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

УТВЕРЖДАЮ
декан факультета математики
и компьютерных наук
имени профессора Н.И. Червякова
Гробова Т.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
Технологии выявления следов компьютерных преступлений, правонарушений и инцидентов

Специальность	10.05.01 Компьютерная безопасность
Специализация	Информационно-аналитическая и техническая экспертиза компьютерных систем
Форма обучения	очная
Год начала обучения	2026
Реализуется в семестре	9

Введение

1. Назначение: обеспечение методической основы для организации и проведения текущего контроля по дисциплине «Технологии выявления следов компьютерных преступлений, правонарушений и инцидентов». Текущий контроль по данной дисциплине – вид систематической проверки знаний, умений, навыков студентов. Задачами текущего контроля являются получение первичной информацию 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 (модуля) «Технологии выявления следов компьютерных преступлений, правонарушений и инцидентов»

3. Разработчик (и): Березницкий А.С., доцент кафедры вычислительной математики и кибернетики

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель Тебуева Ф.Б., профессор кафедры вычислительной математики и кибернетики

Члены комиссии: Осипов Д.Л., доцент кафедры вычислительной математики и кибернетики

Гусева Л.Л., доцент кафедры вычислительной математики и кибернетики

Представитель организации-работодателя: Березницкий А.С., заместитель директора ФБУ «Северо-Кавказский региональный центр судебной экспертизы Министерства юстиции РФ».

Экспертное заключение: Представленный ФОС по дисциплине «Технологии выявления следов компьютерных преступлений, правонарушений и инцидентов» соответствует требованиям ФГОС ВО. Предлагаемые преподавателем формы и средства текущего контроля адекватны целям и задачам реализации образовательной программы высшего образования по специальности 10.05.01 Компьютерная безопасность, а также целям и задачам рабочей программы реализуемой учебной дисциплины. Оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации представлены в полном объеме.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

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

Уровни сформированности компетенци(ий), индикатора (ов)	Дескрипторы			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
Компетенция: ОПК-6.1				
Результаты обучения по дисциплине (модулю): *Индикатор:* ИД-1 определяет причины, цели и условия изменения свойств (состояния) программного и аппаратного обеспечения	Имеет слабое представление о методах определения причин, целей и условий изменения свойств (состояния) программного и аппаратного обеспечения	Имеет частичное представление о методах определения причин, целей и условий изменения свойств (состояния) программного и аппаратного обеспечения	Имеет представление о методах определения причин, целей и условий изменения свойств (состояния) программного и аппаратного обеспечения	Имеет полное представление о методах определения причин, целей и условий изменения свойств (состояния) программного и аппаратного обеспечения
Результаты обучения по дисциплине (модулю): *Индикатор:* ИД-2 ОПК-6.1 применяет инструментальные средствами поиска, фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов	Имеет слабое представление о применении инструментальных средств поиска, фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов	Имеет частичное представление о применении инструментальных средств поиска, фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов	Имеет представление о применении инструментальных средств поиска, фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов	Имеет полное представление о применении инструментальных средств поиска, фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов
Компетенция: ОПК-8				
Результаты обучения по дисциплине (модулю): Индикатор: ИД-1 ОПК-8 составляет обзоры и готовит отчеты о результатах научно-исследовательских и проектных работ	Предоставляет частичный отчёт с грубыми ошибками по составленным обзорам и отчетам о результатах научно-исследовательских и проектных работ	Предоставляет частичный отчёт по составленным обзорам и отчетам о результатах научно-исследовательских и проектных работ	Предоставляет отчёт по составленным обзорам и отчетам о результатах научно-исследовательских и проектных работ	Предоставляет детальный отчёт по составленным обзорам и отчетам о результатах научно-исследовательских и проектных работ

