

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Галунин Сергей Александрович  
Должность: проректор по учебной работе  
Дата подписания: 23.12.2025 13:42:26  
Уникальный программный ключ:  
08ef34338325bdb0ac5a47baa5472ce36cc3fc3b

Приложение к ОПОП  
«Разработка программно-  
информационных систем»



**СПбГЭТУ «ЛЭТИ»**  
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное образовательное учреждение высшего образования  
**«Санкт-Петербургский государственный электротехнический университет  
«ЛЭТИ» им. В.И.Ульянова (Ленина)»  
(СПбГЭТУ «ЛЭТИ»)**

---

**РАБОЧАЯ ПРОГРАММА**

дисциплины

**«ФЕДЕРАТИВНОЕ ОБУЧЕНИЕ»**

для подготовки бакалавров

по направлению

09.03.04 «Программная инженерия»

по профилю

**«Разработка программно-информационных систем»**

Санкт-Петербург

2025

## **ЛИСТ СОГЛАСОВАНИЯ**

Разработчики:

проректор по цифровой трансформации, д.т.н., доцент Холод И.И.  
доцент, к.т.н., доцент Новикова Е.С.

Рабочая программа рассмотрена и одобрена на заседании кафедры ИС  
16.01.2025, протокол № 1

Рабочая программа рассмотрена и одобрена учебно-методической комиссией  
ФКТИ, 28.01.2025, протокол № 1

Согласовано в ИС ИОТ

Начальник ОМОЛА Загороднюк О.В.

## **1 СТРУКТУРА ДИСЦИПЛИНЫ**

Обеспечивающий факультет	ФКТИ
Обеспечивающая кафедра	ИС
Общая трудоемкость (ЗЕТ)	3
Курс	4
Семестр	8

## Виды занятий

Электронные лекции (акад. часов)	16
Электронные практические (академ. часов) (академ. часов)	16
Иная контактная работа (академ. часов)	1
Все контактные часы (академ. часов)	1
Самостоятельная работа, включая часы на контроль (академ. часов)	75
Всего (академ. часов)	108

## Вид промежуточной аггломерации

Дифф. зачет (курс) 4

## **2 АННОТАЦИЯ ДИСЦИПЛИНЫ**

### **«ФЕДЕРАТИВНОЕ ОБУЧЕНИЕ»**

В рамках курса студенты изучают технологию федеративного обучения - анализа методами машинного обучения распределенных данных без их сбора в едином хранилище. Рассматриваются особенности анализа распределенных данных, виды распределенных данных и способы их распределения по источникам. Рассматриваются основные алгоритмы федеративного обучения. Кроме того, обсуждаются типы систем федеративного обучения и варианты их практического применения.

## **SUBJECT SUMMARY**

### **«FEDERATED LEARNING»**

On the course, students study the technology of federated learning -analysis of distributed data using machine learning methods without collecting them in a single repository. The features of distributed data analysis, types of distributed data and methods of their distribution by sources are considered. The main algorithms of federated learning are considered. In addition, the types of federated learning systems and their application options are discussed.

## **3 ОБЩИЕ ПОЛОЖЕНИЯ**

### **3.1 Цели и задачи дисциплины**

1. Цели изучения дисциплины:

- приобретение знаний о принципах построения аналитических систем на основе на основе федеративного обучения и алгоритмов федеративного обучения;
- приобретение знаний о схемах распределения данных в системе и методах обработки неоднородности в распределенных обучающих наборах данных;
- формирование навыков по выбору и обоснования различных стратегий формирования глобальной модели машинного обучения в зависимости от схемы распределения анализируемых данных и решаемой аналитической задачи;
- формирование умений по построению и развертыванию систем распределенной аналитической обработке на основе федеративного обучения;
- формирование умений по применению методов обнаружения вредоносных воздействий на модели машинного обучения и противодействию им.

