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
Менеджмент инцидентов кибербезопасности
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 «Менеджмент инцидентов кибербезопасности».

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

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 «Менеджмент инцидентов кибербезопасности».

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-4 Способен оценивать уровень защищенности киберфизических систем и применять решения по обеспечению их информационной безопасности				
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
ПК-4 ИД-4 реализация организационно-технических мероприятия по обеспечению защиты киберфизических систем	на низком уровне реализует организационно-технических мероприятия по обеспечению защиты киберфизических систем	в основном реализует организационно-технических мероприятия по обеспечению защиты киберфизических систем	умеет реализовать организационно-технических мероприятия по обеспечению защиты киберфизических систем	на высоком профессиональном уровне реализует организационно-технических мероприятия по обеспечению защиты киберфизических систем
ПК-4 ИД-5 управляет инцидентами информационной безопасности киберфизических систем	на низком уровне управляет инцидентами информационной безопасности киберфизических систем	в основном управляет инцидентами информационной безопасности киберфизических систем	Знает, как управлять инцидентами информационной безопасности киберфизических систем	на высоком профессиональном уровне управляет инцидентами информационной безопасности 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.	A	Что такое контрольная сумма файла? A. Результат применения хеш-функции к данным файла для проверки его целостности B. Временная метка создания файла C. Размер файла в байтах D. Дата последнего изменения файла	ПК-4
2.	A	Какие основные свойства имеют криптографические хеш-функции? A. Односторонность и детерминированность B. Обратимость и случайность C. Многопоточность и масштабируемость D. Компрессия и архивация	ПК-4
3.	A	Для чего применяется HMAC? A. Для обеспечения целостности и аутентичности данных с помощью секретного ключа B. Для шифрования файлов C. Для создания цифровых подписей D. Для сжатия данных	ПК-4
4.	A	Какие инструменты используются для мониторинга целостности файлов? A. AIDE, Tripwire, OSSEC B. Nmap, Metasploit, Burp Suite C. Wireshark, Kali Linux, Parrot OS D. OpenVAS, Nessus, Zed Attack Proxy	ПК-4
5.	A	Что является основной целью контроля целостности файлов? A. Обнаружение несанкционированных изменений в системных файлах B. Ускорение работы системы C. Экономия дискового пространства D. Шифрование конфиденциальных данных	ПК-4
6.	A	Какие действия выполняются на этапе подготовки к реагированию на инциденты?	ПК-4

		A. Обеспечение возможности контроля целостности системных данных B. Удаление подозрительных файлов C. Блокировка всех сетевых подключений D. Форматирование жестких дисков	
7.	A	Что такое цифровая подпись? A. Метод подтверждения целостности и авторства документа с помощью асимметричной криптографии B. То же самое, что и HMAC C. Способ шифрования файлов D. Инструмент для создания паролей	ПК-4
8.	A	Какие типы криптографических функций существуют? A. Симметричные и асимметричные B. Линейные и нелинейные C. Простые и сложные D. Открытые и закрытые	ПК-4
9.	A	Что происходит при изменении данных файла? A. Меняется его контрольная сумма B. Остаётся прежней контрольная сумма C. Увеличивается размер файла D. Изменяется дата создания	ПК-4
10.	A	Какие источники событий безопасности существуют? A. Журналы аутентификации, сетевой трафик, системные журналы B. Только системные журналы C. Только сетевой трафик D. Только журналы аутентификации	ПК-4
11.	A	Что такое SID в контексте безопасности Windows? A. Уникальный идентификатор безопасности объекта или пользователя B. Протокол сетевого взаимодействия C. Команда командной строки	ПК-4

		D. Тип системного файла	
12.	A	Какие основные компоненты входят в структуру маркера доступа Windows? A. SID пользователя, SID групп, DACL, привилегии B. Только SID пользователя и пароль C. IP-адрес и порт D. Имя пользователя и права доступа	ПК-4
13.	A	Что такое DACL в Windows? A. Список контроля доступа, определяющий права субъектов к объекту B. Протокол шифрования данных C. Инструмент мониторинга системы D. Тип системного процесса	ПК-4
14.	A	Какой механизм используется для шифрования файлов в Windows? A. EFS (Encrypting File System) B. BitLocker C. Windows Defender D. Active Directory	ПК-4
15.	A	Что такое маркер доступа в Windows? A. Специальный объект, идентифицирующий пользователя и его права B. Файл конфигурации системы C. Сетевой протокол D. Тип системного события	ПК-4
16.	A	Какие привилегии могут быть предоставлены пользователю в Windows? A. Увеличение приоритета процессов, управление аудитом, завершение системы B. Только права на чтение файлов C. Только сетевые права D. Только административные права	ПК-4
17.	A	Как осуществляется идентификация пользователей в Windows? A. По уникальным SID B. Только по имени пользователя	ПК-4

