2.1.2	Групповой проект Устный зачёт Тестирование
4.	Управление доступом	ОР-2.1.3, ОР-4.2.3, ОР-4.2.4	Групповой проект Устный зачёт Тестирование

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 одного из трёх заданий.

Варианты проектного задания

1. Приложение для защищённого соединения между узлами сети

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

- a) Генерация общего сеансового ключа (RSA или DH).
- b) Передача текстовых сообщений между клиентом и сервером в зашифрованном симметричной криптосистемой виде.
- c) Использование Hash-функции для обеспечения целостности сообщений.

2. Облачное хранилище текстовых сообщений

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

- a) Система аутентификации и авторизации пользователей.
- b) Создание, изменение, удаление, чтение текстовых сообщений (в файлах или БД) на сервере и передача прав на данные действия другим пользователям.
- c) Хранение паролей на сервере в форме hash-значений.

3. Сервис цифровой подписи (центр сертификации)

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

- a) Система аутентификации и авторизации пользователей.

- b) Генерация и выдача пары из открытого (public) и закрытого (private) ключей для пользователей.
- c) Генерация цифровой подписи документа клиентом.
- d) Проверка подписи для документа посредством сервера.

Результатом выполнения проекта является отчёт с презентацией.

Типовые вопросы из теста

Открытый текст 01110100 был зашифрован суммой по модулю два (XOR), в результате чего был получен закрытый текст 00111100, вычислите ключ. Ответ: 01001000
Шифр Цезаря является шифром подстановки. Ответ: Верно
Выберите верные утверждения <ul style="list-style-type: none"> a) В асимметричной криптографии может использоваться пара из закрытого и открытого ключа (да) b) Асимметричные шифры часто имеют меньшую длину ключа, чем симметричные (нет) c) Симметричные шифры работают быстрее асимметричных (да) d) Симметричные шифры всегда блочные (нет) e) Ключи для шифрования и расшифрования совпадают при использовании симметричного шифра (да)
Установите соответствие DES - Сеть Фейстеля AES - Использование прямоугольной матрицы (state) для промежуточного результата шифрования RSA - Возведение в степень по модулю

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 Керкхоффа

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. Поточковый 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.

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 на каждом тесте. Для допуска к зачёту также необходимо защитить групповой проект.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

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 пункта 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