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: 19.06.2026 15:10:47
Уникальный программный ключ:
bd39d4208aa94cf4422feb787c81619d42de79a7

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
«Анализ данных в кибербезопасности»

Направление подготовки	02.04.01 Математика и компьютерные науки
Профиль	Искусственный интеллект в кибербезопасности
Год начала обучения	2026
Форма обучения	очная
Реализуется в 3 семестре	

Введение

1. Назначение: Фонд оценочных средств предназначен для обеспечения методической основы для организации и проведения текущего контроля по дисциплине «Анализ данных в кибербезопасности». 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 «Анализ данных в кибербезопасности»

3. Разработчик: 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 направлению подготовки 02.04.01 Математика и компьютерные науки профиль «Искусственный интеллект в кибербезопасности» 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-6 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений				
Результаты обучения по дисциплине (модулю): *Индикатор: ИД-1. УК-6.* устанавливает личные и профессиональные цели в соответствии с уровнем своих ресурсов и приоритетов действий, для успешного развития в избранной сфере профессиональной деятельности.	Не формулирует цель проекта, создает паспорт проекта с грубыми нарушениями	Формулирует цель проекта, создает паспорт проекта с грубыми нарушениями	Формулирует цель проекта, создает паспорт проекта с нарушениями	в полном объёме ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов
ИД-2. УК-6. реализует и корректирует стратегию личностного и профессионального развития, с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда	С ошибками разрабатывает план действий по управлению проектом на всех этапах его жизненного цикла, не учитывает все действующие правовые нормы и имеющиеся ресурсы и ограничений, не может создать портфолио проекта	С ошибками разрабатывает план действий по управлению проектом на всех этапах его жизненного цикла, не учитывает все действующие правовые нормы и имеющиеся ресурсы и ограничений создает портфолио проекта с ошибками	С ошибками разрабатывает план действий по управлению проектом на всех этапах его жизненного цикла, исходя из действующих правовых норм и имеющихся ресурсов и ограничений создает портфолио проекта	в полном объёме выбирает эффективные стратегии и тактики личностного и профессионального развития, методики оценки эффективности применяемых методов решения поставленных задач в сфере своей профессиональной деятельности
Компетенция: ПК-2 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде				

Результаты обучения по дисциплине (модулю): *Индикатор: ИД-1. ПК-2.* Проводит научные исследования в области параллельных компьютерных технологий.	Не проводит научные исследования в области параллельных компьютерных технологий.	С трудом проводит научные исследования в области параллельных компьютерных технологий.	С ошибками проводит научные исследования в области параллельных компьютерных технологий.	Проводит научные исследования в области параллельных компьютерных технологий
ИД-2. ПК-2 Проводит рецензирование научных статей и авторефератов и диссертаций по математическим и информационным направлениям	Не проводит рецензирование научных статей и авторефератов и диссертаций по математическим и информационным направлениям	С трудом проводит рецензирование научных статей и авторефератов и диссертаций по математическим и информационным направлениям	С ошибками проводит рецензирование научных статей и авторефератов и диссертаций по математическим и информационным направлениям	Проводит рецензирование научных статей и авторефератов, и диссертаций по математическим и информационным направлениям

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.	Мир кибербезопасности сосредоточен на защите компьютерных систем, сетей и данных от несанкционированного доступа, атак и повреждений. Он включает в себя различные практики, технологии и процессы, направленные на предотвращение киберугроз, таких как вирусы, фишинг и атаки нулевого дня. В условиях постоянного роста цифровых технологий кибербезопасность становится критически важной для обеспечения конфиденциальности и целостности информации.	Мир кибербезопасности	УК -6 ПК-2
2.	Киберпреступники используют свои навыки для совершения незаконных действий в	Киберпреступники и специалисты по кибербезопасности	УК -6 ПК-2

	цифровом пространстве, таких как хищение данных, распространение вредоносного ПО и финансовые мошенничества. Специалисты по кибербезопасности, наоборот, работают над защитой систем и сетей, разрабатывая стратегии и инструменты для предотвращения атак и минимизации рисков. Эта борьба между преступниками и защитниками постоянно эволюционирует, что требует от специалистов постоянного обновления знаний и навыков.		
3.	Типовые угрозы в кибербезопасности включают вирусы и вредоносное ПО, которые могут повреждать или красть данные, фишинг, направленный на обман пользователей для	Типовые угрозы	УК -6 ПК-2