2. Задачами изучения дисциплины являются:

- приобретение знаний о принципах построения аналитических систем на основе на основе федеративного обучения;
- приобретение знаний об алгоритмах федеративного обучения и их разработке;
- приобретение знаний о способах распределения данных в системе и методах обработки неоднородности в распределенных обучающих наборах данных;
- формирование навыков по выбору и обоснования различных стратегий формирования глобальной модели машинного обучения в зависимости от схемы распределения анализируемых данных и решаемой аналитической задачи;
- формирование умений по построению и развертыванию систем распределенной аналитической обработке на основе федеративного обучения;
- формирование умений по применению методов обнаружения вредоносных воздействий на модели машинного обучения и противодействию им.

действий на модели машинного обучения и противодействию им.

3. Студенты получат знания:

- о принципах построения аналитических систем на основе на основе федеративного обучения;
- об алгоритмах федеративного обучения и их разработке;
- о схемах распределения данных в системе;
- о методах оценки уровня неоднородности в распределенных обучающих наборах данных и методах ее обработки;
- о методах нарушения безопасности моделей ИИ, обученных в федеративном режиме.

4. Студенты получат умения:

- по анализу, синтезу и обобщению необходимой информацию из различных источников, включая сетевые ресурсы сети Интернет для выбора методов алгоритмов федеративного обучения в зависимости от схемы распределения данных, уровня неоднородности в них и решаемой аналитической задачи;
- по разработке методов обучения моделей ИИ в федеративном режиме обучения;
- по обнаружению и предотвращению деструктивных воздействий на модели ИИ, обучаемых в федеративном режиме.

5. Студенты получат практические навыки по использованию программных библиотек и фреймворков, применяемых для построения распределенных аналитических систем на основе федеративного обучения.

### **3.2 Место дисциплины в структуре ОПОП**

Дисциплина изучается на основе ранее освоенных дисциплин учебного плана:

1. «Глубокое обучение»
2. «Большие данные»

и обеспечивает подготовку выпускной квалификационной работы.

### **3.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы**

В результате освоения образовательной программы обучающийся должен достичь следующие результаты обучения по дисциплине:

<b>Код компетенции/ индикатора компетенции</b>	<b>Наименование компетенции/индикатора компетенции</b>
ПК-0	Способен разрабатывать информационные модели и применять их для решения задач профессиональной деятельности
ПК-0.1	<i>Знает современные виды информационных моделей, применяемых при решении задач профессиональной деятельности</i>
ПК-0.2	<i>Создает и модифицирует информационные модели для решения задач профессиональной деятельности</i>
ПК-0.3	<i>Применяет информационные модели для решения задач профессиональной деятельности</i>

## **4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ**

### **4.1 Содержание разделов дисциплины**

#### **4.1.1 Наименование тем и часы на все виды нагрузки**

<b>№ п/п</b>	<b>Наименование темы дисциплины</b>	<b>ЭЛек, ач</b>	<b>ЭПр, ач</b>	<b>ИКР, ач</b>	<b>СР, ач</b>
1	Введение в федеративное обучение	2		1	6
2	Распределение данных	2	4		10
3	Системы федеративного обучения	2			8
4	Безопасность федеративного обучения	4	4		20
5	Специальные алгоритмы федеративного обучения	4	4		20
6	Фреймворки федеративного обучения	2	4		11
	Итого, ач	16	16	1	75
	Из них ач на контроль	0	0	0	0
	Общая трудоемкость освоения, ач/зе				108/3

#### **4.1.2 Содержание**

<b>№ п/п</b>	<b>Наименование темы дисциплины</b>	<b>Содержание</b>
1	Введение в федеративное обучение	Распределенные данные. Проблема обучения на распределенных данных. Новая концепция Сеть данных (Data Mesh). Федеративное обучение. Клавиатура GBoard.
2	Распределение данных	Виды распределения. Горизонтальное распределение данных. Вертикальное распределение данных. Гибридное распределение данных. Оценки неоднородности распределенных данных: метрики и алгоритмы расчета.
3	Системы федеративного обучения	Классификация систем федеративного обучения, масштабирование систем федеративного обучения, топологии систем федеративного обучения, стратегии обучения в системах федеративного обучения. Области применения федеративного обучения.
4	Безопасность федеративного обучения	Модели атак машинного обучения. Модели атак федеративного обучения. Атаки на отравление модели: способы реализации. Механизмы обнаружения отравляющих атак. Механизмы обеспечения конфиденциальной обработки данных: доверенная среда выполнения, дифференциальная приватность, специальные криптографические протоколы.

