Приложение А
(обязательное к рабочей программе дисциплины)

Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Безопасность сетей ЭВМ»

Уровень образования: специалитет
(бакалавриат/магистратура/специалитет)

Специальность: 10.05.03 «Информационная безопасность автоматизированных систем»
(код, наименование направления подготовки/специальности)

Специализация: «Безопасность открытых информационных систем»
(наименование)

Разработчик _____ Фейлмазова С.А_б/с
подпись (ФИО уч. степень, уч. звание)

Фонд оценочных средств обсужден на заседании кафедры ИБ
«20» 09 2021 г., **протокол №** 2

Зав. кафедрой ИБ _____ Качаева Г.И., к.э.н.

г. Махачкала 2021 г.

СОДЕРЖАНИЕ

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины «Безопасность сетей ЭВМ» и предназначен для контроля и оценки образовательных достижений обучающихся (в т.ч. по самостоятельной работе студентов, далее – СРС), освоивших программу данной дисциплины.

Целью фонда оценочных средств является установление соответствия уровня подготовки обучающихся требованиям ФГОС ВО по направлению подготовки/специальности *(указывается код и наименование направления подготовки/специальности).*

Рабочей программой дисциплины «Безопасность сетей ЭВМ» предусмотрено формирование следующих компетенций:

ОПК-9-Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации.

2. Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля)

2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП

Таблица 1

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	Критерии оценивания	Наименование контролируемых разделов и тем[1]
ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.2.1.Знает основную эксплуатационную и проектную документацию на информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, обеспечивающие функционирование топливно-энергетического комплекса	- Знает основную эксплуатационную и проектную документацию телекоммуникационные сети на **удовлетворительно.** -Знает основную эксплуатационную и проектную документацию телекоммуникационные сети на хорошо - Знает основную эксплуатационную и проектную документацию телекоммуникационные сети на **отлично**.	Тема 1: Введение в сетевую безопасность. Тема 2: Аудит информационной безопасности. Тема 3: Протоколы сетевой аутентификации. Модели разграничения доступа. Вредоносное программное обеспечение. Тема 4: Системы предотвращения утечек информации. Системы анализа трафика. Файрвол веб-приложений. Тема 5: Системы обнаружения и предотвращения вторжений (ISD/IPS) Тема 6: Угрозы безопасности на канальном уровне 2. Тема 7: Настройка параметров безопасности коммутатора cisco. Тема 8: Обеспечение безопасности сетевых устройств. Тема 9:Межсетевые экраны.

[1] *Наименования разделов и тем должен соответствовать рабочей программе дисциплины.*

	ОПК-10.2. умеет проводить анализ угроз безопасности в локальных вычислительных сетях	- умеет проводить анализ угроз безопасности в локальных вычислительных сетях на **удовлетворительн** -умеет проводить анализ угроз безопасности в локальных вычислительных сетях на **хорошо**. - умеет проводить анализ угроз безопасности в локальных вычислительных сетях на **отлично**.	Тема 12: Уязвимости по приложениям Тема 10: Дополнительные возможности Wireshark для графического представления получаемых результатов. Тема11: Методы сбора информации. Тема 12: Уязвимости по приложениям Тема 13: Атака на сервер компьютерной сети Тема 14: Способы обхода авторизации
	ОПК-10.3.1.3знает основные системы и способы тестирования на проникновение	- 3знает основные системы и способы тестирования на проникновение на **удовлетворительно**. - 3знает основные системы и способы тестирования на проникновение на **хорошо**. - 3знает основные системы и способы тестирования на проникновение на **отлично**.	Тема 15,16: Sql инъекции Тема 17: Защита от SQL-инъекций Тема 18: Алгоритмы взлома корпоративной сети. Тема 19: Анализ защищённости веб-приложений Тема 20: Инструменты Kali Linux. Тема 21: Методы сканирования и уклонения в Kali Linux.
ОПК-12. Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем.	ОПК-12.1.2. знает принципы построения и функционирования локальных и глобальных вычислительных сетей	-знать принципы построения и функционирования локальных и глобальных вычислительных сетей на удовлетворительно - знать принципы построения и функционирования локальных и глобальных вычислительных сетей на хорошо. - знать принципы построения и функционирования локальных и глобальных вычислительных сетей на отлично.	Тема 22: Инструментальные средства командной строки для анализа пакетов Тема 23: Процесс выявления и анализа критических недостатков безопасности в Kali Linux. Тема 23: Процесс выявления и анализа критических недостатков безопасности в Kali Linux.

