

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Грובה Татьяна Александровна

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: «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

bd39d4208aa94cf4422feb787c81619d42de79a7

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования

УТВЕРЖДАЮ

И.о. декана факультета
математики и компьютерных
наук имени профессора
Н.И. Червякова
Грובה Т.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Модели машинного обучения, сохраняющие конфиденциальность

Направление подготовки

Направленность (профиль)

Год начала обучения

Форма обучения

Реализуется в семестрах

02.04.01 Математика и компьютерные науки

Искусственный интеллект в кибербезопасности

2026

очная

4

Введение

1. Назначение:

Фонд оценочных средств предназначен для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине «Модели машинного обучения, сохраняющие конфиденциальность» для студентов направления подготовки 02.04.01 Математика и компьютерные науки, очной формы обучения.

2. ФОС является приложением к программе дисциплины «Модели машинного обучения, сохраняющие конфиденциальность»

3. Разработчик: Ширяев Е. М., ассистент кафедры вычислительной математики и кибернетики.

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель:

Поддубная Н.А. – председатель УМК факультета математики и компьютерных наук имени профессора Н.И. Червякова

Члены комиссии:

Гладков А.В. – член УМК кафедры вычислительной математики и кибернетики;

Андрухив Л.В. – член УМК кафедры математического моделирования;

Копыткова Л.Б. – член УМК кафедры математического анализа, алгебры и геометрии.

Представитель организации-работодателя: Подопригора Н.Б. – генеральный директор ООО «Медицина ИТ».

Экспертное заключение: ФОС по дисциплине «Искусственный интеллект в профессиональной сфере» позволяет оценить уровень сформированности компетенций. Рекомендовать к использованию в учебном процессе.

« ____ » _____ 2026 г.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

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

Компетенции, индикаторы	Уровни сформированности компетенций			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
<i>Компетенция: ПК-3. Способен проводить методические и экспертные работы в области математики и информатики</i>				
Результаты обучения по дисциплине: <i>Индикатор:</i> ИД-1 ПК-3 Проводит экспертные работы по математике.	Не проводит экспертные работы по математике.	С трудом проводит экспертные работы по математике	Проводит экспертные работы по математике с ошибками	Проводит экспертные работы по математике.
Результаты обучения по дисциплине: <i>Индикатор:</i> ИД-2 ПК-3 Проводит экспертные работы в области информатики	Не проводит экспертные работы в области информатике	С трудом проводит экспертные работы в области информатике	С ошибками проводит экспертные работы в области информатик е	Проводит экспертные работы в области информатике
Результаты обучения по дисциплине: <i>Индикатор:</i> ИД-3 ПК-3 Готовит Методические материалы в области математики и информатики	Не готовит методические материалы в области математики и информатики	С трудом готовит методические материалы в области математики и информатики	С ошибками готовит методически е материалы в области математики и информатик и	Готовит методические материалы в области математики и информатики

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
Семестр 1			
1.	b	Какой тип шифрования чаще всего используется в частных моделях машинного обучения? a) AES b) Гомоморфное шифрование c) RSA d) SHA-256	ПК-3
2.	a	Какой метод машинного обучения позволяет работать с зашифрованными данными без их расшифровки? a) Гомоморфное машинное обучение b) Линейная регрессия c) Метод опорных векторов d) Случайный лес	ПК-3
3.	c	Какой библиотекой можно воспользоваться для работы с гомоморфным шифрованием в Python? a) Scikit-learn b) TensorFlow c) TenSEAL d) PyTorch	ПК-3
4.	a	Какая схема гомоморфного шифрования поддерживается в TenSEAL? a) CKKS b) RSA c) ElGamal d) SHA-3	ПК-3
5.	a	Какой алгоритм чаще всего используется для частного обучения сверточных нейросетей? a) Federated Learning (FL) b) K-means c) Principal Component Analysis (PCA) d) DBSCAN	ПК-3
6.	b	Что означает термин "дифференциальная приватность" в контексте машинного обучения? a) Полное скрывание данных от модели b) Добавление шума к данным для защиты конфиденциальности c) Использование только зашифрованных данных d) Удаление персональной информации из датасета	ПК-3

