



**Учебный план дополнительной профессиональной
программы повышения квалификации:
«Локальные ИИ-агенты языковые модели и агенты в
защищённом контуре для конфиденциальных данных»**

№ п/п	Наименование темы	Описание темы	Всего, час	В том числе			
				Лекции	Практ.	Сам. работа	Итог. аттест.
1.	Зачем контур: данные, требования, открытые модели	Демонстрация: при отключённой сети локальная модель отвечает по внутреннему регламенту со ссылками на пункты; тот же вопрос облачной модели — ответ лучше, но документ ушёл наружу. Три варианта размещения ИИ и их цена. Требования: персональные данные (152-ФЗ), раздел об ИИ приказа ФСТЭК № 117 (запрет передачи информации ограниченного доступа разработчикам моделей, контроль наборов данных, доверенные технологии), суверенные и национальные модели по 243-ФЗ. Демонстрация: Ведущий отключает сеть — и ноутбук отвечает на вопросы по регламенту вымышленного предприятия со ссылками на пункты. Тот же вопрос облачной модели: ответ лучше, но документ целиком ушёл наружу. Карта данных своей организации (что можно в облако, облако РФ, только контур, нельзя никуда); сравнение трёх открытых моделей на учебной задаче.	4	2	-	2	-
2.	Модель и оборудование	Малая или большая модель: малая модель в 10–30 раз дешевле в эксплуатации; маршрутизация задач — простое малой модели, сложное большой (своей или	4	1	2	1	-



		внешней, если данные позволяют). Демонстрация: маршрутизатор отправляет классификацию обращений малой модели, а разбор сложного договора — большой. Каждый запускает модель на своём компьютере. Расчёт памяти видеокарты под модель и контекст, сжатие модели (квантование) и его цена качеством; запуск модели на своём компьютере (Ollama) и проверка на учебном документе. Результат: работающая локальная модель и расчёт оборудования. Посчитать объем памяти, выбрать сервер для своей задачи по калькулятору, выбрать и запустить свою модель.					
3.	Развёртывание и нагрузка	Запуск модели в режиме сервера на своём компьютере (Ollama) с интерфейсом, совместимым с облачными сервисами; серверная раздача для многих пользователей — демонстрация преподавателя; подключение готового приложения; нагрузочный тест (20 одновременных запросов), настройка очередей, лимитов и таймаутов. Результат: модель на сервере и протокол нагрузочного теста. Поднять модель в режиме сервера на своём компьютере, подключить к ней агента и повторить нагрузочный тест после настроек. Задание: прогнать своего агента на локальной модели и сравнить с облачной.	4	-	2	2	-
4.	Корпоративные знания в контуре	Качество поиска по документам: разбор ошибок по трассе запроса;	4	1	2	1	-



		значительная часть ошибок — плохо распознанные сканы и таблицы, а не модель. Демонстрация: Вопрос по регламенту — ответ с цитатой и пунктом документа, всё внутри контура. Сотрудник отдела продаж спрашивает про зарплаты — и после настройки прав доступа поиск ничего ему не показывает. Поиск по документам внутри контура с ответом-цитатой; права доступа к документам (честный провал: модель цитирует документ, к которому у пользователя нет доступа) и фильтр по правам. У каждого документа базы — владелец, происхождение и актуальная версия; правила обновления и удаления из индекса; проверка документа перед индексацией. Результат: поиск по документам с учётом прав доступа и учётом владельцев документов. Сбор базы документов, настройка прав доступа и проверка поиска на двадцати контрольных вопросах. Задание: собрать обезличенную базу документов своего подразделения с владельцем, происхождением и актуальной версией каждого документа и контрольные вопросы.					
5.	Агенты на локальных моделях и гибридная схема	Гибридная схема: локальная модель для конфиденциальных данных, внешняя — для общих знаний после обезличивания. Защита контура: изоляция модели и инструментов, журналы запросов и ответов, внедрённые инструкции в базе знаний, обновление моделей как изменение системы. Что делает контур контуром:	4	2	1	1	-



		учётные записи, права доступа, секреты, сетевые границы, аудит, обновления, резервное копирование, мониторинг, реагирование на инциденты. Демонстрация: Агент на локальной модели ищет в базе, считает в таблице и готовит черновик справки, не выходя из контура. Перед отправкой во внешнюю модель запрос обезличивается: имена, суммы и номера заменяются метками и возвращаются в ответ. Агент на локальной модели с тремя инструментами; строгий формат вызова и проверка кодом (честный провал: малая модель нарушает формат). Результат: локальный агент. Сбор агента с тремя инструментами на локальной модели, проектирование гибридной схемы для своей задачи, проведение мини-аудита учебного контура по разделу об ИИ приказа № 117. Задание: настроить полномочия локального агента по принципу «только чтение и черновики».					
6.	Учётные записи, секреты, сетевые границы, журналы и мониторинг	Учётные записи, права и секреты в контуре: сервисные учётные записи модели, агента и инструментов, единый вход, разделение прав; секреты — только в хранилище или переменных окружения; честный провал — ключ доступа в базе знаний агента. Демонстрация: В учебном контуре спрятан ключ доступа к учётной системе — его видит любой пользователь поиска. Агент пытается обратиться к внешнему адресу — запрос блокируется и	4	1	2	1	-



		попадает в журнал. Сетевые границы и изоляция (сегментация, запрет исходящего доступа, контролируемый шлюз для разрешённых вызовов); журналы, мониторинг и оповещения сервера модели. Результат: сетевые правила, журналы и панель мониторинга учебного контура. Назначение прав всем компонентам, нахождение спрятанного ключа, настройка сетевого правила, журнала и трех оповещений. Задание: настроить мониторинг и журналирование своего учебного контура.					
7.	Обновления, резервное копирование, инциденты и стоимость владения	Обновление модели, базы знаний или инструмента как изменение системы: регрессионная проверка и откат; резервное копирование конфигураций, базы знаний, индексов, журналов, версий моделей; проверка восстановления и план восстановления. Демонстрация: Преподаватель «ломает» модель и индекс поиска — вы восстанавливаете контур по своему регламенту на время. Учебный инцидент: в базу знаний попал документ со спрятанной инструкцией, и агент начал готовить выгрузку данных. Реагирование на учебный инцидент (внедрённая инструкция в базе знаний) по журналам; стоимость владения на 3 года: оборудование, электричество, администрирование, обновления, люди — против облака РФ. Результат: разбор	4	1	2	1	-



		инцидента и расчёт стоимости владения. Отрабатывание восстановления и инцидента по ролям, подсчет стоимости владения контуром на три года в сравнении с облаком РФ. Составить регламент эксплуатации контура, включая смену ответственного и вывод контура из эксплуатации.					
8.	Предварительный проект размещения	Предварительный проект размещения ИИ в своей организации: компоненты, размещение, права, сети, журналы, резервирование, эксплуатация — с явными допущениями и обязательным разделом «открытые вопросы к ИБ и ИТ»; разбор проектов в парах. Результат: предварительный проект размещения. Проектируете предварительный вариант размещения ИИ в своей организации с допущениями и вопросами к ИТ и ИБ и оформляете его паспорт к защите. Задание: оформить паспорт контура.	2	-	1	1	-
9.	Итоговая аттестация	Зачет	2	-	-	-	2
	ИТОГО		32	8	12	10	2