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 вычислительных сетей»

Уровень образования: бакалавриат
(бакалавриат/магистратура/специалитет)

Направление: 10.03.01 Информационная безопасность
(код, наименование направления подготовки/специальности)

Профиль: «Безопасность автоматизированных систем»
(наименование)

Разработчик _____ Мирземагомедова М.М.,к.т.н., доцент
подпись (ФИО уч. степень, уч. звание)

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

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

г. Махачкала 2021 г.

Оглавление

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины «Безопасность вычислительных сетей
» 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:

ПК-1 Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.

ПК-2 Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач

ПК-3 Способность администрировать подсистемы информационной безопасности объекта защиты

ПК-4 Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

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]
ПК-1 Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1.1. Знает порядок установки, настройки и обслуживания программного обеспечения, систем управления базами данных, средств электронного документооборота и средств защиты информации. ПК-1.2. Владеет навыками по установке, настройке и обслуживанию программного обеспечения, программно-аппаратных и технических средств защиты информации с соблюдением требований по защите информации. ПК-1.3. Умеет устанавливать программное обеспечение в соответствии с технической документацией, выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота, формулировать правила безопасной эксплуатации	- знает порядок установки, настройки и обслуживания программного обеспечения, систем управления базами данных, средств электронного документооборота и средств защиты информации на **удовлетворительно.** - знает порядок установки, настройки и обслуживания программного обеспечения, систем управления базами данных, средств электронного документооборота и средств защиты информации на **хорошо.** - знает порядок установки, настройки и обслуживания программного обеспечения, систем управления базами данных, средств электронного документооборота и средств защиты информации на **отлично**.	Лекция №1. Введение в сетевую безопасность Лекция №2 Аудит информационной безопасности Лекция №3 Протоколы сетевой аутентификации. Модели разграничения доступа. Вредоносное программное обеспечение. Лекция №4 Системы предотвращения утечек информации. Системы анализа трафика. Файрвол веб-приложений Лекция №5 Системы обнаружения и предотвращения вторжений (ISD/IPS) Лекция №6 Угрозы безопасности на канальном уровне 2

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

ПК-2 Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	ПК-2.1. Знать архитектуру и принципы построения операционных систем, подсистем защиты информации, состав типовых конфигураций программно-аппаратных средств защиты информации, языки и системы программирования. ПК-2.2. Умеет противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации. ПК-2.3. Владеет контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах	- знает архитектуру и принципы построения операционных систем, подсистем защиты информации, состав типовых конфигураций программно-аппаратных средств защиты информации, языки и системы программирования на **удовлетворительно.** - архитектуру и принципы построения операционных систем, подсистем защиты информации, состав типовых конфигураций программно-аппаратных средств защиты информации, языки и системы программирования на **хорошо.** - архитектуру и принципы построения операционных систем, подсистем защиты информации, состав типовых конфигураций программно-аппаратных средств защиты информации, языки и системы программирования на **отлично**.	Лекция № 7 Настройка параметров безопасности коммутатора cisco. Лекция №8 Обеспечение безопасности сетевых устройств Лекции №9 Межсетевые экраны Лекция 10 Дополнительные возможности Wireshark для графического представления получаемых результатов. Лекция №11 Методы сбора информации. Лекция № 12: Уязвимости по приложениям
ПК-3 Способность администрировать подсистемы информационной безопасности объекта защиты	ПК-3.1 Знает требования к встроенным средствам защиты информации программного обеспечения ПК-3.2 Умеет анализировать угрозы безопасности информации программного обеспечения, формулировать и обосновывать правила безопасной эксплуатации программного обеспечения, производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации ПК-3.3 Владеет навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования	- знает требования к встроенным средствам защиты информации программного обеспечения на **удовлетворительно.** - знает требования к встроенным средствам защиты информации программного обеспечения на **хорошо.** - знает требования к встроенным средствам защиты информации программного обеспечения на **отлично**.	Лекция №13: Атака на сервер компьютерной сети Лекция №14: Способы обхода авторизации Лекция №15: Sql инъекции Лекция №16 Sql инъекции Лекция №17: Защита от SQL-инъекций Лекция №18 Алгоритмы взлома корпоративной сети Лекция № 19: Анализ защищённости веб-приложений

ПК-4 Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	ПК-4.1 Знает виды политик безопасности и их формирование, разработка профилей защиты и заданий по безопасности, решения о необходимости защиты информации, содержащейся в информационной системе ПК-4.2 Умеет формировать политики безопасности, анализировать систему с целью определения необходимого уровня защищенности и доверия ПК-4.3 Владеет навыками разработки руководящих документов по защите информации в организации	- знает виды политик безопасности и их формирование, разработка профилей защиты и заданий по безопасности, решения о необходимости защиты информации, содержащейся в информационной системе на **удовлетворительно.** - знает виды политик безопасности и их формирование, разработка профилей защиты и заданий по безопасности, решения о необходимости защиты информации, содержащейся в информационной системе на **хорошо.** - знает виды политик безопасности и их формирование, разработка профилей защиты и заданий по безопасности, решения о необходимости защиты информации, содержащейся в информационной системе на **отлично**.	Лекция № 20: Инструменты Kali Linux. Лекция № 21: Методы сканирования и уклонения в Kali Linux Лекция № 22: Инструментальные средства командной строки для анализа пакетов Лекция № 23: Процесс выявления и анализа критических недостатков безопасности в Kali Linux Лекция № 24: Python для тестирования на проникновение Лекция № 25: Исследование сетей с Python Лекция № 26: Безопасность беспроводных сетей