<b>№ п/п</b>	<b>Наименование темы дисциплины</b>	<b>Содержание</b>
5	Специальные алгоритмы федеративного обучения	Стратегии агрегирования для горизонтально распределенных данных (нейронные сети, деревья решений), механизмы обработки неидентично распределенных данных. Обнаружение византийских ошибок. 1-раундовое федеративное обучение. Федеративное обучение на вертикально распределенных данных (нейронные сети и деревья решений). Дифференциальная приватности на вертикально распределенных данных.
6	Фреймворки федеративного обучения	Характеристики фреймворков федеративного обучения. Фреймворт TensorFlow Federated (TFF). Фреймворт Flower. Фреймворт Federated AI Technology Enabler (FATE). Фреймворт Paddle Federated Learning (PFL).

## **4.2 Перечень лабораторных работ**

Лабораторные работы не предусмотрены.

## **4.3 Перечень практических занятий**

<b>Наименование практических занятий</b>	<b>Количество ауд. часов</b>
1. Исследование метрик и алгоритмов оценки уровня неоднородности в распределенных данных	4
2. Генерация распределенных данных с разным уровнем неоднородности и схемой разделения данных	4
3. Исследование различных видов атак на федеративное обучение	2
4. Исследование различных методов обнаружения отравляющих атак разного типа	2
5. Специальные алгоритмы федеративного обучения	2
6. Фреймворки федеративного обучения: FATE, PFL	2
<b>Итого</b>	<b>16</b>

## **4.4 Курсовое проектирование**

Курсовая работа (проект) не предусмотрены.

## **4.5 Реферат**

Реферат не предусмотрен.

#### **4.6 Индивидуальное домашнее задание**

Индивидуальное домашнее задание не предусмотрено.

#### **4.7 Доклад**

Доклад не предусмотрен.

#### **4.8 Кейс**

Кейс не предусмотрен.

#### **4.9 Организация и учебно-методическое обеспечение самостоятельной работы**

Изучение дисциплины сопровождается самостоятельной работой студентов с рекомендованными преподавателем литературными источниками и информационными ресурсами сети Интернет.

Планирование времени для изучения дисциплины осуществляется на весь период обучения, предусматривая при этом регулярное повторение пройденного материала. Обучающимся, в рамках внеаудиторной самостоятельной работы, необходимо регулярно дополнять сведениями из литературных источников материал, законспектированный на лекциях. При этом на основе изучения рекомендованной литературы целесообразно составить конспект основных положений, терминов и определений, необходимых для освоения разделов учебной дисциплины.

Особое место уделяется консультированию, как одной из форм обучения и контроля самостоятельной работы. Консультирование предполагает особым образом организованное взаимодействие между преподавателем и студентами, при этом предполагается, что консультант либо знает готовое решение, которое он может предписать консультируемому, либо он владеет способами деятель-

ности, которые указывают путь решения проблемы.

Самостоятельное изучение студентами теоретических основ дисциплины обеспечено необходимыми учебно-методическими материалами (учебники, учебные пособия, конспект лекций и т.п.), выполненными в печатном или электронном виде.

Изучение студентами дисциплины сопровождается проведением регулярных консультаций преподавателей, обеспечивающих практические занятия по дисциплине, за счет бюджета времени, отводимого на консультации (внеаудиторные занятия, относящиеся к разделу «Самостоятельные часы для изучения дисциплины»).

