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
Гробова Т.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
«Технологии расследования компьютерных преступлений и инцидентов»

Специальность	Информационная безопасность автоматизированных систем
Специализация	Анализ безопасности информационных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в 9 семестре	

Введение

1. Назначение: Фонд оценочных средств предназначен для обеспечения методической основы для организации и проведения текущего контроля по дисциплине «Технологии расследования компьютерных преступлений и инцидентов». Текущий контроль по данной дисциплине – вид систематической проверки знаний, умений, навыков студентов. Задачами текущего контроля являются получение первичной информации о ходе и качестве освоения компетенций, а также стимулирование регулярной целенаправленной работы студентов. Для формирования определенного уровня компетенций.

2. ФОС является приложением к программе дисциплины «Технологии расследования компьютерных преступлений и инцидентов»

3. Разработчик: Лапина М. А. доцент кафедры вычислительной математики и кибернетики.

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель

Бабенко М. Г. заведующий кафедрой вычислительной математики и кибернетики.

Члены комиссии:

Пелешенко В.С. доцент кафедры вычислительной математики и кибернетики

Пелешенко Т. А. доцент кафедры вычислительной математики и кибернетики

Представитель организации-работодателя Корниенко С. А. начальник управления филиала ФГУП «Главный радиочастотный центр» в Южном и Северо-Кавказском федеральных округах

Экспертное заключение: фонд оценочных средств соответствует образовательной программе по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация Анализ безопасности информационных систем и рекомендуется для проведения текущего контроля успеваемости и промежуточной аттестации студентов.

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 компетенци(ий),			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
Компетенция: ОПК 13				
Результаты обучения по дисциплине (модулю): Индикатор: ИД-1. ОПК-13. Оценивает вероятность возникновения потенциальных угроз информационной безопасности предприятия (организации); использует методы восстановления работоспособности средств защиты информации при возникновении нештатной ситуации; определяет основные действия сотрудника информационной безопасности предприятия (организации) при возникновении либо обнаружении следов компьютерных преступлений; использует	Не предоставляет отчет в котором демонстрирует основные угрозы информационной безопасности предприятия (организации), а также методы восстановления работоспособности средств защиты информации при возникновении нештатной ситуации и описывает основные действия сотрудника информационной безопасности предприятия (организации) при возникновении либо обнаружении следов компьютерных преступлений	Предоставляет неполный отчет с неполным пояснением в котором демонстрирует основные угрозы информационной безопасности предприятия (организации), а также методы восстановления работоспособности средств защиты информации при возникновении нештатной ситуации и описывает основные действия сотрудника информационной безопасности предприятия (организации) при возникновении либо обнаружении следов компьютерных преступлений с использованием методов	Предоставляет отчет с пояснением в котором демонстрирует основные угрозы информационной безопасности предприятия (организации), а также методы восстановления работоспособности средств защиты информации при возникновении нештатной ситуации и описывает основные действия сотрудника информационной безопасности предприятия (организации) при возникновении либо обнаружении следов компьютерных преступлений с использованием методов расследования	Предоставляет детальный отчет с полным пояснением в котором демонстрирует основные угрозы информационной безопасности предприятия (организации), а также методы восстановления работоспособности средств защиты информации при возникновении нештатной ситуации и описывает основные действия сотрудника информационной безопасности предприятия (организации) при возникновении либо обнаружении следов компьютерных преступлений с использованием методов