	получения конфиденциальной информации, и атаки распределенного отказа в обслуживании (DDoS), которые перегружают системы и делают их недоступными. Также важными угрозами являются утечки данных и атаки на сети, которые могут привести к серьезным финансовым и репутационным потерям. Понимание этих угроз помогает организациям лучше защищать свои активы и информацию.		
4.	Распространение киберугроз происходит через различные каналы, включая электронную почту, вредоносные веб-сайты и социальные сети, где злоумышленники могут использовать фишинг и социальную инженерию для обмана пользователей. Также	Распространение киберугроз	УК -6 ПК-2

	киберугрозы могут распространяться через уязвимости в программном обеспечении и сетях, что позволяет злоумышленникам получать доступ к системам и данным. Эффективная защита требует постоянного мониторинга и обновления систем безопасности.		
5.	Три измерения куба кибербезопасности включают технологии, процессы и людей. Технологии представляют собой инструменты и системы, которые защищают информацию, процессы охватывают политики и процедуры, обеспечивающие безопасность, а люди — это сотрудники и пользователи, ответственные за соблюдение норм безопасности. Все три	Три измерения куба кибербезопасности	УК -6 ПК-2

	измерения должны работать в гармонии для создания эффективной стратегии кибербезопасности.		
6.	Конфиденциальность, целостность и доступность — это три ключевых принципа кибербезопасности, известные как "триаду CIA". Конфиденциальность обеспечивает защиту информации от несанкционированного доступа, целостность гарантирует, что данные остаются неизменными и достоверными, а доступность обеспечивает возможность доступа к данным и системам для авторизованных пользователей. Соблюдение этих принципов помогает защитить информацию и поддерживать доверие пользователей.	Конфиденциальность, целостность, доступность	УК -6 ПК-2
7.	Состояния данных	Состояния данных	УК -6

	относятся к различным этапам, через которые проходят данные в процессе их обработки и хранения. Основные состояния включают "в покое" (данные хранятся на устройствах), "в движении" (данные передаются по сети) и "в использовании" (данные обрабатываются приложениями). Понимание этих состояний помогает обеспечить адекватную защиту данных на каждом этапе их жизненного цикла.		ПК-2
8.	Вредоносное ПО (или malware) — это программное обеспечение, созданное для нанесения вреда компьютерам, сетям или пользователям, включая вирусы, черви и трояны. Вредоносный код — это общее понятие, охватывающее любые вредоносные	Вредоносное ПО и вредоносный код	УК -6 ПК-2

	инструкции или скрипты, которые могут быть внедрены в программы или веб-сайты для выполнения вредоносных действий. Оба типа представляют серьезную угрозу для безопасности данных и систем.		
9.	Искусство и методы обмана относятся к техникам, которые злоумышленники используют для обхода систем защиты и маскировки своих действий. Это включает в себя фальсификацию данных, использование социальных манипуляций и создание поддельных идентификаций. Понимание этих методов позволяет специалистам по кибербезопасности более эффективно выявлять угрозы и защищать системы.	Искусство и методы обмана	УК -6 ПК-2
10.	Атаки могут включать различные методы,	Атаки	УК -6 ПК-2

	такие как фишинг, атаки с использованием вредоносного ПО и DDoS-атаки, направленные на уничтожение или компрометацию данных. Эти атаки часто используют уязвимости в системах и человеческий фактор для достижения своих целей. Эффективный анализ данных помогает выявлять и предотвращать такие угрозы, защищая организации от потенциальных потерь.		
11.	Криптография — это наука о защите информации с помощью математических методов, обеспечивающая конфиденциальность, целостность и аутентичность данных. Она включает в себя техники шифрования, которые преобразуют информацию в неразборчивый формат,	Криптография	УК -6 ПК-2

	доступный только тем, кто обладает соответствующим ключом. Криптография играет ключевую роль в обеспечении безопасности коммуникаций в цифровом мире.		
12.	Функции управления доступом обеспечивают контроль за тем, кто может получать доступ к ресурсам и информации в системе. Они включают аутентификацию пользователей, авторизацию прав доступа и мониторинг активности, что помогает предотвратить несанкционированный доступ и утечку данных. Эффективное управление доступом является ключевым элементом кибербезопасности и защиты конфиденциальной информации.	Функции управления доступом	УК -6 ПК-2
13.	Скрытие данных — это	Скрытие данных	УК -6

	процесс защиты конфиденциальной информации путем ее преобразования в неразборчивый формат или удаления из доступных источников. Это может включать методы, такие как шифрование, а также использование анонимизации или маскирования данных, чтобы предотвратить несанкционированный доступ и утечку информации. Скрытие данных играет важную роль в обеспечении безопасности и соблюдении требований законодательства о защите данных.		ПК-2
14.	Средства контроля целостности данных включают хэш-функции, контрольные суммы и цифровые подписи. Хэш-функции создают уникальный код для каждого набора данных, позволяя обнаружить изменения,	Виды средств контроля целостности	УК -6 ПК-2

	тогда как контрольные суммы используются для проверки целостности данных при передаче. Цифровые подписи обеспечивают проверку подлинности и целостности данных, гарантируя, что они не были изменены после подписания.		
15.	Цифровые подписи — это криптографический метод, который используется для подтверждения подлинности и целостности электронных документов. Они создаются с помощью закрытого ключа отправителя и могут быть проверены с использованием соответствующего открытого ключа, что позволяет удостовериться, что документ не был изменен и действительно исходит	Цифровые подписи	УК -6 ПК-2

	от указанного отправителя. Цифровые подписи играют важную роль в обеспечении безопасности электронных транзакций и коммуникаций.		
16.	Обеспечение целостности данных включает в себя методы и технологии, которые гарантируют, что информация не была изменена или повреждена в процессе хранения или передачи. Это достигается с помощью различных средств контроля, таких как хэш-функции, контрольные суммы и цифровые подписи. Эти меры помогают выявлять несанкционированные изменения и обеспечивают доверие к данным в различных системах и приложениях.	Обеспечение целостности данных	УК -6 ПК-2
17.	Высокая доступность	Высокая доступность ресурсов	УК -6

	ресурсов означает, что системы и приложения обеспечивают минимальное время простоя и максимальную доступность для пользователей. Это достигается за счет использования резервирования, кластеризации и распределенных архитектур, которые позволяют быстро восстанавливать работу в случае сбоев. Такие подходы критически важны для бизнес-приложений, где даже кратковременные перерывы могут привести к значительным потерям.		ПК-2
18.	Меры по повышению доступности включают внедрение резервирования, где критически важные компоненты системы дублируются для обеспечения непрерывности работы.	Меры по повышению доступности	УК -6 ПК-2

	Также используются технологии кластеризации, позволяющие нескольким серверам работать совместно и автоматически переключаться в случае сбоя. Кроме того, регулярное тестирование и мониторинг систем помогают выявлять и устранять потенциальные проблемы до их возникновения.		
19.	Реагирование на инциденты включает в себя процесс выявления, анализа и устранения проблем, которые могут повлиять на доступность и производительность систем. Эффективное реагирование требует наличия четкого плана действий, команды специалистов и инструментов для быстрого восстановления работы.	Реагирование на инциденты	УК -6 ПК-2

	Это помогает минимизировать время простоя и снижает риски для бизнеса.		
20.	Аварийное восстановление — это процесс восстановления систем и данных после серьезных сбоев или катастроф, таких как природные бедствия, кибератаки или аппаратные сбои. Он включает в себя создание резервных копий, разработку планов восстановления и тестирование этих планов для обеспечения быстрой реакции в экстренных ситуациях. Эффективное аварийное восстановление помогает минимизировать потери и обеспечить продолжение бизнес-процессов.	Аварийное восстановление	УК -6 ПК-2
21.	Защита систем и устройств включает в себя набор мер и технологий,	Защита систем и устройств	УК -6 ПК-2

	направленных на предотвращение несанкционированного доступа, кибератак и утечек данных. Это может включать использование антивирусного ПО, фаерволов, шифрования и регулярных обновлений программного обеспечения. Эффективная защита помогает сохранить конфиденциальность информации и обеспечить надежность работы систем.		
22.	Повышение надежности сервера включает в себя использование резервирования, регулярное обновление программного обеспечения и мониторинг состояния оборудования. Внедрение технологий отказоустойчивости и балансировки нагрузки также способствует	Повышение надежности сервера	УК -6 ПК-2

	минимизации времени простоя и поддержанию высокой доступности сервисов. Эти меры обеспечивают стабильную работу серверов и защиту от потенциальных сбоев.		
23.	Повышение надежности сетевой инфраструктуры достигается за счет внедрения дублирующих компонентов, таких как резервные маршрутизаторы и коммутаторы, а также технологий балансировки нагрузки. Регулярное обновление оборудования и мониторинг трафика помогают выявлять и устранять потенциальные проблемы, обеспечивая стабильную и бесперебойную работу сети.	Повышение надежности сетевой инфраструктуры	УК -6 ПК-2
24.	домен	На данном этапе командообразования команда постоянно отслеживает, насколько эффективно она продвигается вперед, называется:_____	УК -6 ПК-2

25.	b	S: Кто такие «белые хакеры» a) Хакеры, совершающие преступления и, возможно, неэтичные поступки, но не в целях личной выгоды или в стремлении причинить ущерб b) Хакеры, олицетворяющие собой этичных хакеров, c) которые используют свои навыки программирования в хороших, этических и законных целях d) Хакеры, являющиеся неэтичными преступниками, которые нарушают компьютерную и сетевую безопасность в целях личной выгоды или для нанесения вреда e) Хакеры, спонсируемые государством	УК -6 ПК-2
26.	кибербезопасности	Целью ### является непрерывная защита сетевых систем и данных от несанкционированного доступа	УК -6 ПК-2
27.	d	Какие данные включает в себя ЭМК? a) Информацию о законченных классах b) Информацию о зарплате и страховании c) Информацию о доходах и расходах d) Данные о физическом и психическом здоровье	УК -6 ПК-2
28.	a	Какая грань куба кибербезопасности определяет цели защиты киберпространства? a) Первая b) Вторая c) Третья	УК -6 ПК-2

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, в полном объёме выбирает эффективные стратегии и тактики личностного и профессионального развития, методики оценки эффективности применяемых методов решения поставленных задач в сфере своей профессиональной деятельности, в полном объёме ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, в полном объёме выбирает эффективные стратегии и тактики личностного и профессионального развития, методики оценки эффективности применяемых методов решения поставленных задач в сфере своей профессиональной деятельности.

Оценка «хорошо» выставляется студенту, если он, ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, выбирает эффективные стратегии и тактики личностного и профессионального развития, методики оценки эффективности применяемых методов решения поставленных задач в сфере своей профессиональной деятельности, с ошибками проводит научные исследования в области параллельных компьютерных технологий, с ошибками проводит рецензирование научных статей и авторефератов и диссертаций по математическим и информационным направлениям.

Оценка «удовлетворительно» выставляется студенту, если он, в основном ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, в основном выбирает эффективные стратегии и тактики личностного и профессионального развития, методики оценки эффективности применяемых методов решения поставленных задач в сфере своей профессиональной деятельности, с трудом проводит научные исследования в области параллельных компьютерных технологий, с трудом проводит рецензирование научных статей и авторефератов и диссертаций по математическим и информационным направлениям. Компетенции УК-6, ПК-2 освоены на удовлетворительном уровне.

Оценка «неудовлетворительно» выставляется студенту, если он, на низком уровне ставит цели в своей профессиональной деятельности и решает профессиональные задачи с учётом своих ресурсных возможностей и приоритетов, на низком уровне выбирает эффективные стратегии и тактики личностного и профессионального развития, методики оценки эффективности применяемых методов решения поставленных задач в сфере своей профессиональной деятельности, на низком уровне проводит оценку эффективность использования времени и других ресурсов, при решении поставленных задач в избранной сфере профессиональной деятельности, не проводит научные исследования в области параллельных компьютерных технологий, не проводит рецензирование научных статей и авторефератов и диссертаций по математическим и информационным направлениям. Компетенции УК-6, ПК-2 не освоены.