Оценочные средства для проверки уровня сформированности компетенций
9 семестр

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
1.		Что такое компьютерная криминалистика?	ОПК-8
2.		Что такое цифровые доказательства?	ОПК-8
3.		Какие типы цифровых доказательств существуют?	ОПК-8
4.		Каковы преимущества использования цифровых доказательств в компьютерной криминалистике?	ОПК-8
5.		Что такое судебно-техническая экспертиза?	ОПК-8
6.		Какие типы судебно-технических экспертиз существуют в компьютерной криминалистике?	ОПК-8
7.		Что такое цифровые улики?	ОПК-8
8.		Каким образом можно изъять цифровые улики?	ОПК-8
9.		Что такое сетевая атака?	ОПК-8
10.		Что такое сканирование портов?	ОПК-8
11.		Что такое блокчейн?	ОПК-8
12.		Что такое криптовалюта?	ОПК-8
13.		Что такое цифровая подпись?	ОПК-8
14.		Какие типы данных могут быть восстановлены при анализе цифровых улик?	ОПК-8
15.		Что такое сниффер?	ОПК-8
16.		Что такое DDoS-атака?	ОПК-8
17.		Какие методы использования социальных сетей могут быть использованы в качестве доказательств?	ОПК-8
18.		Что такое криптография?	ОПК-8
19.		Какие типы криптографии используются в компьютерной криминалистике?	ОПК-8
20.		Что такое вредоносное ПО?	ОПК-8
21.		Что такое кибершпионаж?	ОПК-8
22.		Как можно определить, была ли проведена DDoS-атака?	ОПК-8
23.		Что такое виртуальная машина?	ОПК-8
24.		Какие инструменты используются для анализа цифровых улик?	ОПК-8
25.		Что такое стеганография?	ОПК-8
26.		Как можно защитить компьютерную систему от кибератак?	ОПК-8
27.		Компьютерная криминалистика.	ОПК-8
28.		Что такое "цифровая подпись"?	ОПК-8
29.		Какой тип кибератаки основан на использовании вредоносных программ?	ОПК-8
30.		Какой тип кибератаки основан на перехвате информации, передаваемой по сети?	ОПК-8
31.		Какой тип кибератаки направлен на блокирование доступа к компьютерной системе?	ОПК-8
32.		Какие типы криптографии используются в компьютерной криминалистике?	ОПК-8
33.		Что такое вредоносное ПО?	ОПК-8
34.		Какими методами можно обнаружить вредоносное ПО?	ОПК-8
35.		Что такое доказательства в цепочке?	ОПК-8
36.		Что такое киберпреступность?	ОПК-8
37.		Что такое компьютерное преступление?	ОПК-6.1
38.		Какие виды компьютерных преступлений	ОПК-6.1

		существуют?	
39.		Что такое цифровой след?	ОПК-6.1
40.		Какие основные задачи расследования компьютерных преступлений?	ОПК-6.1
41.		Что такое журнал безопасности?	ОПК-6.1
42.		Какие данные могут содержаться в журнале безопасности?	ОПК-6.1
43.		Что такое хеш-сумма?	ОПК-6.1
44.		Зачем используется хеш-сумма при расследовании компьютерных преступлений?	ОПК-6.1
45.		Какие виды цифровых следов бывают?	ОПК-6.1
46.		Что такое активный цифровой след?	ОПК-6.1
47.		Что такое пассивный цифровой след?	ОПК-6.1
48.		Что такое прямой цифровой след?	ОПК-6.1
49.		Что такое косвенный цифровой след?	ОПК-6.1
50.		Какие инструменты используются для сбора цифровых следов?	ОПК-6.1
51.		Что такое методология сбора данных при расследовании компьютерных преступлений?	ОПК-6.1
52.		Какие этапы включает методология сбора данных при расследовании компьютерных преступлений?	ОПК-6.1
53.		Что такое хеш-сумма?	ОПК-6.1
54.		Зачем используется хеш-сумма в расследовании компьютерных преступлений?	ОПК-6.1
55.		Какие программные инструменты используются при сборе и анализе данных в расследовании компьютерных преступлений?	ОПК-6.1
56.		Что такое кросс-доменная атака?	ОПК-6.1
57.		Что такое SQL-инъекция?	ОПК-6.1
58.		Что такое DDoS-атака?	ОПК-6.1
59.		Какие меры безопасности можно предпринять для защиты от DDoS-атак?	ОПК-6.1
60.		Что такое сетевой протокол?	ОПК-6.1
61.	Wireshark, tcpdump, Snort и другие	Какие инструменты могут использоваться для анализа сетевых протоколов при расследовании компьютерных преступлений?	ОПК-6.1
62.	c) Самостоятельное проведение расследования.	Какую из перечисленных опций НЕ следует выполнять при обнаружении потенциального компьютерного преступления? a) Оповещение соответствующих органов b) Сохранение логов и других данных для последующего анализа c) Самостоятельное проведение расследования d) Обеспечение физической безопасности системы	ОПК-6.1
63.	d) Мобильные приложения.	Что из перечисленного НЕ является примером потенциальных целей для кибератак? a) Банковские аккаунты b) Данные пользователей c) Локальные сети d) Мобильные приложения	ОПК-6.1
64.	b) Изучение криминалистических доказательств, полученных из цифровых устройств и	Что такое "форензический анализ"? a) Исследование документов и файлов, находящихся на сервере b) Изучение криминалистических	ОПК-6.1

