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
«Компьютерная криминалистика»

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 «Компьютерная криминалистика». 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 «Компьютерная криминалистика»

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: УК-10				
Результаты обучения по дисциплине (модулю): Индикатор: ИУК-10.1, УК-10. Формулирует цель проекта, определяет совокупность взаимосвязанных задач, обеспечивающих ее достижение и определяет ожидаемые результаты решения задач.	Не предоставляет отчет в котором демонстрирует понимание механизмов распространения противоправного контента в информационно-телекоммуникационной сети, в том числе экстремистского и террористического характера; может анализировать цифровые следы, указывающие на признаки деструктивной деятельности в сети.	Предоставляет неполный отчет с неполным пояснением в котором демонстрирует понимание механизмов распространения противоправного контента в информационно-телекоммуникационной сети, в том числе экстремистского и террористического характера; может анализировать цифровые следы, указывающие на признаки деструктивной деятельности в сети.	Предоставляет отчет с пояснением в котором демонстрирует понимание механизмов распространения противоправного контента в информационно-телекоммуникационной сети, в том числе экстремистского и террористического характера; может анализировать цифровые следы, указывающие на признаки деструктивной деятельности в сети.	Предоставляет детальный отчет с полным пояснением в котором демонстрирует понимание механизмов распространения противоправного контента в информационно-телекоммуникационной сети, в том числе экстремистского и террористического характера; может анализировать цифровые следы, указывающие на признаки деструктивной деятельности в сети.
ИУК-10.2, УК-10. Умеет применять правовые нормы, обеспечивающие противодействие экстремизму, терроризму, коррупции и	Не предоставляет отчет в котором уверенно ориентируется в нормативно-	Предоставляет неполный отчет с неполным пояснением в котором уверенно ориентируется	Предоставляет отчет с пояснением в котором уверенно ориентируется в нормативно-	Предоставляет детальный отчет с полным пояснением в котором уверенно ориентируется в нормативно-

профилактику их проявлений в сфере профессиональной деятельности	правовой базе по вопросам противодействия ИТ-преступлениям; способен применять положения УК РФ, КоАП РФ, ФЗ №114-ФЗ (о противодействии экстремистской деятельности) и иных актов при анализе цифровых доказательств и составлении экспертных заключений.	в нормативно-правовой базе по вопросам противодействия ИТ-преступлениям; способен применять положения УК РФ, КоАП РФ, ФЗ №114-ФЗ (о противодействии экстремистской деятельности) и иных актов при анализе цифровых доказательств и составлении экспертных заключений.	правовой базе по вопросам противодействия ИТ-преступлениям; способен применять положения УК РФ, КоАП РФ, ФЗ №114-ФЗ (о противодействии экстремистской деятельности) и иных актов при анализе цифровых доказательств и составлении экспертных заключений.	правовой базе по вопросам противодействия ИТ-преступлениям; способен применять положения УК РФ, КоАП РФ, ФЗ №114-ФЗ (о противодействии экстремистской деятельности) и иных актов при анализе цифровых доказательств и составлении экспертных заключений.
ИУК-10.3, УК-10. Владеет средствами формирования нетерпимого отношения к проявлениям экстремизма, терроризма и коррупционного поведения, и противодействия им в профессиональной деятельности	Не предоставляет отчет в котором готов к участию в профилактической и аналитической деятельности, направленной на выявление и пресечение противоправной активности в цифровой среде; осознаёт профессиональную и гражданскую ответственность при работе с информацией, имеющей признаки экстремизма или коррупции.	Предоставляет неполный отчет с неполным пояснением в котором готов к участию в профилактической и аналитической деятельности, направленной на выявление и пресечение противоправной активности в цифровой среде; осознаёт профессиональную и гражданскую ответственность при работе с информацией, имеющей признаки экстремизма или коррупции.	Предоставляет отчет с пояснением в котором готов к участию в профилактической и аналитической деятельности, направленной на выявление и пресечение противоправной активности в цифровой среде; осознаёт профессиональную и гражданскую ответственность при работе с информацией, имеющей признаки экстремизма или коррупции.	Предоставляет детальный отчет с полным пояснением в котором готов к участию в профилактической и аналитической деятельности, направленной на выявление и пресечение противоправной активности в цифровой среде; осознаёт профессиональную и гражданскую ответственность при работе с информацией, имеющей признаки экстремизма или коррупции.

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 научная дисциплина, занимающаяся сбором, анализом и сохранением цифровых доказательств с электронных устройств и цифровых носителей для использования в суде или в ходе расследования.	Что такое компьютерная криминалистика?	УК -10
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?	УК -10
3.	Типы цифровых доказательств включают электронные письма, сообщения, фотографии, видео,	Какие типы цифровых доказательств существуют?	УК -10

	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?	УК -10
5.	Судебно-техническая экспертиза — это исследование цифровых устройств и их содержимого для восстановления информации, идентификации пользователей и анализа данных.	Что такое судебно-техническая экспертиза?	УК -10
6.	Типы судебно-технических экспертиз включают компьютерную экспертизу, сетевую экспертизу, судебный анализ данных и экспертизу мобильных	Какие типы судебно-технических экспертиз существуют в компьютерной криминалистике?	УК -10

	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?	УК -10
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?	УК -10
9.	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?	УК -10
10.	Криптография — это наука об обеспечении конфиденциальности и целостности информации путём	Что такое криптография?	УК -10

	использования криптографических методов и алгоритмов.		
11.	В компьютерной криминалистике используются два типа криптографии: симметричная и асимметричная.	Какие типы криптографии используются в компьютерной криминалистике?	УК -10
12.	Вредоносное ПО — это программное обеспечение, предназначенное для нанесения ущерба или нарушения работы компьютерных систем и сетей.	Что такое вредоносное ПО?	УК -10
13.	Кибершпионаж — это незаконное получение конфиденциальной информации с использованием компьютерных технологий.	Что такое кибершпионаж?	УК -3
14.	Исследование компьютерной техники при криминалистической экспертизе производится с помощью различных методов и оборудования, таких как	Как производится исследование компьютерной техники при криминалистической экспертизе?	УК -3

	анализаторы протоколов, логические анализаторы, сканеры портов и другие инструменты.		
15.	Предмет посягательства при компьютерных преступлениях — это компьютерная информация, которая может включать сведения, сообщения и данные, представленные в форме электрических сигналов.	Предмет посягательства при компьютерных преступления	УК -3
16.	Способы совершения компьютерных преступлений включают кражу компьютерной техники, перехват информации, несанкционированный доступ к информации, манипуляцию данными и управляющими командами, компьютерный саботаж и комплексные методы.	Дайте описание способов совершения компьютерного преступления	УК -3
17.	Личность вероятного компьютерного преступника может быть связана с	Какова личность вероятного компьютерного преступника ивероятные его мотивы?	УК -3

	хакерами, киберпреступниками или лицами, совершающими преступления в сфере компьютерной информации. Их мотивы могут быть связаны с получением прибыли, местью, желанием привлечь внимание или другими причинами.		
18.	Личность вероятного компьютерного потерпевшего может быть связана с организациями или частными лицами, чьи данные или системы были взломаны или повреждены в результате компьютерных преступлений.	Какова личность вероятного компьютерного потерпевшего от компьютерных преступлений?	УК -3
19.	Механизмы образования компьютерных следов могут включать изменение настроек системы, удаление или перемещение файлов, создание новых	Какие бывают механизмы образования компьютерных следов?	УК -3

	учётных записей или использование скрытых процессов.		
20.	Обстановка при совершении компьютерных преступлений может быть связана с использованием интернета, специализированных магазинов компьютерных программ или других мест, где можно приобрести или использовать вредоносное программное обеспечение. Типичные обстоятельства могут включать использование анонимных или фальшивых личностей, использование уязвимостей систем и сетей, а также сокрытие следов преступления.	Какими бывают обстановка и другие типичные обстоятельства при совершении компьютерных преступлений	УК -3