Текущая СРС	Примерная трудоемкость, ач
Работа с лекционным материалом, с учебной литературой	18
Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	16
Самостоятельное изучение разделов дисциплины	
Выполнение домашних заданий, домашних контрольных работ	
Подготовка к лабораторным работам, к практическим и семинарским занятиям	26
Подготовка к контрольным работам, коллоквиумам	
Выполнение расчетно-графических работ	
Выполнение курсового проекта или курсовой работы	
Поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме	
Работа над междисциплинарным проектом	
Анализ данных по заданной теме, выполнение расчетов, составление схем и моделей, на основе собранных данных	
Подготовка к зачету, дифференциированному зачету, экзамену	15
<b>ИТОГО СРС</b>	<b>75</b>

## **5 Учебно-методическое обеспечение дисциплины**

### **5.1 Перечень основной и дополнительной литературы, необходимой для освоения дисциплины**

<b>№ п/п</b>	<b>Название, библиографическое описание</b>	<b>К-во экз. в библ.</b>
<b>Основная литература</b>		
1	Николенко С. Глубокое обучение. — (Серия «Библиотека программиста») / С. Николенко, А. Кадурин, Е. Архангельская, 2020. -480 с. -Текст : электронный.	неогр.
2	Масис С. Интерпретируемое машинное обучение на Python: Пер. с англ. / С. Масис, 2023. -640 с. -Текст : электронный.	неогр.
3	Чио К. Машинное обучение и безопасность : руководство / К. Чио, Д. Фримэн, 2020. -388 с. -Текст : электронный.	неогр.
<b>Дополнительная литература</b>		
1	Гифт Ной Прагматичный ИИ. Машинное обучение и облачные технологии / Ной Гифт, 2019. -304 с. -Текст : электронный.	неогр.

### **5.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых при освоении дисциплины**

<b>№ п/п</b>	<b>Электронный адрес</b>
1	Глубокое обучение. Федеративное обучение <a href="https://habr.com/ru/companies/piter/articles/458800/">https://habr.com/ru/companies/piter/articles/458800/</a>
2	Federated Research <a href="https://github.com/google-research/federated">https://github.com/google-research/federated</a>
3	Flower FL <a href="https://flower.ai/">https://flower.ai/</a>

### **5.3 Адрес сайта курса**

Адрес сайта курса: <https://vec.etu.ru/moodle/course/view.php?id=23414>

## **6 Критерии оценивания и оценочные материалы**

### **6.1 Критерии оценивания**

Для дисциплины «Федеративное обучение» предусмотрены следующие формы промежуточной аттестации: зачет с оценкой.

#### **Зачет с оценкой**

<b>Оценка</b>	<b>Описание</b>
Неудовлетворительно	Курс не освоен. Студент испытывает серьезные трудности при ответе на ключевые вопросы дисциплины
Удовлетворительно	Студент в целом овладел курсом, но некоторые разделы освоены на уровне определений и формулировок теорем
Хорошо	Студент овладел курсом, но в отдельных вопросах испытывает затруднения. Умеет решать задачи
Отлично	Студент демонстрирует полное овладение курсом, способен применять полученные знания при решении конкретных задач.

## **Особенности допуска**

Для допуска к дифф. зачету студент должен:

- посетить не менее 80% дистанционных занятий;
- выполнить и сдать все практические работы в срок. При сдаче практических работ допускается задержка на 1 неделю.

Дифф. зачет проводится по билетам. Критерии оценивания представлены выше.

При прохождении онлайн-курса необходимо изучение материала курса не менее чем на 80% и выполнение заданий, предусмотренных в курсе, в срок.

При сдаче практических работ допускается задержка на 1 неделю.

Дифф. зачет проводится по билетам в формате устного опроса на дистанционной консультации в конце семестра. Критерии оценивания представлены выше.