7.	a	Какой алгоритм машинного обучения можно использовать на зашифрованных данных в TenSEAL? a) Логистическая регрессия b) KNN c) Градиентный бустинг d) Метод главных компонент	ПК-3
8.	b,c	Какие основные ограничения накладывает гомоморфное шифрование на модели машинного обучения? a) Снижение точности моделей b) Значительное увеличение вычислительной сложности c) Увеличение времени обработки данных d) Ограничение количества данных	ПК-3
9.	b	Что является основным преимуществом использования гомоморфного шифрования в машинном обучении? a) Уменьшение размера данных b) Возможность выполнения вычислений без расшифровки c) Увеличение скорости вычислений d) Исключение необходимости обучения модели	ПК-3
10.	b	Какие задачи лучше всего подходят для гомоморфного машинного обучения? a) Обнаружение аномалий b) Классификация c) Регрессия d) Генерация изображений	ПК-3
11.	c,d	Какой тип регрессии можно обучать на зашифрованных данных? a) Полиномиальная регрессия b) Деревья решений c) Линейная регрессия d) Логистическая регрессия	ПК-3
12.	a	Какой механизм используется для уменьшения вычислительной нагрузки при работе с зашифрованными данными? a) Приближенные числа b) Повышение разрядности шифрования c) Сжатие данных перед шифрованием d) Использование частично-гомоморфного шифрования	ПК-3
13.	a,b	Какие преобразования поддерживаются в гомоморфном шифровании CKKS? a) Сложение b) Умножение c) Деление d) Логические операции	ПК-3

14.	b	Какой метод используется для шифрования чисел с плавающей точкой в TenSEAL? a) Целочисленное представление b) Приближенное представление (CKKS) c) Дискретизация значений d) Логарифмическое преобразование	ПК-3
15.	b	Какая основная проблема возникает при работе с приближенными числами в CKKS? a) Потеря данных при шифровании b) Ошибка округления из-за конечной точности c) Невозможность выполнения умножения d) Утрата конфиденциальности	ПК-3
16.	b	Какая концепция позволяет обучать модели без передачи данных на центральный сервер? a) Конволюционные нейросети b) Federated Learning c) Градиентный спуск d) Глубокие автоэнкодеры	ПК-3
17.	a	Какой из перечисленных методов НЕ связан с приватным обучением? a) Метод k-ближайших соседей (KNN) b) Гомоморфное шифрование c) Дифференциальная приватность d) Federated Learning	ПК-3
18.	a,b	Какие механизмы позволяют защитить приватность данных в распределенном обучении? a) Federated Averaging b) Дифференциальная приватность c) Удаление исходных данных после обучения d) Сжатие градиентов	ПК-3
19.	a,c	Какие ограничения имеет Federated Learning? a) Высокие требования к вычислительным ресурсам на клиенте b) Невозможность обновления модели c) Повышенная сложность синхронизации моделей d) Ограничение числа участников обучения	ПК-3
20.	a,b	Какой подход можно использовать для увеличения точности моделей, работающих на зашифрованных данных? a) Оптимизация структуры модели для минимизации числа умножений b) Уменьшение разрядности шифрования для сокращения вычислительных затрат c) Увеличение длины шифра без изменения алгоритма d) Добавление случайного шума в процесс обучения	ПК-3

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».

3. Критерии оценивания компетенций

Оценка **«зачтено»** выставляется студенту, если он показал минимальный, средний или высокий уровень сформированности компетенции ПК-2.

Оценка **«не зачтено»** выставляется студенту, если минимальный уровень сформированности компетенции ПК-2 не достигнут