МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. декана факультета математики
и компьютерных наук имени
профессора Н.И. Червякова
Т.А. Гробова
Ф.И.О.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Анализ защищенности киберфизических систем
название дисциплины (модуля)

Направление подготовки	10.04.01 «Информационная безопасность»
Направленность (профиль)	Информационная безопасность киберфизических систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	3

Введение

1. Назначение: проведение текущего контроля успеваемости и промежуточной аттестации по дисциплине «Анализ защищенности киберфизических систем».

2. ФОС является приложением к программе дисциплины «Анализ защищенности киберфизических систем» в соответствии с образовательной программой по направлению подготовки 10.04.01 Информационная безопасность (профиль «Информационная безопасность киберфизических систем») по дисциплине «Анализ защищенности киберфизических систем»

3. Разработчик Орёл Д.В., доцент кафедры

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель: Петренко В. И., заведующий кафедрой

Члены экспертной группы: Минкина Т. В., доцент кафедры

Рачков В. Е., доцент кафедры

Представитель организации-работодателя Демурчев Н.Г., директор ООО «СГУ-Инфоком»

Экспертное заключение: фонд оценочных средств соответствует ОП ВО по направлению подготовки 10.04.01 Информационная безопасность (профиль «Информационная безопасность киберфизических систем») и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Анализ защищенности киберфизических систем».

5. Срок действия ФОС: определяется сроком реализации образовательной программы.

1. Описание критериев оценивания компетенции на различных этапах их формирования, описание шкал оценивания

Компетенция (ии), индикатор (ы)	Уровни сформированности компетенции(й),			
	Минимальный уровень не достигнут (неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
Компетенция: ПК-1 Способен проводить исследования и анализ информационных процессов защиты информации в киберфизических системах				
ПК-1 ИД-1 технологии поиска, изучения, обобщения, классификации и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах	на низком уровне: применяет технологии поиска, изучения, обобщения, классификации и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах	в основном: применяет технологии поиска, изучения, обобщения, классификации и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах	умеет: применять технологии поиска, изучения, обобщения, классификации и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах	на высоком профессиональном уровне: применяет технологии поиска, изучения, обобщения, классификации и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах
ПК-1 ИД-2 применение современных информационных технологий и программных средств, при решении задач профессиональной деятельности	на низком уровне: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	в основном: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	владеет: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	на высоком профессиональном уровне: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности
ПК-1 ИД-4 применяет технологии исследования и анализа информационных процессов защиты информации в киберфизических системах	на низком уровне: применяет технологии исследования и анализа информационных процессов защиты информации в киберфизических системах	в основном: применяет технологии исследования и анализа информационных процессов защиты информации в киберфизических системах	владеет: навыками применения технологий исследования и анализа информационных процессов защиты информации в киберфизических системах	на высоком профессиональном уровне: применяет технологии исследования и анализа информационных процессов защиты информации в киберфизических системах
Компетенция: ПК-4 Способен оценивать уровень защищенности киберфизических систем и применять решения по				

обеспечению их информационной безопасности				
ПК-4 ИД-1 оценка уровня защищённости киберфизических систем, анализ их структурно-функциональных характеристик	на низком уровне оценивает уровень защищённости киберфизических систем, анализ их структурно-функциональных характеристик	в основном оценивает уровень защищённости киберфизических систем, анализ их структурно-функциональных характеристик	знает, как оценивать уровень защищённости киберфизических систем, анализ их структурно-функциональных характеристик	на высоком профессиональном уровне оценивает уровень защищённости киберфизических систем, анализ их структурно-функциональных характеристик
ПК-4 ИД-2 порядок определение уязвимости и уровня защищённости киберфизических систем	на низком уровне умеет выбирать порядок определение уязвимости и уровня защищённости киберфизических систем	в основном умеет выбирать порядок определение уязвимости и уровня защищённости киберфизических систем	умеет выбирать порядок определение уязвимости и уровня защищённости киберфизических систем	на высоком профессиональном уровне умеет выбирать порядок определение уязвимости и уровня защищённости киберфизических систем
ПК-4 ИД-3 выбор оптимального набора технических мер для повышения защищённости киберфизических систем	на низком уровне владеет навыками выбора оптимального набора технических мер для повышения защищённости киберфизических систем	в основном владеет навыками выбора оптимального набора технических мер для повышения защищённости киберфизических систем	владеет навыками выбора оптимального набора технических мер для повышения защищённости киберфизических систем	на высоком профессиональном уровне владеет навыками выбора оптимального набора технических мер для повышения защищённости киберфизических систем