методы расследования компьютерных преступлений и инцидентов.	с использованием методов расследования компьютерных преступлений и инцидентов	расследования компьютерных преступлений и инцидентов	компьютерных преступлений и инцидентов	расследования компьютерных преступлений и инцидентов
ИД-2. ОПК-13. Проводит диагностику компьютерной системы на обнаружение программно-аппаратных средств совершения киберпреступлений; выявлять следы совершения компьютерных преступлений и проведению оценки защищенности компьютерной системы на защиту информации.	Не предоставляет отчет в котором демонстрирует свою способность проводить диагностику компьютерной системы на обнаружение программно-аппаратных средств совершения киберпреступлений и выявлять следы совершения компьютерных преступлений и проведению оценки защищенности компьютерной системы на защиту информации.	Предоставляет неполный отчет в котором демонстрирует свою способность проводить диагностику компьютерной системы на обнаружение программно-аппаратных средств совершения киберпреступлений и выявлять следы совершения компьютерных преступлений и проведению оценки защищенности компьютерной системы на защиту информации.	Предоставляет отчет в котором демонстрирует свою способность проводить диагностику компьютерной системы на обнаружение программно-аппаратных средств совершения киберпреступлений и выявлять следы совершения компьютерных преступлений и проведению оценки защищенности компьютерной системы на защиту информации.	Предоставляет детальный отчет в котором демонстрирует свою способность проводить диагностику компьютерной системы на обнаружение программно-аппаратных средств совершения киберпреступлений и выявлять следы совершения компьютерных преступлений и проведению оценки защищенности компьютерной системы на защиту информации.
ИД-3. ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей	Не предоставляет отчет в которым показывает свою способность организовывать и проводить диагностику и тестирование систем	Предоставляет неполный отчет в которым показывает свою способность организовывать и проводить диагностику и тестирование систем защиты информации автоматизирова	Предоставляет отчет в которым показывает свою способность организовывать и проводить диагностику и тестирование систем защиты информации автоматизирова	Предоставляет детальный отчет в которым показывает свою способность организовывать и проводить диагностику и тестирование систем защиты информации

систем защиты информации автоматизированны х систем при расследовании компьютерных преступлений и инцидентов	защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем при расследовании компьютерных преступлений и инцидентов	нны х систем, проводить анализ уязвимостей систем защиты информации автоматизированны х систем при расследовании компьютерных преступлений и инцидентов	нны х систем, проводить анализ уязвимостей систем защиты информации автоматизированны х систем при расследовании компьютерных преступлений и инцидентов	автоматизированны х систем, проводить анализ уязвимостей систем защиты информации автоматизированны х систем при расследовании компьютерных преступлений и инцидентов

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/заочная/очно-заочная	
1.	Компьютерная криминалистика — это раздел судебной медицины, изучающий восстановление, расследование, экспертизу и анализ материалов, обнаруженных в цифровых устройствах, особенно мобильных устройствах и компьютерах.	Что такое компьютерная криминалистика?	ОПК-13
2.	Цифровые доказательства — это данные, найденные на цифровых устройствах, которые могут быть использованы в уголовных или гражданских делах для поддержки или опровержения гипотезы.	Что такое цифровые доказательства?	ОПК-13
3.	Типы цифровых доказательств включают электронные письма, сообщения,	Какие типы цифровых доказательств существуют?	ОПК-13

	фотографии, видео, файлы, документы и другие цифровые материалы.		
4.	Преимущества использования цифровых доказательств в компьютерной криминалистике включают объективность, доступность и возможность быстрого анализа большого объёма данных.	Каковы преимущества использования цифровых доказательств в компьютерной криминалистике?	ОПК-13
5.	Судебно-техническая экспертиза — это исследование цифровых устройств и их содержимого для восстановления информации, идентификации пользователей и анализа данных.	Что такое судебно-техническая экспертиза?	ОПК-13
6.	Типы судебно-технических экспертиз включают компьютерную экспертизу, сетевую экспертизу, судебный анализ данных и	Какие типы судебно-технических экспертиз существуют в компьютерной криминалистике?	ОПК-13

	экспертизу мобильных устройств.		
7.	Цифровые улики — это данные, найденные на цифровых устройствах, которые могут быть использованы в качестве доказательств в уголовных или гражданских делах.	Что такое цифровые улики?	ОПК-13
8.	Изъятие цифровых улик может происходить через изъятие самих устройств, копирование данных или использование специальных инструментов для извлечения информации.	Каким образом можно изъять цифровые улики?	ОПК-13
9.	Сетевая атака — это попытка несанкционированного доступа к компьютерной сети или системе с целью получения информации, нарушения безопасности или нанесения ущерба.	Что такое сетевая атака?	ОПК-13
10.	Сканирование портов — это процесс проверки открытых портов на	Что такое сканирование портов?	ОПК-13

