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
Т.А. Гробова.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Технологии выявления следов компьютерных преступлений и инцидентов

Направление подготовки	10.04.01 Информационная безопасность
Направленность (профиль)	Математическое и программное обеспечение защиты информации
Форма обучения	очная
Год начала обучения	2026
Реализуется в 3 семестре	

Введение

1. Назначение: обеспечение методической основы для организации и проведения текущего контроля по дисциплине «Технологии выявления следов компьютерных преступлений 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 и инцидентов»

3. Разработчик: 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., кандидат экономических наук, главный аналитик ФБУ «Северо-Кавказского регионального центра судебной экспертизы Министерства юстиции РФ» ФГБУ Кабардино-Балкарской лаборатории судебной экспертизы Министерства юстиции Российской Федерации.

Экспертное заключение: Представленный ФОС по дисциплине «Технологии выявления следов компьютерных преступлений и инцидентов» соответствует требованиям ФГОС ВО. Предлагаемые преподавателем формы и средства текущего контроля адекватны целям и задачам реализации образовательной программы высшего образования по направлению 10.04.01 Информационная безопасность направленность (профиль) «Математическое и программное обеспечение защиты информации», 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
ИД-1 ПК-4 определяет свойства аппаратных средств в составе компьютерной системы и их фактического и первоначального состояния, классифицирует свойств аппаратных средств в составе компьютерной системы	Предоставляет с грубыми ошибками отчёт по определению свойств аппаратных средств в составе компьютерной системы и их фактического и первоначального состояния, классифицирует свойств аппаратных средств в составе компьютерной системы	Предоставляет частичный отчёт по определению свойств аппаратных средств в составе компьютерной системы и их фактического и первоначального состояния, классифицирует свойств аппаратных средств в составе компьютерной системы	Предоставляет отчёт по определению свойств аппаратных средств в составе компьютерной системы и их фактического и первоначального состояния, классифицирует свойств аппаратных средств в составе компьютерной системы	Предоставляет детальный отчёт по определению свойств аппаратных средств в составе компьютерной системы и их фактического и первоначального состояния, классифицирует свойств аппаратных средств в составе компьютерной системы
ИД-2 ПК-4 проводит диагностику причины, условия изменения свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы, определяет характеристики операционной системы и используемых технологий системного программирования	Предоставляет с грубыми ошибками отчёт по результатам диагностики причины, условия изменения свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы, определяет характеристики операционной системы и используемых технологий системного программирования	Предоставляет частичный отчёт по результатам диагностики причины, условия изменения свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы, определяет характеристики операционной системы и используемых технологий системного программирования	Предоставляет отчёт по результатам диагностики причины, условия изменения свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы, определяет характеристики операционной системы и используемых технологий системного программирования	Предоставляет детальный отчёт по результатам диагностики причины, условия изменения свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы, определяет характеристики операционной системы и используемых технологий системного программирования
ИД-3 ПК-4 выявляет индивидуальные признаки программы, позволяющие впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой	Предоставляет с грубыми ошибками отчёт по результатам выявления индивидуальных признаков программы, позволяющие впоследствии идентифицировать ее автора, а также	Предоставляет частичный отчёт по результатам выявления индивидуальных признаков программы, позволяющие впоследствии идентифицировать ее автора, а также взаимосвязи с	Предоставляет отчёт по результатам выявления индивидуальных признаков программы, позволяющие впоследствии идентифицировать ее автора, а также	Предоставляет детальный отчёт по результатам выявления индивидуальных признаков программы, позволяющие впоследствии идентифицировать ее автора, а также взаимосвязи с