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине «Безопасность вычислительных сетей» 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 (6сем, 7 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**
ПК1 Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1.1. Знает порядок установки, настройки и обслуживания программного обеспечения, систем управления базами данных, средств электронного документооборота и средств защиты информации.	*Контрольная работа*	*Контрольная работа*	*Контрольная работа*		нет	*вопросы для проведения экзамена*
	ПК-1.2. Владеет навыками по установке, настройке и обслуживанию программного обеспечения, программно-аппаратных и технических средств защиты информации с соблюдением требований по защите информации. ПК-1.3. Умеет устанавливать программное обеспечение в соответствии с технической документацией, выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота, формулировать правила безопасной эксплуатации						
ПК-2 Способность применять программные средства системного, прикладного и специального назна-	ПК-2.1. Знать архитектуру и принципы построения операционных систем, подсистем защиты информации, состав типовых конфигураций программно-аппаратных средств защиты информации, языки и системы программирования. ПК-2.2. Умеет противодействовать угрозам безопасности	*Контрольная работа*	*Контрольная работа*	*Контрольная работа*			*вопросы для проведения экзамена*

чения, инструментальные средства, языки и системы программирования для решения профессиональных задач	информации с использованием встроенных средств защиты информации. ПК-2.3. Владеет контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах						
ПК-3 Способность администрировать подсистемы информационной безопасности объекта защиты	ПК-3.1 Знает требования к встроенным средствам защиты информации программного обеспечения ПК-3.2 Умеет анализировать угрозы безопасности информации программного обеспечения, формулировать и обосновывать правила безопасной эксплуатации программного обеспечения, производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации ПК-3.3 Владеет навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования	*Контрольная работа*	*Контрольная работа*	*Контрольная работа*			*вопросы для проведения экзамена*
ПК-4 Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	ПК-4.1 Знает виды политик безопасности и их формирование, разработка профилей защиты и заданий по безопасности, решения о необходимости защиты информации, содержащейся в информационной системе ПК-4.2 Умеет формировать политики безопасности, анализировать систему с целью определения необходимого уровня защищенности и доверия ПК-4.3 Владеет навыками разработки руководящих документов по защите информации в организации	*Контрольная работа*	*Контрольная работа*	*Контрольная работа*			*вопросы для проведения экзамена*

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 вычисслительных сетей» 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

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
Низкий (оценка «неудовлетворительно», «не зачтено»)	Демонстрирует полное отсутствие теоретических знаний материала дисциплины, отсутствие практических умений и навыков	

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

3.1. 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 контрольно3 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) при правильно выбранном алгоритме. Даны верные ответы на все вопросы и условия задач (заданий). При необходимости сделаны пояснения и выводы (содержательные, достаточно полные, правильные, учитывающие специфику проблемной ситуации в задаче или с незначительными ошибками);

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

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

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

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

Список вопросов к зачету (6сем)

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.
13. Атаки на сети VLAN.
14. ARP атаки.
15. Атаки с подменой адреса.

Список вопросов к экзамену (7 семестр)

1. Защита не используемых портов.
2. Нейтрализация атак таблицы MAC-адресов.
3. Ограничение и изучение MAC-адресов.
4. Режимы нарушения безопасности порта.
5. Защита доступа к устройствам.
6. Назначение административных ролей.
7. Простой протокол сетевого управления SNMP.
8. Определение типов межсетевых экранов.
9. Разработка конфигурации межсетевого экрана.
10. Построение набора правил межсетевого экрана.
11. .Выявление различий между межсетевыми экранами различных типов
12. Конечные точки и сетевые диалоги.
13. Выявление наиболее активных сетевых узлов с помощью конечных точек и диалогов
14. Общедоступные сайты, которые можно использовать для сбора информации о целевом домене.
15. Анализ DNS.
16. XXE-атака.
17. XSS-атаки.
18. Снижение риска атак межсайтового скриптинга (XSS) с помощью helmet.xssFilter.
19. BruteForce.
20. Тестирование на проникновение с помощью Burp
21. SQL инъекции.
22. Cookie.
23. Типы SQLi.
24. Защита от SQLi.
25. Union injection.
26. Интерфейс виртуальных туннелей IPsec.
27. Преимущества и недостатки NAT.
28. Варианты подключения к Интернет-провайдеру
29. Функция mysql(i)_real_escape_string
30. Использование анализатора sqlmap.
31. .Захват учетных записей
32. Атака протокола отладки Java Debug Wire Protocol
33. Веб-уязвимости
34. Социальная инженерия.
35. Методология тестирования на проникновение: Метод черного ящика (black box), Метод белого ящика (white box), Метод серого ящика (gray box)
36. Анализ защищённости веб-приложений путём внешних проверок (автоматизированных и ручных).
37. Разведка сайтов. Поиск каталогов и файлов. Dirb, Dirhunt, DirBuster.
38. dirsearch —инструмент командной строки, предназначенный для брут-форса (поиска путём полного перебора) директорий и файлов в веб-сайтах.
39. DVCS-Ripper
40. SQLmap
41. Автоматическое сканирование с помощью Striker.
42. Сокрытие с помощью Nipe.
43. Понимание сокетов и создание TCP-сервера
44. Создание TCP-клиента
45. Разработка сканера Nmap
46. WEP-атаки на конфиденциальность проводных сетей
47. Протоколы WPA и AES

