Приложение 1

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

«_19_» ___мая___ 20_22_ г.

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

Защита информации на уровне программ и данных

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Информационная безопасность

Томск – 2022

ОМ составил(и):

ассистент кафедры компьютерной безопасности  О.В. Брославский

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

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

Протокол от 12 мая 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**			
			Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
ОПК-4. Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.	ИОПК-4.3 Использует современные информационно-коммуникационные технологии для решения задач в области прикладной математики и информатики с учетом требований информационной безопасности.	ОР-1 Знать средства и методы хранения и передачи авторизованной информации. ОР-2 Знать защитные механизмы и средства обеспечения безопасности программ и данных. ОР-3 Знать требования к подсистеме аудита и политике аудита. ОР-4 Уметь противодействовать компьютерным атакам	В совершенстве знает средства и методы хранения и передачи авторизованной информации. В совершенстве знает защитные механизмы и средства обеспечения безопасности программ и данных. В совершенстве знает требования к подсистеме аудита и политике аудита.	Знает средства и методы хранения и передачи авторизованной информации. Знает защитные механизмы и средства обеспечения безопасности программ и данных. Знает требования к подсистеме аудита и политике аудита. Умеет противодействовать	Знает основные средства и методы хранения и передачи авторизованной информации. Знает основные защитные механизмы и средства обеспечения безопасности программ и данных. Знает основные требования к подсистеме аудита и политике аудита.	Не знает средства и методы хранения и передачи авторизованной информации. Не знает защитные механизмы и средства обеспечения безопасности программ и данных. Не знает требования к подсистеме аудита и политике аудита. Не умеет противодействовать компьютерным

		и вирусам с использованием антивирусного программного обеспечения.	В совершенстве умеет противодействовать компьютерным атакам и вирусам с использованием антивирусного программного обеспечения.	компьютерным атакам и вирусам с использованием антивирусного программного обеспечения.	Умеет противодействовать компьютерным атакам с использованием антивирусного программного обеспечения.	атакам с использованием антивирусного программного обеспечения.
ПК-2. Способен оценить уровень безопасности компьютерных систем и разработать программно-аппаратные средства защиты информации.	ИПК-2.1 Осуществляет проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации, разработку требований к программно-аппаратным средствам защиты информации компьютерных систем; ИПК-2.2 Осуществляет разработку требований по защите, формирование политик безопасности компьютерных систем и сетей, проектирование программно-аппаратных средств защиты информации компьютерных систем; ИПК-2.3 Осуществляет проведение анализа безопасности компьютерных систем, проведение сертификации программно-аппаратных средств защиты	ОР-5 Уметь осуществлять анализ программного обеспечения на наличия уязвимостей. ОР-6 Уметь проводить дизассемблирование и отладку программного обеспечения.	В совершенстве умеет осуществлять анализ программного обеспечения на наличия уязвимостей. В совершенстве умеет проводить дизассемблирование и отладку программного обеспечения.	Умеет осуществлять анализ программного обеспечения на наличия уязвимостей. Умеет проводить дизассемблирование и отладку программного обеспечения.	Умеет не все осуществлять анализ программного обеспечения на наличия уязвимостей. Умеет проводить дизассемблирование программного обеспечения.	Не умеет осуществлять анализ программного обеспечения на наличия уязвимостей. Не умеет проводить дизассемблирование программного обеспечения.

	информации и анализ результатов, разработку и тестирование средств защиты информации компьютерных систем.					

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.	Анализ программных реализаций	ОР 1-6	Практические работы, теоретические вопросы
2.	Защита программ от изучения	ОР 1-6	Теоретические вопросы
3.	Программные закладки	ОР 1-6	Теоретические вопросы

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 практических работ:

1. Исследование бинарных приложений, имеющих архитектуру x86
2. Исследование бинарных приложений, имеющих архитектуру AMD64

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине
Примеры тем для теоретических вопросов в устном зачёте:

- Что такое calling convention? Основные СС для архитектуры i386: ключевые особенности и отличия.
- Что такое calling convention? Основные СС для архитектуры amd64: ключевые особенности и отличия.
- Принципы работы вариадических функций в 32-битных СС
- Принципы работы вариадических функций в 64-битных СС
- Особенности стековых фреймов в 64-битных СС
- Динамическая линковка и загрузка кода.
- Механизм сигналов в Linux. Запутывание потока исполнения на основе сигналов.

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

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

Критерием выполнения студентом практической работы является:

- способность студента объяснить алгоритм, реализуемый приложением, предоставляемом в лабораторной работе;
- понимание и способность объяснить низкоуровневые детали реализации алгоритма, сгенерированные компилятор, такие как: соглашение о вызовах, используемое данной функцией, структура стекового фрейма, используемые в приложении методы запутывания.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Промежуточная аттестация по дисциплине проводится в форме устного зачета по теоретическому материалу.

Каждый билет для устного зачёта состоит из двух теоретических вопросов по двум темам дисциплины.