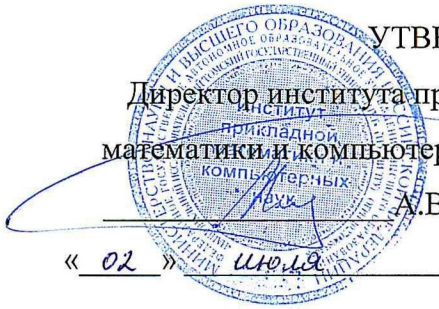
МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук



УТВЕРЖДАЮ
Директор института прикладной
математики и компьютерных наук
_____ А.В. Замятин
«_02_» _июля_ 2021 г.

Фонд оценочных средств по дисциплине

Основы построения защищённых компьютерных сетей

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	Хорошо	Удовлетворительно	Неудовлетворительно
ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты 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.	ИОПК-9.1 Учитывает современные тенденции развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных при решении задач своей профессиональной деятельности; ИОПК-9.2 Обладает знанием и демонстрирует навыки применения базовых методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных.	ОР-9.1.1 Умеет формулировать и настраивать политику безопасности основных операционных систем. ОР-9.1.2 Умеет формулировать и настраивать политику безопасности локальных компьютерных	В совершенстве умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе	Умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе	Умеет формулировать и настраивать политику безопасности основных операционных систем	Не умеет формулировать и настраивать политику безопасности основных операционных систем

ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.	ИОПК-16.1 Осуществляет оценку работоспособности применяемых средств защиты информации в компьютерных системах и сетях с использованием штатных средств и методик; ИОПК-16.2 Осуществляет оценку эффективности применяемых средств защиты информации в компьютерных системах и сетях с использованием штатных средств и методик; ИОПК-16.3 Определяет уровень защищенности и доверия средств защиты информации в компьютерных системах и сетях.	ОР-16.1.1 Владеет средствами инструментального анализа работоспособности и защищенности компьютерных сетей ОР-16.1.2 Оценивает эффективность применяемых средств защиты информации в компьютерных системах и сетях	Владеет в совершенстве средствами инструментального анализа защищенности компьютерных сетей	Уверенно владеет средствами инструментального анализа защищенности компьютерных сетей	Посредственно владеет средствами инструментального анализа защищенности компьютерных сетей	Не владеет средствами инструментального анализа защищенности компьютерных сетей
ОПК-18. Способен проводить анализ защищенности и осуществлять поиск уязвимости компьютерной системы.	ИОПК-18.1 Определяет уровень защищенности и доверия в компьютерных системах и прогнозирует возможные пути развития действий нарушителя информационной безопасности; ИОПК-18.2 Оценивает соответствие механизмов безопасности	ОР-18.1.1 Знает механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровней, защитные механизмы и средства обеспечения сетевой безопасности ОР-18.1.2 Знает средства и методы предотвращения вторжений	Владеет основными средствами анализа защищенности компьютерных сетей, средствами построения защищенных компьютерных сетей	Владеет основными средствами анализа защищенности компьютерных сетей. Умеет применять защищенные протоколы, межсетевые экраны и средства	Владеет основными средствами анализа защищенности компьютерных сетей	Не владеет основными средствами анализа защищенности компьютерных сетей, средствами построения защищенных компьютерных сетей

	компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам; ИОПК-18.3 Составляет и оформляет аналитический отчет по результатам проведенного анализа, разрабатывает предложения по устранению выявленных уязвимостей.	ОР-18.1.3 Владеет основными средствами анализа защищенности компьютерных сетей ОР-18.1.4 Умеет применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в компьютерных сетях	Умеет применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в компьютерных сетях.	обнаружения вторжений для защиты информации в компьютерных сетях.		

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.	Защита от атак канального уровня	ОР-16.1.1, ОР-16.1.2, ОР-18.1.1 – 18.1.4	Вопросы, задания лаб. работы
2.	Защита коммутации	ОР-16.1.1, ОР-16.1.2, ОР-18.1.1 – 18.1.4	Вопросы, задания лаб. работы
	Технология VPN	ОР-9.1.1, ОР-9.1.2 ОР-16.1.1, ОР-16.1.2,	Вопросы, задания лаб. работы
	Защита от атак DoS н DDoS	ОР-16.1.1, ОР-16.1.2, ОР-18.1.1 – 18.1.4	Вопросы, задания лаб. работы
	Защита маршрутизации	ОР-16.1.1, ОР-16.1.2,	Вопросы, задания лаб. работы
	Защита транспортного уровня	ОР-18.1.1 – 18.1.4	Вопросы, задания лаб. работы
	Защита сетевых устройств	ОР-16.1.1, ОР-16.1.2, ОР-18.1.1 – 18.1.4	Вопросы, задания лаб. работы
	Технологии межсетевого экранирования	ОР-9.1.1, ОР-9.1.2	Вопросы, задания лаб. работы
	Методы н технологии обнаружения вторжений	ОР-9.1.1, ОР-9.1.2	Вопросы, задания лаб. работы
	Сканирование защищенности сетей	ОР-16.1.1, ОР-16.1.2, ОР-18.1.1 – 18.1.4	Вопросы, задания лаб. работы
	Дизайн защищенных сетей	ОР-9.1.1, ОР-9.1.2	Вопросы, задания лаб. работы

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. Проанализировать конфигурационный файл. Перечислить все недостатки и уязвимости конфигурации маршрутизатора.

2. Проанализировать конфигурационный файл и перечислить все способы получения конфигурации с устройства, настроенного в соответствии с этим файлом.

3. Для заданной атаки написать правило для IDS Suricata.

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;
- обнаружение вредоносного узла сети;

- обнаружения эксплоита PHPMailer;
- обнаружения эксплоита bnageTragic;
- обнаружения эксплоита DROWN;
- обнаружение атаки LDAP Injection.

3. В тестовом окружении реализовать атаку ARP Spoofing.
4. В тестовом окружении реализовать атаку MAC Flooding.
5. В тестовом окружении реализовать атаку HeartBleed.
6. В тестовом окружении реализовать атаку подбора паролей для SSH.
7. Настроить механизмы защиты от НСД маршрутизатора.
8. Настроить механизмы защиты от НСД коммутатора.
9. Обнаружить вредоносную активность по дапму сетевой активности.

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине

Вопросы к зачету:

1. Атаки на STP.
2. Методы и технологии защиты от атак канального уровня.
3. Протоколы GRE и IPSec.
4. Технология SYN Cookie и SYN Proxy.
5. Методы защиты от IP Spoofing.
6. Методы защиты протоколов маршрутизации.
7. Протоколы SSL/TLS.
8. Защищенная настройка TLS.
9. Защищенная настройка маршрутизаторов и коммутаторов.
10. Технологии NAT, statefiil inspection, stateless inspection.
11. Методы обнаружения вторжений в сетях.
12. Атаки MAC Flooding, MAC Spoofing, VLAN Hopping, ARP Spoofing.