## **6.2 Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине**

### **Вопросы к дифф.зачету**

<b>№ п/п</b>	<b>Описание</b>
1	Общая схема федеративного обучения.
2	Свойства систем на основе федеративного обучения.
3	Особенности построения распределенной аналитической системы на основе федерации устройств.
4	Особенности построения распределенной аналитической системы на основе федерации организаций.
5	Схемы разделения данных.
6	Вертикальное разделение данных.
7	Горизонтальное разделение данных.
8	Гибридное разделение данных.
9	Топология систем федеративного обучения.
10	Масштаб систем федеративного обучения.
11	Ковариативный сдвиг в данных.
12	Априорных сдвиг в данных.
13	Сдвиг концепций в данных.
14	Метрики и алгоритмы оценки уровня неоднородности (сдвига) в данных.
15	Стратегии агрегирования для горизонтально распределенных данных.

16	Стратегии агрегирования локальных моделей МО, устойчивые к византийским ошибкам.
17	Стратегии агрегирования локальных моделей МО, устойчивые к отравляющим атакам.
18	Классификация стратегий агрегирования локальных моделей МО.
19	Особенности построения глобальной модели на вертикально распределенных данных.
20	Методы дифференциальной приватности в федеративном обучении.
21	Методы защиты данных в федеративном обучении.
22	Специальные криптографические протоколы в федеративном обучении.

## Форма билета

Министерство науки и высшего образования Российской Федерации  
 ФГАОУ ВО «Санкт-Петербургский государственный электротехнический  
 университет «ЛЭТИ» имени В.И. Ульянова (Ленина)»

---

### БИЛЕТ № 1

Дисциплина **Федеративное обучение ФКТИ**

1. Горизонтальное разделение данных.
2. Методы защиты данных в федеративном обучении

**УТВЕРЖДАЮ**

Заведующий кафедрой

Весь комплект контрольно-измерительных материалов для проверки сформированности компетенции (индикатора компетенции) размещен в закрытой части по адресу, указанному в п. 5.3

### **6.3 График текущего контроля успеваемости**

<b>Неделя</b>	<b>Темы занятий</b>	<b>Вид контроля</b>
1	Распределение данных	
2		Практическая работа
3	Распределение данных	
4		
5		Практическая работа
6	Безопасность федеративного обучения	Практическая работа
7	Безопасность федеративного обучения	
8		
9		
10		Практическая работа
11	Специальные алгоритмы федеративного обучения	
12		
13		Практическая работа
14	Фреймворки федеративного обучения	
15		
16		
17		Практическая работа

### **6.4 Методика текущего контроля**

#### **На лекционных занятиях**

Текущий контроль включает в себя контроль посещаемости (не менее **80** % дистанционных занятий), по результатам которого студент получает допуск к дифф. зачету.

#### **На практических (семинарских) занятиях**

Текущий контроль включает в себя контроль посещаемости (не менее **80** % дистанционных занятий), по результатам которого студент получает допуск к дифф. зачету.

В ходе проведения практических занятий целесообразно привлечение студентов к как можно более активному участию в дискуссиях, решении задач, обсуждениях и т. д. При этом активность студентов также может учитываться преподавателем, как один из способов текущего контроля на практических

занятиях. Критерием текущего контроля является полнота и своевременность выполнения практических работ. В ходе проведения практических занятий целесообразно привлечение студентов как можно более активному участию в дискуссиях, решении задач, обсуждениях и т. д. При этом активность студентов также может учитываться преподавателем, как один из способов текущего контроля на практических занятиях.

### ***Для курсов с @***

**Текущий контроль лекционных занятий** включает в себя контроль освоения онлайн-курса на платформе Moodle (просмотр не менее 80% материалов онлайн-курса), а также контроль посещаемости эл. лекций (не менее 80% дистанционных занятий), по результатам которого студент получает допуск к дифф. зачету.

**Порядок выполнения практических заданий, подготовки отчетов и их защит** включает в себя контроль посещаемости эл. практических занятий (не менее 80% дистанционных занятий), по результатам которого студент получает допуск к дифф. зачету.

В ходе проведения семинарских и практических занятий целесообразно привлечение студентов к как можно более активному участию в дискуссиях, решении задач, обсуждениях и т. д. При этом активность студентов также может учитываться преподавателем, как один из способов текущего контроля на практических занятиях.