	систем.	доказательств, полученных из цифровых устройств и систем c) Процесс взлома учетной записи пользователя d) Метод поиска источников вредоносных программ на веб-сайтах	
65.	a) Метод защиты от атак, которые используют множество устройств для отправки трафика на один веб-сервер.	Что такое "защита от DDoS-атак"? a) Метод защиты от атак, которые используют множество устройств для отправки трафика на один веб-сервер b) Метод защиты от атак, при которых злоумышленники пытаются получить доступ к системе путем перебора паролей c) Метод защиты от атак, при которых злоумышленники пытаются перехватить данные, передаваемые между клиентом и сервером d) Метод защиты от атак, при которых злоумышленники используют вредоносные программы, которые перехватывают данные на компьютере пользователя	ОПК-6.1
66.	b) Расследование, проводимое внутри компании или организации	Что такое "внутреннее расследование"? a) Расследование, проводимое правоохранительными органами b) Расследование, проводимое внутри компании или организации c) Расследование, проводимое в отношении иностранных агентов d) Расследование, проводимое по поводу проблем с безопасностью внешней среды.	ОПК-6.1
67.	d) Метод похищения финансовых данных пользователей, который часто используется в отношении банковских карт.	Что такое "скимминг"? a) Метод защиты от взлома посредством перебора паролей b) Метод защиты от атаки DDoS c) Метод защиты от вредоносных программ, которые перехватывают данные на компьютере пользователя d) Метод похищения финансовых данных пользователей, который часто используется в отношении банковских карт	ОПК-6.1
68.	c) Вредоносная программа, которая позволяет злоумышленникам получить удаленный доступ к зараженному устройству.	Что такое "бекдор"? a) Вредоносная программа, предназначенная для перехвата данных, передаваемых между клиентом и сервером b) Вредоносная программа, которая перехватывает управление над компьютером пользователя c) Вредоносная программа, которая позволяет злоумышленникам получить удаленный доступ к зараженному устройству d) Вредоносная программа, которая шифрует данные на компьютере пользователя и требует выкупа для их восстановления	ОПК-6.1
69.	a) Совокупность фактов и данных, которые свидетельствуют о том, что преступление было совершено.	Что такое "цепочка доказательств"? a) Совокупность фактов и данных, которые свидетельствуют о том, что преступление было совершено b) Метод, позволяющий защититься от кибератак путем создания нескольких слоев защиты c) Метод, позволяющий противостоять вредоносным программам, которые используют социальную инженерию для	ОПК-6.1

		получения доступа к учетной записи пользователя d) Система мер, которые позволяют защитить конфиденциальную информацию от несанкционированного доступа	

2. Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Рейтинговая система оценки знаний студентов основана на использовании совокупности контрольных мероприятий по проверке пройденного материала (контрольных точек), оптимально расположенных на всем временном интервале изучения дисциплины. Принципы рейтинговой системы оценки знаний студентов основываются на требованиях, описанных в Положении об организации образовательного процесса на основе рейтинговой системы оценки знаний студентов в ФГАОУ ВО «СКФУ».

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:

- знает полностью понятия математической логики, теории дискретных функций и теории алгоритмов, а также возможности применения общих логических принципов в математике и профессиональной деятельности; язык и средства современной математической логики и теории логических исчислений; основные способы задания булевых функций и функций многозначной логики формулами и их свойства; различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов
- умеет полностью производить основные логические операции в исчислении высказываний и исчислении предикатов; находить и исследовать свойства представлений булевых и многозначных функций формулами в различных базисах; оценивать сложность алгоритмов и вычислений; применять методы атематической логики и теории алгоритмов к решению задач математической кибернетики
- владеет полностью навыками использования языка современной символической логики; навыками упрощения формул алгебры высказываний и алгебры предикатов; навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач

Оценка «хорошо» выставляется, если студент:

- знает на хорошем уровне понятия математической логики, теории дискретных функций и теории алгоритмов, а также возможности применения общих логических принципов в математике и профессиональной деятельности; язык и средства современной математической логики и теории логических исчислений; основные способы задания булевых функций и функций многозначной логики формулами и их свойства; различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов
- умеет на хорошем уровне производить основные логические операции в исчислении высказываний и исчислении предикатов; находить и исследовать свойства представлений булевых и многозначных функций формулами в различных базисах; оценивать сложность алгоритмов и вычислений; применять методы атематической логики и теории алгоритмов к решению задач математической кибернетики
- владеет на хорошем уровне навыками использования языка современной символической логики; навыками упрощения формул алгебры высказываний и алгебры

предикатов; навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач

Оценка «удовлетворительно» выставляется, если студент:

- знает понятия математической логики, теории дискретных функций и теории алгоритмов, а также возможности применения общих логических принципов в математике и профессиональной деятельности; язык и средства современной математической логики и теории логических исчислений; основные способы задания булевых функций и функций многозначной логики формулами и их свойства; различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов
- в основном, умеет производить основные логические операции в исчислении высказываний и исчислении предикатов; находить и исследовать свойства представлений булевых и многозначных функций формулами в различных базисах; оценивать сложность алгоритмов и вычислений; применять методы атематической логики и теории алгоритмов к решению задач математической кибернетики
- в основном, навыками использования языка современной символической логики; навыками упрощения формул алгебры высказываний и алгебры предикатов; навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач

Оценка «неудовлетворительно» выставляется, если студент:

- знает не все понятия математической логики, теории дискретных функций и теории алгоритмов, а также возможности применения общих логических принципов в математике и профессиональной деятельности; язык и средства современной математической логики и теории логических исчислений; основные способы задания булевых функций и функций многозначной логики формулами и их свойства; различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов
- недостаточно умеет производить основные логические операции в исчислении высказываний и исчислении предикатов; находить и исследовать свойства представлений булевых и многозначных функций формулами в различных базисах; оценивать сложность алгоритмов и вычислений; применять методы атематической логики и теории алгоритмов к решению задач математической кибернетики
- слабо владеет навыками использования языка современной символической логики; навыками упрощения формул алгебры высказываний и алгебры предикатов; навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач