Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гробова Татьяна Анатольевна
Должность: и.о. декана факультета математики и компьютерных наук имени профессора Н.И. Червякова
Дата подписания: 17.06.2026 16:06:56
Уникальный программный ключ:
bd39d4208aa94cf4422feb787c816194d42de79a7

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

Технологии выявления следов киберпреступлений и инцидентов
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: данный фонд оценочных предназначен для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов, обучающихся по направлению подготовки 10.04.01 Информационная безопасность, направленность (профиль) «Информационная безопасность киберфизических систем» по дисциплине «Технологии выявления следов киберпреступлений и инцидентов».

2. Фонд оценочных средств текущего контроля и промежуточной аттестации на основе рабочей программы дисциплины «Технологии выявления следов киберпреступлений и инцидентов» в соответствии с образовательной программой 10.04.01 Информационная безопасность, направленность (профиль) «Информационная безопасность киберфизических систем».

3. Разработчик Ванина Анна Георгиевна, к.т.н., доцент кафедры организации и технологии защиты информации.

4. Проведена экспертиза ФОС.
Члены экспертной группы:
Председатель: Петренко В.И., заведующий кафедрой
Члены экспертной группы: Жук А.П., профессор кафедры
Минкина Т.В., доцент кафедры

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

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

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-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-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 очная, семестр 3	
3 семестр			
1.	b)	Выберите правильное определение понятия «Судебная экспертиза» a) это процессуальное действие, состоящее из проведения осмотра, описания и дачи заключения экспертом по вопросам, разрешение которых требует специальных знаний в области науки, техники, искусства или ремесла и которые поставлены перед экспертом судом, судьей, органом дознания, лицом, производящим дознание, следователем, в целях установления обстоятельств, подлежащих доказыванию по конкретному делу b) это процессуальное действие, состоящее из проведения исследований и дачи заключения экспертом по вопросам, разрешение которых требует специальных знаний в области науки, техники, искусства или ремесла и которые поставлены перед экспертом судом, судьей, органом дознания, лицом, производящим дознание, следователем, в целях установления обстоятельств, подлежащих доказыванию по конкретному делу c) это процессуальное действие, состоящее из дачи заключения d) это процесс исследования оборудования	ПК-4
2.	b) c) d) e) f)	Что исследует компьютерно-техническая экспертиза? a) все виды любой электронной техники b) комплексно исследует компьютерные средства: c) техническую (аппаратную) часть компьютерных средств; d) программное обеспечение; e) объекты сетевых информационных технологий; f) информацию, содержащуюся в компьютерной системе	ПК-4
3.	a) b) c) d) e)	Что входит в перечень требований к экспертному заключению? a) полнота – указание всех признаков; исследование в отношении всех поставленных вопросов; ответ на все поставленные вопросы; исследование всех объектов, предоставленных на исследование; исследование всех материалов, относящихся к предмету экспертизы;	ПК-4

		использование необходимых методик, обеспечивающих полноту исследования b) объективность – применение объективно существующих специальных знаний; объективный подход к исследованию; использование научно обоснованных методик c) всесторонность – изучение объекта со всех сторон, в том числе экспертная инициатива d) достоверность – возможность проверки экспертного заключения на относимость (относимость установленного факта к предмету доказывания) e) допустимость (возможность допущения экспертного заключения, как средства доказывания – соблюдение процессуальных требований)	
4.	c)	Что классически используют для классификации методик компьютерно-технической экспертизы? a) теорию множеств b) гиперграф c) ориентированный граф A(B, C) d) последовательность	ПК-4
5.	a) c) e)	Критерии классификации методик компьютерно-технической экспертизы a) Категория задач b) Методы КТЭ c) Цели (вопросы КТЭ) d) Признаки оборудования e) Объекты КТЭ f) Типы работ	ПК-4
6.	d)	Что используется для решения задачи оценки трудозатрат при производстве КТЭ a) Системный подход b) Алогичный подход c) Общая задача трудозатрат d) Методология PERT e) Методология IDEF0	ПК-4
7.	b) a) f) d) c) e)	Выберите верную последовательность стадий производства КТЭ? a) аналитическая стадия;	ПК-4