ОПК-15..Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.1.3знает программные средства, позволяющие вести автоматизированный аудит	-3знает программные средства, позволяющие вести автоматизированный аудит на удовлетворительно. -3знает программные средства, позволяющие вести автоматизированный аудит на хорошо. -3знает программные средства, позволяющие вести автоматизированный аудит на отлично.	Тема 24: Python для тестирования на проникновение. Тема 25: Исследование сетей с Python. Тема 26: Безопасность беспроводных сетей.

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине «Безопасность сетей ЭВМ» определяется на следующих этапах:
1. **Этап текущих аттестаций** *(Для проведения текущих аттестаций могут быть использованы оценочные средства, указанные в разделе 2)*
2. **Этап промежуточных аттестаций** (*Для проведения промежуточной аттестации могут быть использованы другие оценочные средства*)

Таблица 2

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	**Этапы формирования компетенции (5сем, 6 сем)**					
		Этап текущих аттестаций					**Этап промежуточной аттестации**
		1-5 неделя	**6-10 неделя**	**11-15 неделя**	**1-17 неделя**		**18-20 неделя**
		Текущая аттестация №1	Текущая аттестация №2	Текущая аттестация №3	СРС	КР/КП	Промежуточная аттестация
1		**2**	**3**	**4**	**5**	**6**	**7**
ОПК-10	ОПК-10.2.Умеет проводить анализ угроз безопасности в локальных вычислительных сетях	*Контрольная работа*	*Контрольная работа*	*Контрольная работа*			
	ОПК-10.2.1.3нает основную эксплуатационную и проектную документацию на информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, обеспечивающие функционирование топливно-энергетического комплекса.	*Контрольная работа*	*Контрольная работа*	*Контрольная работа*		нет	*вопросы для проведения экзамена*
	ОПК-10.3.1.3знает основные системы и способы тестирования на проникновение	*Контрольная работа*	*Контрольная работа*	*Контрольная работа*	-		
ОПК-12.	Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем.	*Контрольная работа*	*Контрольная работа*	*Контрольная работа*			

СРС – самостоятельная работа студентов;
КР – курсовая работа;
КП – курсовой проект.

2.2. Показатели уровней сформированности компетенций на этапах их формирования, описание шкал оценивания

2.2.1. Показатели уровней сформированности компетенций на этапах их формирования

Результатом освоения дисциплины «Безопасность сетей ЭВМ» является установление одного из уровней сформированности компетенций: высокий, повышенный, базовый, низкий.

