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_» _июня_ 2021 г.

Фонд оценочных средств по дисциплине

Анализ уязвимостей программного обеспечения

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	Хорошо	Удовлетворительно	Неудовлетворительно
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 информации в компьютерных системах; ИОПК-13.3 Проводит анализ компонент	ОР-1 Знать основные средства и методы анализа программных реализаций на предмет уязвимостей. ОР-5 Владеть приемами анализа программных реализаций на наличие уязвимостей. ОР-3 Уметь выявлять и устранять уязвимости программных реализаций и локализовать их последствия.	В совершенстве знает основные средства и методы анализа программных реализаций на предмет уязвимостей. В совершенстве владеет приемами анализа программных реализаций на наличие уязвимостей. В совершенстве умеет выявлять и	Знает основные средства и методы анализа программных реализаций на предмет уязвимостей. Владеет приемами анализа программных реализаций на наличие уязвимостей. Умеет выявлять и устранять уязвимости	Знает основные средства анализа программных реализаций на предмет уязвимостей. Слабо владеет приемами анализа программных реализаций на наличие уязвимостей. Умеет выявлять уязвимости программных реализаций и локализовать их последствия.	Не знает основные средства и методы анализа программных реализаций на предмет уязвимостей. Не владеет приемами анализа программных реализаций на наличие уязвимостей. Не умеет выявлять уязвимости программных реализаций и локализовать их последствия.

	программных и программно-аппаратных средств защиты информации в компьютерных системах с целью определения уровня обеспечиваемой ими защищенности и доверия.		устранять уязвимости программных реализаций и локализовать их последствия.	программных реализаций и локализовать их последствия.		
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-2 Знать статические и динамические методы анализы программных реализаций. ОР-4 Уметь проводить экспертизу качества и надежности программных и программно-аппаратных средств обеспечения информационной безопасности.	В совершенстве знает статические и динамические методы анализы программных реализаций. В совершенстве умеет проводить экспертизу качества и надежности программных и программно-аппаратных средств обеспечения информационной безопасности.	Знает статические и динамические методы анализы программных реализаций. Умеет проводить экспертизу качества и надежности программных и программно-аппаратных средств обеспечения информационной безопасности.	Знает основные статические и динамические методы анализы программных реализаций. Умеет проводить экспертизу качества программных средств обеспечения информационной безопасности.	Не знает статические и динамические методы анализы программных реализаций Не умеет проводить экспертизу качества программных средств обеспечения информационной безопасности.
ПК-2. Способен проектировать и разрабатывать средства защиты информации	ИПК-2.3 Осуществляет разработку требований, проектирует и разрабатывает средства защиты информации в	ОР-6 Знать способы, методы и критерии оценки эффективности реализации систем защиты информации.	В совершенстве знает способы, методы и критерии оценки эффективности	Знает способы, методы и критерии оценки эффективности реализации	Знает основные способы, методы и критерии оценки эффективности реализации систем	Не знает способы, методы и критерии оценки эффективности реализации систем

компьютерных систем и сетей	соответствии с техническим заданием		реализации систем защиты информации.	систем защиты информации.	защиты информации.	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.	Актуальные уязвимости современного программного обеспечения	ОР 1-6	Теоретические вопросы
2.	Анализ бинарных уязвимостей программного обеспечения	ОР 1-6	Лабораторные работы, теоретические вопросы
3.	Предотвращение уязвимостей на этапе реализации	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 лабораторных работ:

1. Выданное приложение уязвимо к атаке типа off-by-one. Произвести атаку и получить права администратора в тестовом приложении, доступном по адресу host:port.
2. Выданное приложение уязвимо к атаке переполнения стекового буфера. Произвести атаку и получить возможность выполнения произвольного кода в тестовом приложении, доступном по адресу host:port.
3. Выданное приложение уязвимо к атаке типа Return Oriented Programming. Произвести атаку и получить возможность выполнения произвольного кода в тестовом приложении, доступном по адресу host:port.
4. Выданное приложение уязвимо к атаке типа Return to libc. Произвести атаку и получить возможность выполнения произвольного кода в тестовом приложении, доступном по адресу host:port.

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине

Примеры тем для теоретических вопросов в устном зачёте:

- Атаки на бинарные приложения типа переполнения локального буфера. Методы обнаружения. Способы предотвращения.
- Атаки на бинарные приложения типа переполнения буфера на куче. Методы обнаружения. Способы предотвращения.
- Атаки на бинарные приложения типа Return Oriented Programming. Методы обнаружения. Способы предотвращения.
- Атаки на бинарные приложения типа Return to libc. Методы обнаружения. Способы предотвращения.
- Атаки на бинарные приложения при помощи контроля форматной строки. Методы обнаружения. Способы предотвращения.
- Атаки на бинарные приложения типа arbitrary read. Методы обнаружения. Способы предотвращения.

- Атаки на бинарные приложения типа arbitrary write. Методы обнаружения. Способы предотвращения.
- Атаки на бинарные приложения типа off-by-one. Методы обнаружения. Способы предотвращения.
- Атаки на бинарные приложения типа type confusion. Методы обнаружения. Способы предотвращения.

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

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

Критерием выполнения студентом лабораторной работы является:

- наличие у студента программной реализации атаки на рассматриваемое в рамках лабораторной работы приложение;
- способность студента объяснить суть атаки, уязвимость, приводящую к возможности осуществления атаки, и причины ее возникновения, а также меры, которые необходимо предпринять чтобы сделать произведенную атаку невозможной для воспроизведения злоумышленником.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Промежуточная аттестация по дисциплине проводится в форме 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.