ЭТАП 1	РАССЫЛКА	01.09-07.09
ЭТАП 2	ОТБОР	08.09-09.09
ЭТАП 3	РЕЗУЛЬТАТЫ	10.09-12.09
ЭТАП 4	**СТАРТ**	**15.09 (понедельник), 19:00**
очно	Центральный Университет, ул. Гашека 7, 8 этаж, ауд.B802 (возьми паспорт, следуй по навигации)	
онлайн	трансляция - https://centraluniversity.ktalk.ru/hec6uxhjsst2	
Пн и Чт, 19:00 - 20:30 (1,5 академических часа)		
ЭТАП 5	**МОДУЛЬ MPC**	**15.09-15.10**
Лектор 1	Петр Емельянов, Bloomtech, Генеральный директор	
Лектор 2	Михаил Ершов, ведущий разработчик, Ubic Technologies	

Дата		№	Формат	Тема	Содержание	Есть ДЗ?
15.09.2025	Вводная часть 1 неделя	1	Лекция	Введение в криптографию	Введение - Почему конфиденциальные вычисления? Что такое конф вычисления, на чем базируются, какие перспективы и какие ограничения. Компании, российские и международные, которые занимаются конфиденциальными вычислениями, какие подходы решают и в каких областях человеческой жизнедеятельности работают. Криптография как основа конф.вычислений	0

					История криптографии, цели и задачи криптографии, классические примитивы и протоколы (Data-at-Rest, Data-in-Transit)	
18.09.2025		2	Лекция	Введение в конфиденциальные вычисления	История Data-in-Use криптографии, основные методы и подходы: централизация (административная и аппаратная), децентрализация (эвристики и строгие методы – MPC/HME/DP).	0
22.09.2025	MPC + HE 3 недели	3	Лекция	Введение в распределенные вычисления	Необходимый инженерный минимум: интерфейсы параллельных вычислений (MPI), фреймворки (Torch Distributed). Практическая часть: лаборатория из docker-контейнеров, в которой будем строить дальнейшую работу.	1
25.09.2025		4	Лекция	Методы разделения секрета: сложение и умножение	История разделения секрета, основные схемы: арифметические, пороговые (схемы с репликацией), схема Шамира, бинарная схема, – их свойства и применения. Реализация сложения и умножения в схеме арифметического разделения секрета с репликацией и нет (тройки Бивера, введение в протокол SPDZ).	1
29.09.2025		5	Семинар	Обучение линейной регрессии	На основе простых реализаций сложения и умножения строим конфиденциальное обучение и инференс линейной регрессии.	0
02.10.2025		6	Лекция	MPC: операция сравнения	Сравнение – самая сложная операция в MPC – необходима для обучения более сложных ML-моделей (например, сравнение нужно для ReLU). Реализация самого простого метода с двойным разделением секрета и битовой декомпозицией.	0

06.10.2025		7	Лекция	Сопутствующие протоколы	Обзор алгоритмов и протоколов, которые применяются в конфиденциальных вычислениях: PSI теория, Oblivious-алгоритмы (OT) теория + детальный разбор прикладного кейса	1
09.10.2025		8	Лекция	Сопутствующие протоколы	Гомоморфное шифрование - теория (кусочное и полное, сложность применения и известные шифры) + детальный разбор прикладного кейса	0
13.10.2025		9		Итоговая работа	Итоговое тестирование/задание на уточнении	1
ИТОГО		9				4
ЭТАП 6	ОТДЫХ	1 неделя				
ЭТАП 7	МОДУЛЬ DP и FL	27.10 - 21.11				
Лектор	Александр Безносиков, МФТИ, Заведующий лабораторией фундаментальных исследований искусственного интеллекта МФТИ, Заведующий лабораторией проблем федеративного обучения ИСП РАН					
Дата		№	Формат	Тема	Содержание	Есть ДЗ?
27.10.2025	Дифференциальная приватность (DP) 3 недели	1	Лекция	Введение в DP	Определение. Гауссовский подход и подход Лапласа. Теорема о групповой и композитной DP	0
30.10.2025		2	Лекция	Продвинутые концепции DP	DP Рени (Renyi). Локальная и перестановочная (shuffle) DP	1

03.11.2025		3	Лекция	DP и минимизация эмпирического риска	Защита модели (output peretrubation). Защита процесса обучения (градиентов).	0
06.11.2025		4	Семинар	Атака реконструкцией и DP, как способ защиты	Воспроизведение атаки на данные через итоговую модель и получемые в процессе обучения градиенты. Защита с помощью DP	1
10.11.2025		5	Лекция	DP и глубокое обучение	Особенности обучения, влияние функции потерь, модели и других факторов. Защита CV моделей и картиночных данных. Защита NLP моделей и текстовых данных.	0
13.11.2025		6	Лекция	DP в федеративном обучении	Введение в федеративное обучение. DP-FedAvg. DP-FTRL. Персонализация в федеративном обучении в условиях DP	0
17.11.2025		7		Итоговая работа	Итоговое тестирование/задание на уточнении	1
	ИТОГО	7				3