Таблица 3

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
Высокий (оценка «отлично», «зачтено»)	Сформированы четкие системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные и верные. Даны развернутые ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции	Обучающимся усвоена взаимосвязь основных понятий дисциплины, в том числе для решения профессиональных задач. Ответы на вопросы оценочных средств самостоятельны, исчерпывающие, содержание вопроса/задания оценочного средства раскрыто полно, профессионально, грамотно. Даны ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции
Повышенный (оценка «хорошо», «зачтено»)	Знания и представления по дисциплине сформированы на повышенном уровне. В ответах на вопросы/задания оценочных средств изложено понимание вопроса, дано достаточно подробное описание ответа, приведены и раскрыты в тезисной форме основные понятия. Ответ отражает полное знание материала, а также наличие, с незначительными пробелами, умений и навыков по изучаемой дисциплине. Допустимы единичные негрубые ошибки. Обучающимся продемонстрирован повышенный уровень освоения компетенции	Сформированы в целом системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные, грамотные. Продемонстрирован повышенный уровень владения практическими умениями и навыками. Допустимы единичные негрубые ошибки по ходу ответа, в применении умений и навыков.
Базовый (оценка «удовлетворительно», «зачтено»)	Ответ отражает теоретические знания основного материала дисциплины в объеме, необходимом для дальнейшего освоения ОПОП. Обучающийся допускает неточности в ответе, но обладает необходимыми знаниями для их устранения. Обучающимся продемонстрирован базовый уровень освоения компетенции	Обучающийся владеет знаниями основного материал на базовом уровне. Ответы на вопросы оценочных средств неполные, допущены существенные ошибки. Продемонстрирован базовый уровень владения практическими умениями и навыками, соответствующий минимально необходимому уровню для решения профессиональных задач
Низкий (оценка	Демонстрирует полное отсутствие теоретических знаний материала дисциплины, отсутствие практических умений и навыков	

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
«не зачтено»)		

Показатели уровней сформированности компетенций могут быть изменены, дополнены и адаптированы к конкретной рабочей программе дисциплины.

2.2.2. Описание шкал оценивания

В ФГБОУ ВО «ДГТУ» внедрена модульно-рейтинговая система оценки учебной деятельности студентов. В соответствии с этой системой применяются пятибальная, двадцатибальная и стобальная шкалы знаний, умений, навыков.

Шкалы оценивания			Критерии оценивания
пятибальная	двадцатибальная	стобальная	
«Отлично» - 5 баллов	«Отлично» - 18-20 баллов	«Отлично» - 85 – 100 баллов	Показывает высокий уровень сформированности компетенций, т.е.: – продемонстрирует глубокое и прочное усвоение материала; – исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал; – правильно формирует определения; – демонстрирует умения самостоятельной работы с нормативно-правовой литературой; – умеет делать выводы по излагаемому материалу.
«Хорошо» - 4 баллов	«Хорошо» - 15 - 17 баллов	«Хорошо» - 70 - 84 баллов	Показывает достаточный уровень сформированности компетенций, т.е.: – демонстрирует достаточно полное знание материала, основных теоретических положений; – достаточно последовательно, грамотно логически стройно излагает материал; – демонстрирует умения ориентироваться в нормальной литературе; – умеет делать достаточно обоснованные выводы по излагаемому материалу.
«Удовлетворительно» - 3 баллов	«Удовлетворительно» - 12 - 14 баллов	«Удовлетворительно» - 56 – 69 баллов	Показывает пороговый уровень сформированности компетенций, т.е.: – демонстрирует общее знание изучаемого материала; – испытывает серьезные затруднения при ответах на дополнительные вопросы; – знает основную рекомендуемую литературу; – умеет строить ответ в соответствии со структурой излагаемого материала.
«Неудовлетворительно» - 2 баллов	«Неудовлетворительно» - 1-11 баллов	«Неудовлетворительно» - 1-55 баллов	Ставится в случае: – незнания значительной части программного материала; – не владения понятийным аппаратом дисциплины; – допущения существенных ошибок при изложении учебного материала; – неумение строить ответ в соответствии со структурой излагаемого вопроса; – неумение делать выводы по излагаемому материалу.

3. Типовые контрольные задания, иные материалы и методические рекомендации, необходимые для оценки сформированности компетенций в процессе освоения ОПОП

Задания и вопросы для входного контроля

1. Какие угрозы безопасности сетей вы знаете?
2. Что такое прокси-серверы?
3. Какие системы выявления и предотвращения угроз взлома вы знаете*
4. Какие системы сетевого мониторинга вы знаете?
5. Как обеспечивается безопасность передачи данных по сетям.