		C. Только по паролю D. По IP-адресу	
18.	A	Что такое EFS? A. Шифрующая файловая система Windows B. Сетевой протокол C. Система управления пользователями D. Инструмент мониторинга	ПК-4
19.	A	Какие журналы событий существуют в Windows? A. Журнал приложений, безопасности, системы B. Только системный журнал C. Только журнал безопасности D. Только журнал приложений	ПК-4
20.	A	Какие категории событий подлежат аудиту в Windows? A. Вход в систему, управление учетными записями, доступ к объектам B. Только ошибки системы C. Только сетевые события D. Только действия администратора	ПК-4
21.	A	Что такое сетевое наблюдение? A. Процесс сбора, анализа и интерпретации данных о сетевом трафике B. Только мониторинг производительности сети C. Система обнаружения вирусов D. Метод шифрования данных	ПК-4
22.	A	Какой инструмент является наиболее распространённым для анализа сетевого трафика? A. Wireshark B. Nmap C. Metasploit D. Kali Linux	ПК-4
23.	A	Какие протоколы относятся к основным сетевым протоколам передачи данных? A. IP, TCP, UDP, DNS, HTTP, HTTPS	ПК-4

		B. FTP, SMTP, POP3 C. SNMP, ICMP D. Все перечисленные	
24.	A	Что такое сетевой сниффер? A. Программа для перехвата и анализа сетевых пакетов B. Антивирусная программа C. Файервол D. VPN-клиент	ПК-4
25.	A	Для чего используется фильтрация сетевого трафика? A. Для выделения определённых пакетов по заданным критериям B. Только для блокировки вредоносных пакетов C. Для ускорения работы сети D. Для шифрования данных	ПК-4
26.	A	Какой метод защиты используется для предотвращения перехвата сетевого трафика? A. Использование защищённых протоколов (HTTPS, VPN) B. Только файервол C. Антивирусное ПО D. Регулярное обновление системы	ПК-4
27.	A	Что позволяет определить анализ сетевых пакетов? A. Источник соединения, тип данных, подозрительную активность B. Только скорость передачи данных C. Только IP-адреса D. Только протоколы передачи	ПК-4
28.	A	Какие данные содержатся в сетевом пакете? A. Адрес отправителя, адрес получателя, номер порта, тип протокола B. Только данные пользователя C. Только служебная информация D. Только IP-адреса	ПК-4
29.	A	Что такое DNS-запрос?	ПК-4

		A. Запрос к серверу доменных имён для получения IP-адреса B. Команда для проверки связи C. Протокол передачи файлов D. Метод шифрования данных	
30.	A	В чём основное отличие HTTP от HTTPS? A. HTTPS использует шифрование данных, а HTTP — нет B. HTTP быстрее C. HTTPS работает только в определённых браузерах D. HTTP более безопасен	ПК-4
31.	A	Что такое система обнаружения вторжений (IDS)? A. Программно-аппаратный комплекс для выявления несанкционированной активности B. Программа для защиты от вирусов C. Файервол D. Система резервного копирования	ПК-4
32.	A	Какие основные функции выполняет IDS? A. Анализ трафика, выявление атак, регистрация событий безопасности B. Только блокировка вредоносного трафика C. Только мониторинг производительности сети D. Шифрование данных	ПК-4
33.	A	Какие режимы работы поддерживает Snort? A. Сниффер, логгер пакетов, система обнаружения вторжений B. Только режим анализатора трафика C. Только режим файервола D. Только режим обнаружения вторжений	ПК-4
34.	A	Что такое сигнатура в контексте IDS? A. Уникальный шаблон, описывающий известную атаку B. Пароль для доступа к системе C. Сетевой адрес злоумышленника	ПК-4