Оценивание уровня сформированности компетенции по дисциплине осуществляется на основе «Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры - в федеральном государственном автономном образовательном учреждении высшего образования «Северо-Кавказский федеральный университет» в актуальной редакции.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		Форма обучения ОФО семестр 2,3	
1.	B	Как называется мобильная версия Kali Linux? A. Kali Mobile B. Kali NetHunter C. AndroidKali D. Kali Phone	ПК-1
2.	C	Какая команда Linux используется для проверки SHA256-хеша образа? A. sha256check B. hash256 C. sha256sum D. checksum256	ПК-1
3.	A,B,D,E	Какие существуют Live-режимы использования Kali Linux? (Выберите все правильные варианты) A. Live DVD B. Live USB C. Cloud Live D. Virtual Machine E. Portable USB	ПК-1
4.	C	Какая команда обновляет список пакетов из репозиториев? A. apt-get refresh B. apt-get install C. apt-get update D. apt-get upgrade	ПК-1
5.	C	Какой тип сетевого подключения в VirtualBox рекомендуется для пентеста и почему? A. NAT, так как обеспечивает доступ в интернет B. Host-only, для безопасности C. Сетевой мост (Bridge), так как позволяет виртуальной машине получить IP в локальной сети D. Внутренняя сеть, для изоляции	ПК-1

6.	A	Какие существуют основные типы тестирования на проникновение в зависимости от объема доступной информации? A. Белый ящик, черный ящик, серый ящик B. Открытый, закрытый, смешанный C. Активный, пассивный, комбинированный D. Прямой, косвенный, комплексный	ПК-1
7.	A	Что является основным назначением руководства OWASP? A. Обеспечение безопасности веб-приложений B. Тестирование сетевых протоколов C. Защита от DDoS-атак D. Управление паролями	ПК-1
8.	B	Сколько основных этапов включает стандарт PTES? A. 5 B. 7 C. 6 D. 8	ПК-1
9.	C	Какой этап PTES включает сканирование портов с помощью Nmap? A. Предварительное взаимодействие B. Моделирование угроз C. Анализ уязвимостей D. Эксплуатация	ПК-1
10.	C	Какая методология тестирования применяется для компаний, работающих с платежными картами? A. PTES B. OWASP C. PCI D. NIST	ПК-1
11.	B	Какой тип тестирования максимально приближен к реальной атаке злоумышленника? A. Белый ящик B. Черный ящик	ПК-1

		C. Серый ящик D. Комбинированный	
12.	A	Что включает в себя этап предварительного взаимодействия в PTES? A. Определение целей и правил тестирования B. Непосредственное тестирование системы C. Анализ уязвимостей D. Составление отчета	ПК-1
13.	B	Какая из перечисленных методологий является стандартом с открытым исходным кодом? A. PCI B. NIST 800-115 C. OSSTMM D. PTES	ПК-1
14.	B	Какой этап PTES следует после сбора разведданных? A. Эксплуатация B. Моделирование угроз C. Анализ уязвимостей D. Пост-эксплуатация	ПК-1
15.	B	Что является ключевым преимуществом тестирования методом серого ящика? A. Имитация реальной атаки B. Комбинация преимуществ белого и черного ящика C. Быстрота проведения теста D. Низкая стоимость	ПК-1
16.	A	Что такое OSINT? A. Сбор информации из открытых источников B. Протокол сетевого взаимодействия C. Инструмент для сканирования портов D. Метод шифрования данных	ПК-1
17.	B	Какой инструмент используется для получения информации о регистрации домена? A. dig	ПК-1

		B. whois C. nmap D. host	
18.	A,B,E	Какие типы DNS-записей существуют? (Выберите все правильные варианты) A. A (IPv4-адрес) B. MX (почтовые серверы) C. IP (интернет-протокол) D. NS (серверы имён) E. CNAME (каноническое имя)	ПК-1
19.	A	Какой инструмент используется для автоматизированного сбора информации? A. Devploit B. Metasploit C. John the Ripper D. Hydra	ПК-1
20.	B	Что представляет собой Shodan? A. Сканер уязвимостей B. Поисковую систему подключённых устройств C. Инструмент для взлома паролей D. Генератор отчётов	ПК-1
21.	A	Какой инструмент используется для анализа DNS-записей? A. dig B. p0f C. hping3 D. fping	ПК-1
22.	B	Что такое передача зоны DNS? A. Процесс обновления DNS-серверов B. Метод получения полной информации о домене C. Способ шифрования DNS-трафика D. Протокол для передачи файлов	ПК-1