Каждое задание нацелено на проверку полученных студентом знаний, умений. Критерии оценки у каждого задания свои. Задается максимальное количество баллов, которое студент может получить за задание.

**Выполнение практических работ** оценивается по четырехбалльной шкале:

- «Отлично» – оцениваются практические работы, в которых точно и чет-

ко описаны исходные данные, постановка задачи, описаны и обоснованы выбранные параметры модели анализа, полученные результаты обоснованы и продемонстрированы на рисунках. Выводы содержательны. Отчет о выполнении практической работы отвечает всем требованиям по оформлению и содержанию. Представлен программный код, реализующий практическую работу. Студент полно отвечает на два дополнительных вопроса по теме практической работе.

– «Хорошо» – оцениваются практические работы, в которых представлены исходные данные, постановка задачи, описаны и обоснованы выбранные параметры модели анализа, полученные результаты обоснованы и продемонстрированы на рисунках. Допускаются недостатки в обосновании выбора параметров модели анализа, графическом материале отчета по практической работе и сделанных выводах. Отчет о выполнении практической работы отвечает всем требованиям по оформлению и содержанию. Представлен программный код, реализующий практическую работу. Студент отвечает на два дополнительных вопроса по теме практической работе с затруднением или неполно.

– «Удовлетворительно» – оцениваются практические работы, в которых частично представлены исходные данные, постановка задачи, описаны выбранные параметры модели анализа, полученные результаты частично обоснованы. Графический материал отсутствует, студент затрудняется объяснить и обосновать выбор параметров модели анализа. Выводы очень краткие. Отчет о выполнении практической работы не соответствует всем требованиям по оформлению и содержанию. Представлен программный код, реализующий практическую работу, студент отвечает на вопросы по коду программы. Студент отвечает с трудом на два дополнительных вопроса по теме практической работе.

– «Неудовлетворительно» – оцениваются практические работы, в которых представлены отсутствует описание исходных данных, постановка задачи, описаны и обоснованы выбранные параметры модели анализа, полученные ре-

зультаты обоснованы. Графический материал отсутствует, студент затрудняется объяснить и обосновать выбор параметров модели анализа. Отчет о выполнении практической работы не отвечает всем требованиям по оформлению и содержанию. Представлен программный код, реализующий практическую работу. Студент не отвечает на вопросы по коду программы. Ответы на два дополнительных вопроса - неудовлетворительны

Сдача практических работ выполняется по выше представленному графику (работы загружаются в Moodle в соответствующий элемент курса), при сдаче работы не в срок оценка за нее снижается на один балл.

### **самостоятельной работы студентов**

Контроль самостоятельной работы студентов осуществляется на дистанционных лекционных и дистанционных практических занятиях студентов по методикам, описанным выше.

## **7 Описание информационных технологий и материально-технической базы**

<b>Тип занятий</b>	<b>Тип помещения</b>	<b>Требования к помещению</b>	<b>Требования к программному обеспечению</b>
Лекция	Лекционная аудитория	Количество посадочных мест – в соответствии с контингентом, рабочее место преподавателя. Помещение оснащено компьютерной техникой, включая проектор и экран, с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.	1) Альт Образование, 2) Яндекс браузер
Практические занятия	Аудитория	Количество посадочных мест – в соответствии с контингентом, рабочее место преподавателя. Помещение оснащено компьютерной техникой, включая проектор и экран, с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.	1) Альт Образование, 2) Яндекс браузер
Самостоятельная работа	Помещение для самостоятельной работы	Оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.	1) Альт Образование, 2) Яндекс браузер

## **8 Адаптация рабочей программы для лиц с ОВЗ**

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.

## **ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ**

<b>№ п/п</b>	<b>Дата</b>	<b>Изменение</b>	<b>Дата и номер протокола заседания УМК</b>	<b>Автор</b>	<b>Начальник ОМОЛА</b>