		D. Протокол шифрования	
35.	A	Какие протоколы может анализировать Snort? A. TCP, UDP, ICMP, ARP, DNS, SMTP, FTP B. Только HTTP и HTTPS C. Только TCP и UDP D. Только ICMP	ПК-4
36.	A	Что такое препроцессор в архитектуре Snort? A. Компонент, подготавливающий данные для детектора B. Модуль для шифрования трафика C. Инструмент для создания правил D. Система управления базами данных	ПК-4
37.	A	Какие преимущества имеет Snort? A. Поддержка множества протоколов, плагинов, работа с правилами B. Только высокая скорость работы C. Только простота установки D. Только бесплатность	ПК-4
38.	A	Для чего используются правила в Snort? A. Для описания условий обнаружения атак B. Для настройки сетевого подключения C. Для управления пользователями D. Для шифрования трафика	ПК-4
39.	A	Что такое libpcap в контексте Snort? A. Библиотека для перехвата сетевого трафика B. Модуль шифрования C. Система управления правилами D. База данных атак	ПК-4
40.	A	Какие действия можно выполнять с помощью Snort?	ПК-4

		A. Анализировать трафик, обнаруживать атаки, логировать события B. Только сканирование портов C. Только анализ производительности сети D. Только блокировка трафика	
41.	A	Что такое Honey Pot? A. Специализированная система для привлечения потенциальных злоумышленников B. Антивирусная программа C. Файервол D. Система резервного копирования	ПК-4
42.	A	Какие основные цели использования Honey Pot? A. Отвлечение, сбор информации, фиксация следов B. Только защита данных C. Только мониторинг сети D. Только обнаружение вирусов	ПК-4
43.	A	Что такое Padded Cell? A. Изолированная среда для контроля действий злоумышленника B. Тип антивирусного ПО C. Сетевой протокол D. Система шифрования	ПК-4
44.	A	Как взаимодействуют IDS и Padded Cell при обнаружении атаки? A. IDS перенаправляет злоумышленника в контролируемую среду Padded Cell B. IDS блокирует атаку C. Padded Cell самостоятельно обнаруживает атаки D. Они работают независимо друг от друга	ПК-4
45.	A	Какой тип информации размещается в Honey Pot? A. Ложная информация, выглядящая ценной для атакующего B. Действительные корпоративные данные	ПК-4

		C. Только системные файлы D. Личные данные пользователей	
46.	A	Почему любое обращение к Honey Pot считается подозрительным? A. Легитимные пользователи не должны иметь доступа к этой системе B. Система всегда находится в автономном режиме C. Honey Pot не подключается к сети D. Система работает только ночью	ПК-4
47.	A	Какое преимущество дает использование Honey Pot и Padded Cell? A. Получение времени для анализа атаки и принятия решений B. Полное предотвращение атак C. Автоматическое удаление вирусов D. Ускорение работы сети	ПК-4
48.	A	Какой риск связан с использованием Honey Pot? A. Опытный злоумышленник может распознать ловушку B. Увеличение нагрузки на сеть C. Потеря реальных данных D. Снижение скорости работы системы	ПК-4
49.	A	Что фиксируется в логах Honey Pot? A. IP-адрес атакующего, сканируемые порты, попытки определения сервисов B. Только время подключения C. Только тип используемого оборудования D. Только географическое положение атакующего	ПК-4
50.	A	Какая квалификация требуется администратору Honey Pot? A. Высокая квалификация в области информационной безопасности B. Базовые знания компьютера C. Только навыки программирования D. Опыт работы с офисными программами	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-4 компетенции.

Для подготовки к данному оценочному мероприятию необходимо ответить на вопросы, предлагаемые преподавателем, ведущим дисциплину «Менеджмент инцидентов кибербезопасности», 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 всесторонние умения самостоятельно выполнять планирование, идентификацию и анализ инцидентов кибербезопасности, моделировать риски, проводить мониторинг; применять технические и программные решения для угроз кибербезопасности; применять специализированное программное обеспечение для управления инцидентами кибербезопасности.

Оценка «хорошо» выставляется, если студент продемонстрировал умение выполнять планирование, идентификацию и анализ инцидентов кибербезопасности, моделировать риски, проводить мониторинг; применять технические и программные решения для угроз кибербезопасности; применять специализированное программное обеспечение для управления инцидентами кибербезопасности.

Оценка «удовлетворительно» выставляется, если студент продемонстрировал посредственное умение выполнять планирование, идентификацию и анализ инцидентов кибербезопасности, моделировать риски, проводить мониторинг; применять технические и программные решения для угроз кибербезопасности; применять специализированное программное обеспечение для управления инцидентами кибербезопасности.

Оценка «неудовлетворительно» выставляется, если студент не продемонстрировал умение выполнять планирование, идентификацию и анализ инцидентов кибербезопасности, моделировать риски, проводить мониторинг; применять технические и программные решения для угроз кибербезопасности; применять специализированное программное обеспечение для управления инцидентами кибербезопасности.