23.	B	Какой инструмент используется для массового сканирования доступности хостов? A. ping B. fping C. host D. dig	ПК-1
24.	B	Что такое Maltego? A. Инструмент для взлома паролей B. Программа для визуализации связей между данными C. Сканер уязвимостей D. Генератор отчётов	ПК-1
25.	B	Какой метод сбора информации считается пассивным? A. Сканирование портов B. Использование поисковых систем C. Тестирование на проникновение D. Взлом паролей	ПК-1
26.	A	Какой инструмент используется для массовой проверки доступности узлов в сети? A. fping B. ping C. hping3 D. traceroute	ПК-1
27.	B	Что такое активное снятие отпечатков ОС? A. Анализ захваченного трафика B. Отправка специально сформированных пакетов C. Пассивное наблюдение D. Мониторинг DNS-запросов	ПК-1
28.	C	Какой тип сканирования Nmap является самым скрытным? A. TCP Connect scan B. UDP scan C. TCP SYN scan	ПК-1

		D. XMAS scan	
29.	C	Какая команда используется для определения версий служб на открытых портах? A. nmap -sV B. nmap -sC C. nmap -sV -p- D. nmap -O	ПК-1
30.	B	Какой инструмент используется для пассивного определения ОС? A. Nmap B. p0f C. hping3 D. Striker	ПК-1
31.	B	Что означает параметр -f в Nmap? A. Быстрое сканирование B. Фрагментация пакетов C. Фильтрация результатов D. Фиксация портов	ПК-1
32.	C	Какой инструмент позволяет автоматизировать сбор информации о цели? A. Nmap B. p0f C. Striker D. hping3	ПК-1
33.	A,B,C,E	Какие состояния портов существуют в Nmap? (Выберите все правильные варианты) A. open B. closed C. filtered D. hidden E. unfiltered	
34.	B	Какой параметр Nmap используется для запуска базовых сценариев NSE?	ПК-1

		A. -sV B. –script=default C. -sC D. -O	
35.	C	В чем преимущество использования Striker? A. Только сканирование портов B. Только определение ОС C. Автоматизация сбора информации D. Только анализ уязвимостей	ПК-1
36.	A	Что является основным компонентом фреймворка Metasploit? A. MSFConsole, модули, интерфейсы B. Только эксплойты C. Только полезные нагрузки D. Только вспомогательные инструменты	ПК-4
37.	A,B,C,D	Какие типы модулей существуют в Metasploit? (Выберите все правильные варианты) A. Exploit B. Payload C. Auxiliary D. Encoders E. Antivirus	ПК-4
38.	C	Какая команда используется для запуска Metasploit? A. metasploit B. msf C. msfconsole D. msfstart	ПК-4
39.	B	Что такое полезная нагрузка (payload) в контексте эксплуатации? A. Инструмент для сканирования портов	ПК-4

		B. Код, выполняемый после успешной эксплуатации C. Программа для поиска уязвимостей D. Метод шифрования данных	
40.	C	Какой язык программирования используется для написания модулей Metasploit? A. Python B. C++ C. Ruby D. Java	ПК-4
41.	B	Для чего используется команда search в MSFConsole? A. Для сканирования портов B. Для поиска модулей по имени или описанию C. Для установки параметров D. Для запуска эксплойта	ПК-4
42.	A,B,C,E	Какие основные факторы определяют успех исследования уязвимостей? (Выберите все правильные варианты) A. Навыки программирования B. Инженерный анализ C. Инструментальные средства D. Физическая подготовка E. Создание полезной нагрузки	ПК-4
43.	B	Что такое Exploit-DB? A. База данных вирусов B. База данных эксплойтов C. Система обнаружения вторжений D. Файервол	ПК-4
44.	C	Какая команда используется для просмотра параметров выбранного модуля в MSFConsole? A. show params	ПК-4

		B. display C. show options D. list	
45.	B	Что такое Meterpreter? A. Тип эксплойта B. Расширенная полезная нагрузка C. Сканер уязвимостей D. Инструмент для анализа трафика	ПК-4
46.	A	Что такое уязвимость в контексте информационной безопасности? A. Недостаток в системе, который может быть использован злоумышленником B. Программа для защиты информации C. Метод шифрования данных D. Инструмент для тестирования сети	ПК-4
47.	A	Какие типы уязвимостей существуют? A. Локальные и удаленные B. Внутренние и внешние C. Активные и пассивные D. Открытые и закрытые	ПК-4
48.	A	Какой инструмент является коммерческим сканером уязвимостей? A. Nessus B. OpenVAS C. Lynis D. SPARTA	ПК-4
49.	A	Что такое локальная уязвимость? A. Уязвимость, требующая предварительного доступа к системе B. Уязвимость, эксплуатируемая через сеть C. Уязвимость в веб-приложении	ПК-4

