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

Безопасность веб-приложений

Специальность
10.05.01 Компьютерная безопасность
код и наименование специальности

Анализ безопасности компьютерных систем
наименование специализации

Томск–2021

ФОС составил(и):
канд. техн. наук, доцент,
заведующий кафедрой компьютерной безопасности С.А. Останин

Рецензент:
канд. физ.-мат. наук, доцент,
доцент кафедры компьютерной безопасности Н.А. Вихорь

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-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	ИОПК-2.2 Определяет порядок настройки и эксплуатации программных средств системного и прикладного назначений, в том числе отечественного производства, используемых для решения задач профессиональной деятельности.	ОР-1. Владеет навыками использования различных программных средств обеспечения информационной безопасности	В совершенстве владеет навыками использования программных средств	Владеет навыками использования программных средств	Слабо владеет навыками использования программных средств	Не владеет навыками использования программных средств
ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты	ИОПК-9.2 Обладает знанием и демонстрирует навыки применения базовых методов защиты информации в операционных системах, компьютерных сетях и	ОР-2. Знает основные виды и источники уязвимостей веб-приложений ОР-3. Знает методы анализа безопасности веб-приложений. ОР-4. Умеет проводить анализ безопасности веб-приложений.	В совершенстве знает основные виды и источники уязвимостей веб-приложений, методы анализа	Знает основные виды и источники уязвимостей веб-приложений, методы анализа	Знает основные виды и источники уязвимостей веб-приложений; знает методы анализа безопасности веб-	Не знает основные виды и источники уязвимостей веб-приложений; не знает методы анализа безопасности веб-

информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	системах управления базами данных.		безопасности веб-приложений. Умеет проводить анализ безопасности веб-приложений.	безопасности веб-приложений. Умеет проводить анализ безопасности веб-приложений	приложений.	приложений. Не умеет проводить анализ безопасности веб-приложений.
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. Знает основные методы исследования компьютерных систем с целью выявления уязвимостей веб-приложений. ОР-6. Умеет проводить работы по оценке защищенности веб-приложений и составлять отчеты по результатам проведенных работ.	Знает основные методы исследования компьютерных систем с целью выявления уязвимостей веб-приложений. Проводит работы по оценке защищенности веб-приложений и составляет отчеты по результатам проведенных работ	Знает основные методы исследования компьютерных систем с целью выявления уязвимостей веб-приложений. Проводит работы по оценке защищенности веб-приложений	Знает основные методы исследования компьютерных систем с целью выявления уязвимостей веб-приложений.	Не знает основные методы исследования компьютерных систем с целью выявления уязвимостей веб-приложений.
ПК-3. Способен проектировать программно-аппаратные средства защиты информации компьютерных систем и сетей	ИПК-3.3 Проведение аттестации программ и алгоритмов на предмет соответствия требованиям защиты информации	ОР-7. Знает порядок проведения аттестации по требованиям защиты информации.	В совершенстве знает состав и содержание работ по аттестации программ и	Знает состав и содержание работ по аттестации программ и алгоритмов на	Знает порядок проведения аттестации по требованиям защиты информации	Не знает порядок проведения аттестации по требованиям защиты информации

			алгоритмов на соответствие требованиям о защите информации	соответствие требованиям о защите 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.	Архитектура веб-приложений.	ОР 1-7	Задания, вопросы к зачету
2.	Поиск уязвимостей	ОР 1-7	Задания, вопросы к зачету
3	Методы автоматизации поиска уязвимостей	ОР 1-7	Задания, вопросы к зачету

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 контрольных заданий

1. В веб-приложении, доступном по адресу https://example.com, выявить уязвимости к атакам Reflected XSS.

2. В веб-приложении, доступном по адресу https://example.com, выявить уязвимости к атакам CSRF.

Примеры задач

1. Сгенерировать цепочку сертификатов (корневой, промежуточный, клиента, сервера и т.д.). Настроить аутентификацию клиента перед веб-сервером по сертификату.

2. На защищаемом сервере установить и настроить систему обнаружения и предотвращения атак Suricata или Snort. Написать следующие правила, реализующие:

обнаружение взаимодействия зараженных браузеров с сервером BeEF обнаружение атаки Heartbleed обнаружение атаки SSRF

3. В тестовом окружении реализовать атаки SSL Strip и HTTP Injection.

4. Имеется веб-приложение, в котором защита от атак CSRF реализована методом Double Submit Cookies. Реализовать атаку, позволяющую обойти механизм защиты от атак CSRF приложения https://example.com если известно, что другие компоненты веб-приложения доступны по адресам:

https://test.example.com

https://aum.example.com

http://blog.example.com

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине

Вопросы к зачету

1. Протокол HTTP.

2. Политика и механизм Same Origin Policy.

3. Механизм сессий.

4. Механизм Cookie.

5. Механизм Content-Security Policy.

6. Протоколы SSL/TLS.

7. Атаки на протоколы SSL/TLS.

8. Тестирование защищенности конфигурации SSL/TLS.

9. Управление доступом в веб-приложениях.
10. Атаки типа «инъекция».
11. Атаки подбора паролей на веб-приложения.
12. Атаки XSS.
13. Атаки CSRF.
14. Атаки SQLI.
15. Атака ClickJacking.
16. Атаки ШОК.
17. Принципы работы сканеров уязвимостей веб-приложений.
18. Автоматизированный поиск уязвимостей.
19. Основные механизмы защиты веб-приложений.
20. Принципы работы межсетевых экранов уровня веб-приложений.