48. Заблуждения о безопасности беспроводной сети
49. Беспроводные атаки и защита от них

Экзамены могут быть проведены в письменной форме, а также в письменной форме с устным дополнением ответа.

Экзамен по дисциплине (модулю) служит для оценки работы студента в течении семестра (года, всего срока обучения и др.) и призван выявить уровень, качество и систематичность полученных им теоретических и практических знаний, приобретения навыков самостоятельной работы, развития творческого мышления, умения синтезировать полученные знания и применять их в решении практических задач. По итогам экзамена, в соответствии с модульно – рейтинговой системой университета выставляются баллы, с последующим переходом по шкале оценок на оценки: «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно», свидетельствующие о приобретенных компетенциях или их отсутствии.

Форма экзаменационного билета (пример оформления)

Министерство науки и высшего образования РФ

ФГБОУ ВО "Дагестанский государственный технический университет"

Дисциплина (модуль) «**Безопасность вычислительных сетей**»
Код специальности 10.05.03 «Информационная безопасность автоматизированных систем»
Специальность **Безопасность открытых информационных систем**
Кафедра __ИБ_____ Курс _4___Семестр __7___
Форма обучения – очная, очно-заочная

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №__1___.

1. Атака протокола отладки Java Debug Wire Protocol
2. Веб-уязвимости

Экзаменатор.....Мирземагомедова М.М..

Утвержден на заседании кафедры (протокол №___ от _____20___ г.)

Зав. кафедрой (название) ИБ.....Г.И. Качаева

Критерии оценки уровня сформированности компетенций по результатам проведения зачета:

- оценка «зачтено»: обучающийся демонстрирует всестороннее, систематическое и глубокое знание материала, свободно выполняет задания, предусмотренные программой дисциплины, усвоивший основную и дополнительную литературу. Обучающийся выполняет задания, предусмотренные программой дисциплины, на уровне не ниже базового;

- оценка «не зачтено»: обучающийся демонстрирует незнание материала, не выполняет задания, предусмотренные программой дисциплины. Обучающийся не выполняет задания, предусмотренные программой дисциплины, на уровне ниже базового. Дальнейшее освоение ОПОП не возможно без дополнительного изучения материала и подготовки к зачету.

Критерии оценки уровня сформированности компетенций по результатам проведения дифференцированного зачёта (зачета с оценкой) / экзамена:

-оценка «отлично»: обучающийся дал полный, развернутый ответ на поставленный вопрос, проявил со-

вокупность осознанных знаний об объекте, доказательно раскрыл основные положения темы. В ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, явлений. Обучающийся подкрепляет теоретический ответ практическими примерами. Ответ сформулирован научным языком, обоснована авторская позиция обучающегося. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа или с помощью «наводящих» вопросов преподавателя. Обучающимся продемонстрирован высокий уровень владения компетенцией(-ями);

-оценка «хорошо»: обучающимся дан полный, развернутый ответ на поставленный вопрос, проявлено умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, но есть недочеты в формулировании понятий, решении задач. При ответах на дополнительные вопросы допущены незначительные ошибки. Обучающимся продемонстрирован повышенный уровень владения компетенцией(-ями);

-оценка «удовлетворительно»: обучающимся дан неполный ответ на вопрос, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, явлений, нарушена логика ответа, не сделаны выводы. Речевое оформление требует коррекции. Обучающийся испытывает затруднение при ответе на дополнительные вопросы. Обучающимся продемонстрирован базовый уровень владения компетенцией(-ями);

-оценки «неудовлетворительно»: обучающийся испытывает значительные трудности в ответе на вопрос, допускает существенные ошибки, не владеет терминологией, не знает основных понятий, не может ответить на «наводящие» вопросы преподавателя. Обучающимся продемонстрирован низкий уровень владения компетенцией(-ями).