компьютерной системы	взаимосвязи с информационным обеспечением исследуемой компьютерной системы	информационным обеспечением исследуемой компьютерной системы	взаимосвязи с информационным обеспечением исследуемой компьютерной системы	информационным обеспечением исследуемой компьютерной системы
ИД-4 ПК-4 определяет механизмы, динамики и обстоятельств события по имеющейся информации на носителе данных или ее копиям	Предоставляет с грубыми ошибками отчёт по результатам определения механизмов, динамики и обстоятельств события по имеющейся информации на носителе данных или ее копиям	Предоставляет частичный отчёт по результатам определения механизмов, динамики и обстоятельств события по имеющейся информации на носителе данных или ее копиям	Предоставляет отчёт по результатам определения механизмов, динамики и обстоятельств события по имеющейся информации на носителе данных или ее копиям	Предоставляет детальный отчёт по результатам определения механизмов, динамики и обстоятельств события по имеющейся информации на носителе данных или ее копиям
ИД-5 ПК-4 устанавливает участников события, их роли, места, условий, при которых была создана, модифицирована или удалена информация, устанавливает соответствия либо несоответствие действий с информацией специальному регламенту (правилам)	Предоставляет с грубыми ошибками отчёт по результатам установления участников события, их ролей, места, условий, при которых была создана, модифицирована или удалена информация, установления соответствия либо несоответствия действий с информацией специальному регламенту (правилам)	Предоставляет частичный отчёт по результатам установления участников события, их ролей, места, условий, при которых была создана, модифицирована или удалена информация, установления соответствия либо несоответствия действий с информацией специальному регламенту (правилам)	Предоставляет отчёт по результатам установления участников события, их ролей, места, условий, при которых была создана, модифицирована или удалена информация, установления соответствия либо несоответствия действий с информацией специальному регламенту (правилам)	Предоставляет детальный отчёт по результатам установления участников события, их ролей, места, условий, при которых была создана, модифицирована или удалена информация, установления соответствия либо несоответствия действий с информацией специальному регламенту (правилам)
ИД-1 ПК-5 формализует задачи автоматизированной информационно-аналитической поддержки процессов принятия решений в сфере безопасности в конкретной предметной области	Предоставляет с грубыми отчетами отчёт по формализованным задачам автоматизированной информационно-аналитической поддержки процессов принятия решений в сфере безопасности в конкретной предметной области	Предоставляет частичный отчёт по формализованным задачам автоматизированной информационно-аналитической поддержки процессов принятия решений в сфере безопасности в конкретной предметной области	Предоставляет отчёт по формализованным задачам автоматизированной информационно-аналитической поддержки процессов принятия решений в сфере безопасности в конкретной предметной области	Предоставляет детальный отчёт по формализованным задачам автоматизированной информационно-аналитической поддержки процессов принятия решений в сфере безопасности в конкретной предметной области
ИД-2 ПК-5 решает задачи прогнозирования, планирования, выработки решений при различной	Предоставляет с грубыми ошибками отчет по решению задач прогнозирования, планирования,	Предоставляет частичный отчет по решению задач прогнозирования, планирования, выработки решений	Предоставляет отчет по решению задач прогнозирования, планирования, выработки	Предоставляет детальный отчет по решению задач прогнозирования, планирования, выработки

априорной неопределенности имеющейся информации	выработки решений при различной априорной неопределенности имеющейся информации.	при различной априорной неопределенности имеющейся информации.	решений при различной априорной неопределенности имеющейся информации.	решений при различной априорной неопределенности имеющейся информации.
ИД-3 ПК-5 оценивает эффективность и качество в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации	Предоставляет с грубыми ошибками отчет по оценке эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации	Предоставляет частичный отчет по оценке эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации	Предоставляет отчет по оценке эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации	Предоставляет детальный отчет по оценке эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации

Оценочные средства для проверки уровня сформированности компетенций
9 семестр

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
1.		Что такое компьютерная криминалистика?	ПК-4
2.		Что такое цифровые доказательства?	ПК-4
3.		Какие типы цифровых доказательств существуют?	ПК-4
4.		Каковы преимущества использования цифровых доказательств в компьютерной криминалистике?	ПК-4
5.		Что такое судебно-техническая экспертиза?	ПК-4
6.		Какие типы судебно-технических экспертиз существуют в компьютерной криминалистике?	ПК-4
7.		Что такое цифровые улики?	ПК-4
8.		Каким образом можно изъять цифровые улики?	ПК-4
9.		Что такое сетевая атака?	ПК-4
10.		Что такое сканирование портов?	ПК-4
11.		Что такое блокчейн?	ПК-4
12.		Что такое криптовалюта?	ПК-4
13.		Что такое цифровая подпись?	ПК-4
14.		Какие типы данных могут быть восстановлены при анализе цифровых улик?	ПК-4
15.		Что такое сниффер?	ПК-4
16.		Что такое DDoS-атака?	ПК-4