		b) подготовительная стадия; c) результирующая стадия; d) синтезирующая стадия; e) стадия формирования выводов f) эксперимент;	
8.	a)	Основная задача подготовительной стадии производства КТЭ a) Клонирование данных b) Обесточивание оборудования c) Изъятие документов d) Разное	ПК-4
9.	d)	Чем является результирующая стадия при производстве КТЭ a) Формирование доказательств b) Поиск улик c) Поиск подозреваемых d) Подведение итогов e) Методология IDEF0	ПК-4
10.	a) b) d)	Что может исследовать аппаратно-компьютерная экспертиза? a) Мобильный телефон b) IP-камера c) Образ SSD диска d) SSD диск	ПК-4
11.	a)	Основная задача программно-компьютерной экспертизы a) Исследование образов носителей информации b) Обесточивание оборудования c) Изъятие документов d) Разное	ПК-4
12.	d)	Чем является результат компьютерно-сетевой экспертизы? a) Формирование доказательств b) Поиск улик c) Поиск подозреваемых d) Написание заключения об определенных сетевых действиях e) Методология IDEF0	ПК-4

13.	a) b) c)	Перечисленные способы несанкционированного доступа к электронным почтовым ящикам и другим онлайн-аккаунтам a) методом подбора пароля (brute-force), включая ручной утопический вариант, а также использование многочисленных программ, реализующих атаки по словарям и гибридные атаки; посредством вредоносной программы, исполняемой на компьютерном оборудовании жертвы (компьютере, ноутбуке, мобильном телефоне), внедряемой удаленно; b) посредством вредоносной программы, исполняемой на компьютерном оборудовании (компьютере, ноутбуке, мобильном телефоне) жертвы, при физическом доступе к оборудованию пользователя; c) путем использования программных утилит (HackTool) при физическом доступе к компьютерной технике пользователя; d) посредством кражи оборудования e) путем киднэппинга	ПК-4
14.	a) b) d) e)	Источники сбора информации при атаке с использованием социальной инженерии? a) Опубликованные резюме, статьи, научные работы b) Социальные сети, профили связей c) Доски объявлений d) Онлайн-сервисы e) Публичная корпоративная информация f) Медицинские организации	ПК-4
15.	b)	Для чего используется платформа AMPPS? a) Платформа для взлома b) Платформа для пентестинга c) Хакерская программа	ПК-4
16.	a)	Инструмент для определения браузера пользователя a) UserAgent b) Partition Recovery c) GRUB	ПК-4
17.	b)	Опишите тип инъекции Trojan-Spy.Win64.Lurk? a) Инъектор для кражи паролей b) Инъектор для изучения сети	ПК-4

18.	b)	Инструмент для анализа паразитного мобильного траффика с привязкой к приблизительным геоданным? a) X-plore b) Show info MAC c) SniffToolPro	ПК-4
19.	a)	Двухфакторная авторизация – это a) Инструмент повышения уровня безопасности и индикации параллельного использования аккаунтов b) Инструмент индикации параллельного использования аккаунтов c) GRUB	ПК-4
20.	b)	Механизм фишинга с использованием похожего доменного имени позволяет? a) Получить обход антивирусов b) Получить информацию напрямую от жертвы	ПК-4
21.	b)	Что такое DynDNS? a) Инструмент скрытия локации b) Возможность использовать локальный сервер для своего сайта/портала c) Антибот-сервис	ПК-4
22.	№ 374-ФЗ	Новый вид ОРМ «получение компьютерной информации» введен в действие федеральным законом …	ПК-4
23.	b)	В каком случае оператор по переводу денежных средств возмещает средства клиента? a) В случае перевода средств клиентом мошеннику b) В случае перевода средств без согласия клиента	ПК-4
24.	a) b) c)	Виды мероприятий при расследовании инцидентов? a) Служебная проверка b) Компьютерное исследование c) Компьютерно-техническая экспертиза	ПК-4
25.	b)	Законна ли выдача геолокации абонента без его согласия? a) Да b) Да, в установленном законом порядке c) Нет	ПК-4
26.	b)	Кто имеет право проверять физическое лицо по государственным информационным системам?	ПК-4

		a) Уполномоченные структуры b) Уполномоченные структуры, либо физ.лица при использовании открытых гос. источников информации c) Физические лица	
27.	a) b)	Легально ли применение специальных технических средств, замаскированных под бытовые устройства? a) Нет b) Да, в рамках ОРМ c) Да	ПК-4
28.	b)	Что косвенно исследуется на начальных этапах анализа трафика? a) Пакеты b) Все пункты c) Мас-адреса d) Ip-адреса e) Arp-таблицы	ПК-4
29.	b)	На каком уровне производится взаимодействие между процессами? a) Прикладной b) Транспортный c) Сетевой d) Канальный	ПК-4
30.	3	Сколько этапов рукопожатия нужно для установления канала связи и обеспечения удалённого доступа к исследуемому хосту?	ПК-4
31.	b)	Что такое генератор псевдослучайной последовательности? a) Пакеты b) алгоритм, который всегда генерирует один и тот же кажущийся случайным результат при использовании одного и того же ключа c) алгоритм, который всегда генерирует разные результаты при использовании одного и того же ключа d) Ip-адреса e) алгоритм, который всегда генерирует один и тот же результат при использовании одного и того же ключа	ПК-4
32.	a)	Какая система предполагает использование двух ключей? a) Криптосистема с открытым ключом	ПК-4