3.2. Оценочные средства и критерии сформированности компетенций

Комплект заданий для контрольной работы №1 для первой аттестации (5сем.)

Время выполнения __90_ мин.
• Количество вариантов контрольной работы - _2__.
• Количество заданий в каждом варианте контрольной работы - _3__.
• Форма работы – самостоятельная, индивидуальная.

Вариант 1

Задание1. Основные понятия безопасности сетей
Задание 2. Основные виды аудита безопасности
Задание 3. Протоколы аутенитфикации

Вариант 2

Задание 1. Типы атак.
Задание 2. Основные функции канального уровня.
Задание 3. Инструментальный анализ защищенности.

Комплект заданий для контрольной работы №2 для второй аттестации (5сем.)

Время выполнения __90_ мин.
• Количество вариантов контрольной работы - _2__.
• Количество заданий в каждом варианте контрольной работы - _3__.
• Форма работы – самостоятельная, индивидуальная.

Вариант 1

Задание 1. DMZ –системы
Задание 2. Что такое системы обнаружения вторжений (IDS).
Задание 3. Сетевые ISD (NIDS)

Вариант 2

Задание 1. DPI- системы
Задание 2. WAF-системы.
Задание 3. Протоколы сетевой аутентификации

Комплект заданий для контрольной работы №3 для второй аттестации (5сем.)

Время выполнения __90_ мин.
• Количество вариантов контрольной работы - _2__.
• Количество заданий в каждом варианте контрольной работы - 3__.
• Форма работы – самостоятельная, индивидуальная.

Вариант 1

Задание 1. Атака на таблицу MAC.
Задание 2. Атаки на сети VLAN.
Задание 3. Атаки, связанные с DHCP.

Вариант 2

Задание 1. ARP атаки.
Задание 2. Атаки с подменой адреса.
Задание 3. Атаки, связанные с DHCP.

Комплект заданий для контрольной работы №1 для первой аттестации (6сем.)

Время выполнения __90_ мин.

• Количество вариантов контрольной работы - _5__.
• Количество заданий в каждом варианте контрольной работы - _4__.
• Форма работы – самостоятельная, индивидуальная.

Вариант 1

Задание 1. Защита не используемых портов.
Задание 2. Нейтрализация атак таблицы MAC-адресов.
Задание 3. Ограничение и изучение MAC-адресов.
Задание 4. Режимы нарушения безопасности порта.

Вариант 2

Задание 1. Защита доступа к устройствам.
Задание 2. Назначение административных ролей.
Задание 3. Простой протокол сетевого управления SNMP.
Задание 4. Определение типов межсетевых экранов.

Вариант 3

Задание 1. Разработка конфигурации межсетевого экрана.
Задание 2.Построение набора правил межсетевого экрана.
Задание 3. Выявление различий между межсетевыми экранами различных типов
Задание 4. Конечные точки и сетевые диалоги.

Вариант 4

Задание 1. Выявление наиболее активных сетевых узлов с помощью конечных точек и диалогов
Задание 2. Общедоступные сайты, которые можно использовать для сбора информации о целевом домене.
Задание 3. Информация о регистрации домена.
Задание 4. Анализ DNS.

Вариант 5

Задание1. SSTI.
Задание 2. XXE-атака.
Задание 3. XSS-атаки.
Задание 4. Снижение риска атак межсайтового скриптинга (XSS) с помощью helmet.xssFilter.

Комплект заданий для контрольной работы №2 для второй аттестации (6сем.)

Время выполнения __90_ мин.

• Количество вариантов контрольной работы - _5__.
• Количество заданий в каждом варианте контрольной работы - _4__.
• Форма работы – самостоятельная, индивидуальная.

Вариант 1

Задание 1 BruteForce.
Задание 2. Тестирование на проникновение с помощью Burp
Задание 3. SQL инъекции.
Задание 4. Cookie.