17.		Какие методы использования социальных сетей могут быть использованы в качестве доказательств?	ПК-4
18.		Что такое криптография?	ПК-4
19.		Какие типы криптографии используются в компьютерной криминалистике?	ПК-4
20.		Что такое вредоносное ПО?	ПК-4
21.		Что такое кибершпионаж?	ПК-4
22.		Как можно определить, была ли проведена DDoS-атака?	ПК-4
23.		Что такое виртуальная машина?	ПК-4
24.		Какие инструменты используются для анализа цифровых улик?	ПК-4
25.		Что такое стеганография?	ПК-4
26.		Как можно защитить компьютерную систему от кибератак?	ПК-4
27.		Компьютерная криминалистика.	ПК-4
28.		Что такое "цифровая подпись"?	ПК-4
29.		Какой тип кибератаки основан на использовании вредоносных программ?	ПК-4
30.		Какой тип кибератаки основан на перехвате информации, передаваемой по сети?	ПК-4
31.		Какой тип кибератаки направлен на блокирование доступа к компьютерной системе?	ПК-5
32.		Какие типы криптографии используются в компьютерной криминалистике?	ПК-5
33.		Что такое вредоносное ПО?	ПК-5
34.		Какими методами можно обнаружить вредоносное ПО?	ПК-5
35.		Что такое доказательства в цепочке?	ПК-5
36.		Что такое киберпреступность?	ПК-5
37.		Что такое компьютерное преступление?	ПК-5
38.		Какие виды компьютерных преступлений существуют?	ПК-5
39.		Что такое цифровой след?	ПК-5
40.		Какие основные задачи расследования компьютерных преступлений?	ПК-5
41.		Что такое журнал безопасности?	ПК-5
42.		Какие данные могут содержаться в журнале безопасности?	ПК-5
43.		Что такое хеш-сумма?	ПК-5

44.		Зачем используется хеш-сумма при расследовании компьютерных преступлений?	ПК-5
45.		Какие виды цифровых следов бывают?	ПК-5
46.		Что такое активный цифровой след?	ПК-5
47.		Что такое пассивный цифровой след?	ПК-5
48.		Что такое прямой цифровой след?	ПК-5
49.		Что такое косвенный цифровой след?	ПК-5
50.		Какие инструменты используются для сбора цифровых следов?	ПК-5
51.		Что такое методология сбора данных при расследовании компьютерных преступлений?	ПК-5
52.		Какие этапы включает методология сбора данных при расследовании компьютерных преступлений?	ПК-5
53.		Что такое хеш-сумма?	ПК-5
54.		Зачем используется хеш-сумма в расследовании компьютерных преступлений?	ПК-5
55.		Какие программные инструменты используются при сборе и анализе данных в расследовании компьютерных преступлений?	ПК-5
56.		Что такое кросс-доменная атака?	ПК-5
57.		Что такое SQL-инъекция?	ПК-5
58.		Что такое DDoS-атака?	ПК-5
59.		Какие меры безопасности можно предпринять для защиты от DDoS-атак?	ПК-5
60.		Что такое сетевой протокол?	ПК-5
61.	Wireshark, tcpdump, Snort и другие	Какие инструменты могут использоваться для анализа сетевых протоколов при расследовании компьютерных преступлений?	ПК-5
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	ПК-5
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	ПК-5
64.	b) Изучение криминалистических доказательств, полученных из цифровых устройств и систем.	Что такое "форензический анализ"? a) Исследование документов и файлов, находящихся на сервере b) Изучение криминалистических доказательств, полученных из цифровых	ПК-5

		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	ПК-5
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.	ПК-5
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	ПК-5
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	ПК-5
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 получения доступа к учетной записи	ПК-5

		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.

2. 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