		b) Любая криптосистема	
33.	HMAC	Какая функция используется для проверки подлинности сообщений?	ПК-4
34.	b)	Атака с визуальной подделкой сайта… a) Сниффинг b) Фишинг c) Хакинг d) Крэкинг	ПК-4
35.	a)	Для чего предназначена система Shodan? a) Для поиска активных IP-адресов b) Для поиска активных Mac-адресов c) Для поиска физических адресов	ПК-4
36.	2	Основное количество этапов создания дипфэйка?	ПК-4
37.	b)	На что направлена уязвимость Heartbleed? a) ActiveDirectory b) OpenSSL c) PowerShell d) Honeypot	ПК-4
38.	a)	Что такое фаззинг? a) Метод динамического тестирования и проникновения b) Метод социальной инженерии c) Метод обработки пакетов	ПК-4
39.	Сканирования адресов	Инструмент Armitage предназначен для …?	ПК-4
40.	8	Основное количество компонентов качественного отчёта о тесте на проникновение?	ПК-4
41.	1. подготовительная стадия; 2. аналитическая стадия; 3. эксперимент; 4. синтезирующая стадия; 5. результирующая стадия;	Постройте последовательность стадий проведения компьютерно-технической экспертизы	ПК-4

	6. стадия формирования выводов.		
42.	C:\windows\system32\config\SAM	Напишите основной путь к информации об артефактах о смене пароля в ОС Windows	ПК-4
43.	-d	Какой флаг требуется указать для развёртывания Docker в режиме демона?	ПК-4
44.	-compose logs	Какой флаг требуется указать для просмотра логов Docker?	ПК-4
45.		Постройте классическую схему работы с почтовым сервером при фишинг атаке	ПК-4
46.		Опишите схему работы протокола, через который происходит внедрение через электронную почту с применением методов социальной инженерии?	ПК-4
47.	ip_forward	Какую функцию необходимо включить в случае проведения атаки ARP-spoofing и, соответственно, выключить в момент совершения инцидента, для защиты от атаки данного типа, при использовании Metasploitable?	ПК-4
48.	1. Сбор информации 2. Целенаправленное проникновение 3. Постэксплуатация и увеличение прав доступа 4. Документирование	Назовите четыре основных этапа теста на проникновение в сеть:	ПК-4
49.	1. пароли/конфигурации по умолчанию; 2. одинаковые учетные данные в нескольких системах; 3. наличие прав локального администратора у всех пользователей; 4. отсутствующие патчи общедоступных эксплойтов.	Назовите основные элементы Low-hanging fruits (доступных мишеней при тестировании на проникновение):	ПК-4
50.	/etc/passwd	Какой файл сервера Linux обычно перезаписывается без создания учётных записей при пентесте?	ПК-4

2. Описание шкалы оценивания

Оценка «отлично» выставляется обучающемуся, если студент продемонстрировал высокое умение применять полученные знания на практике черезрешение 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 не более одной ошибки.

Оценка «удовлетворительно» выставляется обучающемуся, если студент продемонстрировал посредственное умение применять полученные знания на практике через решение конкретного задания, с трудом справился с поставленным заданием, при этом допустил не более двух ошибок

Оценка «неудовлетворительно» выставляется обучающемуся, если студент не продемонстрировал умение применять полученные знания на практике через решениеконкретного задания, не справился с поставленным заданием или допустил при его решении три и более серьезные ошибки.

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 студенту, если он уверенно разрабатывает проекты организационно-распорядительной документации по обеспечению информационной безопасности; самостоятельно проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности

Оценка «хорошо» выставляется студенту, если он умеет разрабатывать проекты организационно-распорядительной документации по обеспечению информационной безопасности; хорошо проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности

Оценка «удовлетворительно» выставляется студенту, если он частично разрабатывает проекты организационно-распорядительной документации по обеспечению информационной безопасности; плохо проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности

Оценка «неудовлетворительно» выставляется студенту, если он не умеет разрабатывать проекты организационно-распорядительной документации по обеспечению информационной безопасности; не проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности