

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Грובה 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
Грובה Т. А.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
«Этика и безопасность искусственного интеллекта»**

Направление подготовки
Профиль

02.04.01 Математика и компьютерные науки
Искусственный интеллект в
кибербезопасности

Год начала обучения
Форма обучения

2026
очная

Реализуется во 2 семестре

Введение

1. Назначение: Фонд оценочных средств предназначен для обеспечения методической основы для организации и проведения текущего контроля по дисциплине «Этика и безопасность искусственного интеллекта». 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 «Этика и безопасность искусственного интеллекта»

3. Разработчик: кафедры вычислительной математики и кибернетики.

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель

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

Члены комиссии:

Пелешенко В.С. доцент кафедры кафедры вычислительной математики и кибернетики

Пелешенко Т. А. доцент кафедры 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 (Неудовлетворит ельно) 2 балла	Минимальный уровень (удовлетворитель но) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
<i>Компетенция: ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства</i>				
Результаты обучения по дисциплине (модулю): <i>Индикатор: ИД-1. ОПК-1.</i> Формулирует цель проекта, определяет совокупность взаимосвязанных задач, обеспечивающих ее достижение, и определяет ожидаемые результаты решения задач.	с трудом ориентируется в основных понятиях, связанных с обеспечением информационно психологической безопасности личности, общества и государства, понятиях информационного противоборства, информационной войны и форм их проявлений в современном мире	в основном ориентируется в основных понятиях, связанных с обеспечением информационно психологической безопасности личности, общества и государства, понятиях информационного противоборства, информационной войны и форм их проявлений в современном мире	ориентируется в основных понятиях, связанных с обеспечением информационно психологической безопасности личности, общества и государства, понятиях информационного противоборства, информационной войны и форм их проявлений в современном мире	в полном объеме ориентируется в основных понятиях, связанных с обеспечением информационно психологической безопасности личности, общества и государства, понятиях информационного противоборства, информационной войны и форм их проявлений в современном мире
<i>ИД-2. ОПК-1.</i> Разрабатывает план действий для решения задач проекта, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений	с трудом анализирует источники и даёт классификацию и оценку угрозам информационной безопасности	в основном анализирует источники и даёт классификацию и оценку угрозам информационной безопасности	анализирует источники и даёт классификацию и оценку угрозам информационной безопасности	в полном объеме анализирует источники и даёт классификацию и оценку угрозам информационной безопасности

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.	Этика ИИ — это область, изучающая моральные и этические аспекты разработки и применения систем ИИ	Что такое этика ИИ?	ОПК -1
2.	Основные проблемы включают предвзятость, прозрачность, подотчетность и защита данных.	Какие основные проблемы этики ИИ?	ОПК -1
3.	Принципы включают уважение автономии, непричинение вреда, благодеяние и справедливость	Какие этические принципы следует учитывать при разработке ИИ?	ОПК -1
4.	Использование разнообразных наборов данных, тестирование на предвзятость и аудит моделей.	Как предотвратить предвзятость в системах ИИ?	ОПК -1
5.	Прозрачность означает понимание того, как работает система ИИ и как она принимает решения.	Что такое прозрачность в ИИ?	ОПК -1
6.	Установление механизмов обратной связи и жалоб, а также	Как обеспечить подотчетность в системах ИИ?	ОПК -1

	прозрачность в принятии решений		
7.	Риски включают ошибки диагностики, предвзятость в лечении и конфиденциальность данных	Какие риски связаны с использованием ИИ в здравоохранении?	ОПК -1
8.	Проблемы включают предвзятость в оценке, доступ к образованию и конфиденциальность данных.	Какие этические проблемы возникают при использовании ИИ в образовании?	ОПК -1
9.	Использование шифрования, анонимизации и минимизации данных	Какие меры можно предпринять для защиты данных в ИИ?	ОПК -1
10.	Стандарты включают рекомендации UNESCO и руководящие принципы ЕС по ИИ.	Какие международные стандарты регулируют этику ИИ?	ОПК -1
11.	Безопасность ИИ — это обеспечение защиты систем ИИ от вредоносных воздействий и ошибок	Что такое безопасность ИИ?	ОПК -1
12.	Риски включают кибератаки, ошибки программирования и непредвиденные последствия	Какие основные риски безопасности в ИИ?	ОПК -1
13.	Использование безопасных протоколов,	Какие меры можно предпринять для защиты ИИ от кибератак?	ОПК -1

	регулярные обновления и мониторинг.		
14.	Методы включают тестирование на проникновение и анализ уязвимостей.	Какие методы используются для тестирования безопасности ИИ?	ОПК -1
15.	Последствия включают финансовые потери, ущерб репутации и физический вред.	Какие последствия могут иметь ошибки в системах ИИ?	ОПК -1
16.	Подходы включают тестирование, верификацию и валидацию систем.	Какие подходы используются для обеспечения надежности ИИ?	ОПК -1
17.	Риски включают непредсказуемое поведение и отсутствие контроля.	Какие риски связаны с автономными системами ИИ?	ОПК -1
18.	Использование проверок качества, тестирование и регулярные обновления	Какие меры можно предпринять для предотвращения ошибок в ИИ?	ОПК -1
19.	Стандарты включают руководящие принципы ISO по безопасности ИИ.	Какие международные стандарты регулируют безопасность ИИ?	ОПК -1
20.	Инструменты включают программы для анализа уязвимостей и тестирования на проникновение.	Какие инструменты используются для анализа безопасности ИИ?	ОПК -1
21.	Проблемы включают ответственность,	Какие правовые проблемы возникают при использовании ИИ?	ОПК -1

	интеллектуальная собственность и защита данных.		
22.	Законы варьируются, но включают GDPR в ЕС и ССРА в США.	Какие законы регулируют использование ИИ в разных странах?	ОПК -1
23.	Риски включают судебные иски и штрафы за дискриминацию	Какие правовые риски связаны с предвзятостью в ИИ?	ОПК -1
24.	Использование юридических консультаций и соблюдение существующих законов	Какие меры можно предпринять для соблюдения правовых требований при разработке ИИ?	ОПК -1
25.	Соглашения включают рекомендации ОЭСР по ИИ.	Какие международные соглашения регулируют правовые аспекты ИИ?	ОПК -1
26.	Инструменты включают юридические базы данных и консультационные услуги.	Какие инструменты используются для анализа правовых рисков ИИ?	ОПК -1
27.	Последствия включают штрафы, судебные иски и ущерб репутации	Какие последствия могут иметь нарушения правовых требований в ИИ?	ОПК -1
28.	Подходы включают регулярные аудиты и консультации с юристами	Какие подходы используются для обеспечения правовой безопасности ИИ?	ОПК -1
29.	Риски включают нарушения патентов и авторских прав.	Какие риски связаны с интеллектуальной собственностью в ИИ?	ОПК -1

30.	Использование патентов, авторских прав и соглашений о неразглашении	Какие меры можно предпринять для защиты интеллектуальной собственности в ИИ?	ОПК -1
31.	Проблемы включают потерю рабочих мест, дискриминацию и влияние на общество	Какие социальные проблемы возникают при использовании ИИ?	ОПК -1
32.	Меры включают переподготовку работников и социальные программы поддержки.	Какие меры можно предпринять для смягчения социальных последствий ИИ?	ОПК -1
33.	а) Риски включают стресс, зависимость и социальную изоляцию.	Какие риски связаны с влиянием ИИ на психическое здоровье?	ОПК -1
34.	Подходы включают разработку социально ответственных систем и оценку воздействия на общество	Какие подходы используются для обеспечения социальной ответственности ИИ?	ОПК -1
35.	Инициативы включают программы ООН по цифровому развитию.	Какие международные инициативы направлены на решение социальных проблем ИИ?	ОПК -1
36.	Инструменты включают социологические исследования и оценку воздействия.	Какие инструменты используются для анализа социальных последствий ИИ?	ОПК -1
37.	Последствия включают социальную напряженность и	Какие последствия могут иметь игнорирование социальных проблем ИИ?	ОПК -1

	снижение доверия к технологиям.		
38.	Подходы включают разработку систем, учитывающих социальные факторы	Какие подходы используются для обеспечения социальной безопасности ИИ?	ОПК -1
39.	Риски включают культурную гомогенизацию и потерю традиционных ценностей.	Какие риски связаны с влиянием ИИ на культуру?	ОПК -1
40.	Меры включают разработку культурно чувствительных систем и поддержку культурных программ	Какие меры можно предпринять для сохранения культурного разнообразия при использовании ИИ?	ОПК -1
41.	Проблемы включают вопросы сознания, свободной воли и моральной ответственности.	Какие философские проблемы возникают при использовании ИИ?	ОПК -1
42.	Теории включают утилитаризм, деонтологию и виртуализм.	Какие философские теории лежат в основе этики ИИ?	ОПК -1
43.	Риски включают потерю контроля и непредсказуемое поведение	Какие риски связаны с созданием сильного ИИ?	ОПК -1
44.	Подходы включают разработку систем с учетом философских принципов	Какие подходы используются для обеспечения философской безопасности ИИ?	ОПК -1

45.	Дискуссии включают обсуждения в академических кругах и на конференциях.	Какие международные дискуссии ведутся по философским аспектам ИИ?	ОПК -1
46.	Инструменты включают философские тексты и дискуссии в академических журналах.	Какие инструменты используются для анализа философских последствий ИИ?	ОПК -1

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 объеме ориентируется в основных понятиях, связанных с обеспечением информационно психологической безопасности личности, общества и государства, понятиях информационного противоборства, информационной войны и форм их проявлений в современном мире. В полном объеме анализирует источники и даёт классификацию и оценку угрозам информационной безопасности.

Оценка «хорошо» выставляется студенту, если он, ориентируется в основных понятиях, связанных с обеспечением информационно психологической безопасности личности, общества и государства, понятиях информационного противоборства, информационной войны и форм их проявлений в современном мире. Анализирует источники и даёт классификацию и оценку угрозам информационной безопасности.

Оценка «удовлетворительно» выставляется студенту, если он, в основном ориентируется в основных понятиях, связанных с обеспечением информационно психологической безопасности личности, общества и государства, понятиях информационного противоборства, информационной войны и форм их проявлений в современном мире. В основном анализирует источники и даёт классификацию и оценку угрозам информационной безопасности.

Оценка «не удовлетворительно» выставляется студенту, если он с трудом ориентируется в основных понятиях, связанных с обеспечением информационно психологической безопасности личности, общества и государства, понятиях информационного противоборства, информационной войны и форм их проявлений в современном мире. С трудом анализирует источники и даёт классификацию и оценку угрозам информационной безопасности.