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
«_09_» _июля_ 2021 г.

Фонд оценочных средств по практике

Учебно-лабораторная практика (Защита программ и данных)

Специальность
10.05.01 Компьютерная безопасность
код и наименование специальности

Анализ безопасности компьютерных систем
наименование специализации

Томск–2021

ФОС составил(и):
ассистент кафедры компьютерной безопасности О.В. Брославский

Рецензент:
канд. техн. наук, доцент,
заведующий кафедры 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 (зачтено)	Хорошо (зачтено)	Удовлетворительно (зачтено)	Неудовлетворительно (не зачтено)
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 интерфейсы компонент программных и программно-аппаратных средств защиты	ОР-1 Знать средства и методы хранения и передачи авторизованной информации. ОР-2 Знать защитные механизмы и средства обеспечения безопасности программ и данных.	В совершенстве знает средства и методы хранения и передачи авторизованной информации. В совершенстве знает защитные механизмы и средства обеспечения безопасности программ и данных.	Знает средства и методы хранения и передачи авторизованной информации. Знает защитные механизмы и средства обеспечения безопасности программ и данных.	Знает основные средства и методы хранения и передачи авторизованной информации. Знает основные защитные механизмы и средства обеспечения безопасности программ и данных.	Не знает средства и методы хранения и передачи авторизованной информации. Не знает защитные механизмы и средства обеспечения безопасности программ и данных.

	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.					
ОПК-19. Способен оценивать корректность программных реализаций алгоритмов защиты информации	ИОПК-19.1 Обладает знанием формальных приемов, правил, алгоритмов, технологий создания и документирования контрольных примеров и тестовых наборов данных; ИОПК-19.2 Осуществляет подготовку тестовых наборов данных в соответствии с выбранной методикой, а также проверку работоспособности программного обеспечения на основе разработанных тестовых наборов данных;	ОР-3 Уметь осуществлять анализ программного обеспечения на наличия уязвимостей. ОР-4 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.

	ИОПК-19.3 Содержание Осуществляет сбор и анализ полученных результатов проверки работоспособности программного обеспечения, оценку соответствия программного обеспечения требуемым характеристикам.					
ОПК-20. Способен проводить тестирование и использовать средства верификации механизмов защиты информации.	ИОПК-20.1 Понимает принципы организации, состав и алгоритмы работы механизмов защиты информации, стандарты оценивания защищенности компьютерных систем; ИОПК-20.2 Проводит исследование механизмов защиты информации, в том числе с использованием средств верификации, и делает выводы по оценке защищенности и доверия.	ОР-5 Владеть навыками оценки уровня защиты программ и данных.	В совершенстве владеет навыками оценки уровня защиты программ и данных.	Владеет навыками оценки уровня защиты программ и данных.	Слабо владеет навыками оценки уровня защиты программ и данных.	Не владеет навыками оценки уровня защиты программ и данных.
ПК-2. Способен разрабатывать требования к программно-аппаратным средствам защиты информации	ИПК-2.3 Проводит исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации.	ОР-6 Знать требования к подсистеме аудита и политике аудита. ОР-7 Уметь противодействовать компьютерным атакам и	В совершенстве знает требования к подсистеме аудита и политике аудита. В совершенстве умеет	Знает требования к подсистеме аудита и политике аудита. Умеет противодействовать компьютерным	Знает основные требования к подсистеме аудита и политике аудита. Умеет противодействовать	Не знает требования к подсистеме аудита и политике аудита. Не умеет противодействовать компьютерным

компьютерных систем и сетей компьютерных систем и сетей		вирусам с использованием антивирусного программного обеспечения.	противодействовать компьютерным атакам и вирусам с использованием антивирусного программного обеспечения.	атакам и вирусам с использованием антивирусного программного обеспечения.	компьютерным атакам с использованием антивирусного программного обеспечения.	атакам с использованием антивирусного программного обеспечения.
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 ИПК-3.3 Проведение аттестации программ и алгоритмов на предмет соответствия требованиям защиты информации	ОР-8 Знать основные средства и методы анализа программных реализаций средств защиты информации ОР-9 Владеть навыками анализа программных реализаций средств защиты информации	В совершенстве знает средства и методы анализа программных реализаций средств защиты информации. Владееет навыками анализа программных реализаций средств защиты информации	Знает средства и методы анализа программных реализаций средств защиты информации Владееет навыками анализа программных реализаций средств защиты информации	Знает основные средства и методы анализа программных реализаций средств защиты информации Владееет навыками анализа программных реализаций средств защиты информации	Не знает основные средства и методы анализа программных реализаций средств защиты информации Не владееет навыками анализа программных реализаций средств 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.	Анализ программных реализаций	ОР 1-9	Лабораторные работы, теоретические вопросы
2.	Защита программ от изучения	ОР 1-9	Лабораторные работы, теоретические вопросы
3.	Программные закладки	ОР 1-9	Лабораторные работы, теоретические вопросы
4.	Внедрение программных закладок	ОР 1-9	Лабораторные работы, теоретические вопросы
5.	Противодействие программным закладкам	ОР 1-9	Лабораторные работы, 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 лабораторных работ:

1. Исследование бинарных приложений, имеющих архитектуру x86
2. Исследование бинарных приложений, имеющих архитектуру AMD64
3. Исследование бинарных приложений, имеющих архитектуру ARM
4. Исследование приложений, использующих методы запутывания потока исполнения
5. Исследование приложений, использующих методы сокрытия данных
6. Применение SAT/SMT решателей при исследовании бинарных приложений

3.2. Типовые задания для проведения промежуточной аттестации

Примеры тем для теоретических вопросов в устном зачёте:

- Что такое calling convention? Основные CC для архитектуры i386: ключевые особенности и отличия.
- Что такое calling convention? Основные CC для архитектуры amd64: ключевые особенности и отличия.
- Принципы работы вариадических функций в 32-битных CC
- Принципы работы вариадических функций в 64-битных CC
- Особенности стековых фреймов в 64-битных CC
- 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 практике.

Критерием выполнения студентом лабораторной работы является:

- наличие у студента программной реализации генератора корректных ключей для рассматриваемой лабораторной работы;
- способность студента объяснить алгоритм, реализуемый приложением, предоставляемом в лабораторной работе;
- понимание и способность объяснить низкоуровневые детали реализации алгоритма, сгенерированные компилятором, такие как: соглашение о вызовах, используемое данной функцией, структура стекового фрейма, используемые в приложении методы запутывания.

4.2. Методические материалы для проведения промежуточной аттестации.

Промежуточная аттестация проводится в форме защиты лабораторных работ и устного зачета по теоретическому материалу.

К зачету допускаются только студенты, успешно выполнившие все, предусматриваемые курсом лабораторные работы.

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