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 «отлично» выставляется студенту, если он, предоставляет детальный отчет с полным пояснением в котором демонстрирует понимание механизмов распространения противоправного контента в информационно-телекоммуникационной сети, в том числе экстремистского и террористического характера; может анализировать цифровые следы, указывающие на признаки деструктивной деятельности в сети. Предоставляет детальный отчет с полным пояснением в котором уверенно ориентируется в нормативно-правовой базе по вопросам противодействия ИТ-преступлениям; способен применять положения УК РФ, КоАП РФ, ФЗ №114-ФЗ (о противодействии экстремистской деятельности) и иных актов при анализе цифровых доказательств и составлении экспертных заключений. Предоставляет детальный отчет с полным пояснением в котором готов к участию в профилактической и аналитической деятельности, направленной на выявление и пресечение противоправной активности в цифровой среде; осознаёт профессиональную и гражданскую ответственность при работе с информацией, имеющей признаки экстремизма или коррупции.

Оценка «хорошо» выставляется студенту, если он предоставляет отчет с пояснением в котором демонстрирует понимание механизмов распространения противоправного контента в информационно-телекоммуникационной сети, в том числе экстремистского и террористического характера; может анализировать цифровые следы, указывающие на признаки деструктивной деятельности в сети. Предоставляет отчет с пояснением в котором уверенно ориентируется в нормативно-правовой базе по вопросам противодействия ИТ-преступлениям; способен применять положения УК РФ, КоАП РФ, ФЗ №114-ФЗ (о противодействии экстремистской деятельности) и иных актов при анализе цифровых доказательств и составлении экспертных заключений. Предоставляет отчет с пояснением в котором готов к участию в профилактической и аналитической деятельности, направленной на выявление и пресечение противоправной активности в цифровой среде; осознаёт профессиональную и гражданскую ответственность при работе с информацией, имеющей признаки экстремизма или коррупции.

Оценка «удовлетворительно» выставляется студенту, если он предоставляет неполный отчет с неполным пояснением в котором демонстрирует понимание механизмов распространения противоправного контента в информационно-телекоммуникационной сети, в том числе экстремистского и террористического характера; может анализировать цифровые следы, указывающие на признаки деструктивной деятельности в сети.

Предоставляет неполный отчет с неполным пояснением в котором уверенно ориентируется в нормативно-правовой базе по вопросам противодействия ИТ-преступлениям; способен применять положения УК РФ, КоАП РФ, ФЗ №114-ФЗ (о противодействии экстремистской деятельности) и иных актов при анализе цифровых доказательств и составлении экспертных заключений.

Предоставляет неполный отчет с неполным пояснением в котором готов к участию в профилактической и аналитической деятельности, направленной на выявление и пресечение противоправной активности в цифровой среде; осознаёт профессиональную и гражданскую ответственность при работе с информацией, имеющей признаки экстремизма или коррупции.

Оценка «не удовлетворительно» выставляется студенту, если он не предоставляет отчет в котором демонстрирует понимание механизмов распространения противоправного контента в информационно-телекоммуникационной сети, в том числе экстремистского и

террористического характера; может анализировать цифровые следы, указывающие на признаки деструктивной деятельности в сети. Не предоставляет отчет в котором уверенно ориентируется в нормативно-правовой базе по вопросам противодействия ИТ-преступлениям; способен применять положения УК РФ, КоАП РФ, ФЗ №114-ФЗ (о противодействии экстремистской деятельности) и иных актов при анализе цифровых доказательств и составлении экспертных заключений. Не предоставляет отчет в котором готов к участию в профилактической и аналитической деятельности, направленной на выявление и пресечение противоправной активности в цифровой среде; осознаёт профессиональную и гражданскую ответственность при работе с информацией, имеющей признаки экстремизма или коррупции.