	сетевых устройствах для определения доступных сервисов и уязвимостей.		
11.	Блокчейн — это распределённая база данных, которая хранит информацию о транзакциях в виде цепочки блоков.	Что такое блокчейн?	ОПК-13
12.	Криптовалюта — это цифровая валюта, использующая криптографию для обеспечения безопасности и анонимности транзакций.	Что такое криптовалюта?	ОПК-13
13.	Цифровая подпись — это криптографический метод аутентификации и подтверждения авторства электронных документов или сообщений.	Что такое цифровая подпись?	ОПК-13
14.	При анализе цифровых улик могут быть восстановлены различные типы данных, такие как текстовые файлы, документы, аудио- и видеофайлы,	Какие типы данных могут быть восстановлены при анализе цифровых улик?	ОПК-13

	изображения, архивы, базы данных, электронные таблицы и другие форматы файлов.		
15.	Сниффер — это программное или аппаратное средство, предназначенное для перехвата и анализа сетевого трафика.	Что такое сниффер?	ОПК-13
16.	DDoS-атака — это тип сетевой атаки, при которой множество компьютеров или устройств одновременно отправляют запросы на сервер, перегружая его и вызывая отказ в обслуживании.	Что такое DDoS-атака?	ОПК-13
17.	Методы использования социальных сетей в качестве доказательств включают анализ контента, отслеживание активности пользователей и изучение связей между ними.	Какие методы использования социальных сетей могут быть использованы в качестве доказательств?	ОПК-13
18.	Криптография — это наука об обеспечении конфиденциальности и	Что такое криптография?	ОПК-13

	целостности информации путём использования криптографических методов и алгоритмов.		
19.	В компьютерной криминалистике используются различные типы криптографии для защиты данных и обеспечения их подлинности.	Какие типы криптографии используются в компьютерной криминалистике?	ОПК-13
20.	Вредоносное ПО — это программное обеспечение, предназначенное для нанесения ущерба или нарушения работы компьютерных систем и сетей. Оно может включать вирусы, черви, троянские кони и другие типы вредоносных программ.	Что такое вредоносное ПО?	ОПК-13
21.	Wireshark, tcpdump, Snort и другие	Какие инструменты могут использоваться для анализа сетевых протоколов при расследовании компьютерных преступлений?	ОПК-13
22.	c) Самостоятельное проведение расследования.	Какую из перечисленных опций НЕ следует выполнять при обнаружении потенциального компьютерного преступления? a) Оповещение соответствующих органов	ОПК-13

2. Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Система оценки знаний студентов основана на использовании совокупности контрольных мероприятий по проверке пройденного материала, оптимально расположенных на всем временном интервале изучения дисциплины.

3. Критерии оценивания компетенций*

Оценка «**зачтено**» выставляется студенту, если студент знает ключевых понятия, демонстрирует понимание основных терминов, принципов и теоретических основ дисциплины, материал излагается логично, с выделением причинно-следственных связей и примеров, используются рекомендованные учебные материалы, а также дополнительные достоверные источники, работы (индивидуальные, групповые, проектные) сданы в установленные сроки и соответствуют требованиям, студент корректно использует изученные методики, инструменты или технологии, в работах присутствуют обоснованные заключения, а в случае проектов – практическая значимость.

Оценка «**не зачтено**» выставляется студенту в следующих случаях: неудовлетворительное освоение программы: не продемонстрировано понимание базовых понятий и принципов дисциплины в работах содержатся грубые теоретические ошибки отсутствует логика в изложении материала ответы не соответствуют поставленным вопросам, невыполнение практических требований: работа не сдана в установленный срок без уважительной причины практические задания выполнены менее чем на 50% от требуемого объема нарушены методические требования к оформлению работ обнаружен плагиат (более 50% заимствованного текста без указания источников).