Вариант 2

Задание 1. Принцип атаки внедрения SQL.
Задание 2. Типы SQLi.
Задание 3. Защита от SQLi.
Задание 4. Union injection.

Вариант 3

Задание 1. Интерфейс виртуальных туннелей IPsec.
Задание 2. Преимущества и недостатки NAT.
Задание 3. Варианты подключения к Интернет-провайдеру

Вариант 4

Задание 1. Функция mysql(i)_real_escape_string
Задание 2. Использование анализатора sqlmap.
Задание 3. Захват учетных записей
Задание 4. Атака протокола отладки Java Debug Wire Protocol

Вариант 5

Задание 1. Веб-уязвимости
Задание 2. Социальная инженерия.
Задание 3. Методология тестирования на проникновение: Метод черного ящика (black box), Метод белого ящика (white box), Метод серого ящика (gray box)
Задание 4. Анализ защищённости веб-приложений путём внешних проверок (автоматизированных и ручных).

№3 для третьей аттестации (6 сем.)

Время выполнения __90_ мин.

- Количество вариантов контрольной работы - _3__.
- Количество заданий в каждом варианте контрольной работы - _4__.
- Форма работы – самостоятельная, индивидуальная.

Вариант 1

Задание 1. Разведка сайтов. Поиск каталогов и файлов. Dirb, Dirhunt, DirBuster.
Задание 2. dirsearch —инструмент командной строки, предназначенный для брут-форса (поиска путём полного перебора) директорий и файлов в веб-сайтах.
Задание 3. DVCS-Ripper
Задание 4. SQLmap

Вариант 2

Задание 1. Автоматическое сканирование с помощью Striker.
Задание 2. Сокрытие с помощью Nipe.
Задание 3. Понимание сокетов и создание TCP-сервера
Задание 4 Создание TCP-клиента
Задание 4Разработка сканера Nmap

Вариант 3

Задание 1. WEP-атаки на конфиденциальность проводных сетей
Задание 2. Протоколы WPA и AES
Задание 3. Заблуждения о безопасности беспроводной сети
Задание 4. Беспроводные атаки и защита от них

Критерии оценки уровня сформированности компетенций при проведении контрольной работы:

- оценка «отлично»: продемонстрировано грамотное последовательное решение задач (заданий) пр правильно выбранном алгоритме. Даны верные ответы на все вопросы и условия задач (заданий). При необходимост сделаны пояснения и выводы (содержательные, достаточно полные, правильные, учитывающие специфи проблемной ситуации в задаче или с незначительными ошибками);

- оценка «хорошо»: грамотное последовательное решение задач (заданий) при правильно выбранно алгоритме. Однако, ответы на вопросы и условия задач (заданий) содержат незначительные ошибки. Пояснения выводы отсутствуют или даны неверно;

- оценка «удовлетворительно»: обучающийся ориентируется в материале, но применяет его неверно, выбира неправильный алгоритм решения задач (неверные исходные данные, неверная последовательность решения и д ошибки), допускает вычислительные ошибки. Пояснения и выводы отсутствуют или даны неверно;

- оценка «неудовлетворительно»: обучающийся слабо ориентируется в материале, выбирает неправильны алгоритм решения, допускает значительное количество вычислительных ошибок. Пояснения и выводы отсутствую

3.3. Задания для промежуточной аттестации (зачета и (или) экзамена)

Список вопросов к зачету (5сем)

Комплект заданий для контрольной работы №1 для первой аттестации (5сем.)

1. Основные понятия безопасности сетей
2. Основные виды аудита безопасности
3. Протоколы аутенитфикации
4. Типы атак.
5. Инструментальный анализ защищенности.
6. DMZ –системы
7. Что такое системы обнаружения вторжений (IDS).
8. Сетевые ISD (NIDS)
9. DPI- системы
10. WAF-системы.
11. Протоколы сетевой аутентификации
12. Атака на таблицу MAC.