		D. Уязвимость в сетевом оборудовании	
50.	A,B,C,D	Какие инструменты входят в состав Kali Linux для автоматического сканирования уязвимостей? (Выберите все правильные варианты) A. Nmap B. OpenVAS C. Lynis D. SPARTA E. Wireshark	ПК-4

2. Описание шкалы оценивания

Оценка «отлично» выставляется обучающемуся, если студент продемонстрировал высокое умение применять полученные знания на практике через решение конкретного задания, свободно без затруднений справился с поставленным заданием, показав владение разносторонними приемами и навыками его выполнения, не допустил ошибок и неточностей.

Оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал умение применять полученные знания на практике через решение конкретного задания, справился с поставленным заданием, показав владение необходимыми приемами и навыками его выполнения, при этом допустил незначительную ошибку.

Оценка «удовлетворительно» выставляется обучающемуся, если студентпродемонстрировал посредственное умение применять полученные знания на практике, с трудом справился с поставленным заданием, при этом допустил значительную ошибку.

Оценка «неудовлетворительно» выставляется обучающемуся, если студент не продемонстрировал умение применять полученные знания на практике через решение конкретного задания, не справился с поставленнымзаданием или допустил при его решении серьезную ошибку.

Процедура проведения данного оценочного мероприятия включает в себя Предлагаемые студенту задания позволяют проверить ПК-1, ПК-4 компетенции.

Для подготовки к данному оценочному мероприятию необходимо ответить на вопросы, предлагаемые преподавателем, ведущим дисциплину «Анализ защищенности киберфизических систем» Знания оцениваются преподавателем согласно правильно отвеченными вопросами.

Рейтинговая система оценки не предусмотрено для студентов, обучающихся на образовательных программах уровня высшего образования магистратуры, для обучающихся на образовательных программах уровня высшего образования бакалавриата заочной и очно-заочной формы обучения.

3. Критерии оценивания компетенций*

Оценка «отлично» выставляется, если студент продемонстрировал высокое самостоятельное владение методами сбора и структурирования данных для выявления потенциальных уязвимостей и угроз; разбирается в классификации угроз по критериям: субъект и объект атаки, метод воздействия, предпосылки и последствия; самостоятельно строит модели угроз для конкретных типов киберфизических систем с учётом их структурно-функциональных характеристик; демонстрирует высокое владение методиками проведения аудита информационной безопасности киберфизических систем; самостоятельно оценивает уровень защищенности киберфизических систем; выбирает адекватные средства и методы защиты информации для заданных типов киберфизических систем и сценариев угроз.

Оценка «хорошо» выставляется, если студент продемонстрировал владение методами сбора и структурирования данных для выявления потенциальных уязвимостей и угроз; разбирается в классификации угроз по критериям: субъект и объект атаки, метод воздействия, предпосылки и последствия; строит модели угроз для конкретных типов киберфизических систем с учётом их структурно-функциональных характеристик; демонстрирует владение методиками проведения аудита информационной безопасности киберфизических систем; оценивает уровень защищенности киберфизических систем; выбирает адекватные средства и методы защиты информации для заданных типов киберфизических систем и сценариев угроз.

Оценка «удовлетворительно» выставляется, если студент продемонстрировал посредственное владение методами сбора и структурирования данных для выявления потенциальных уязвимостей и угроз; разбирается в классификации угроз по критериям: субъект и объект атаки, метод воздействия, предпосылки и последствия; посредственно строит модели угроз для конкретных типов киберфизических систем с учётом их структурно-функциональных характеристик; демонстрирует посредственное владение методиками проведения аудита информационной безопасности киберфизических систем; посредственно оценивает уровень защищенности киберфизических систем; выбирает адекватные средства и методы защиты информации для заданных типов киберфизических систем и сценариев угроз.

Оценка «неудовлетворительно» выставляется, если студент не продемонстрировал владение

методами сбора и структурирования данных для выявления потенциальных уязвимостей и угроз; не разбирается в классификации угроз по критериям: субъект и объект атаки, метод воздействия, предпосылки и последствия; строит модели угроз для конкретных типов киберфизических систем с учётом их структурно-функциональных характеристик; не демонстрирует владение методиками проведения аудита информационной безопасности киберфизических систем; не оценивает уровень защищенности киберфизических систем; выбирает адекватные средства и методы защиты информации для заданных типов киберфизических систем и сценариев угроз.