Оглавление

Отзывы о книге «Agentic Mesh. Автономная экосистема агентов на базе GenAI»....15

От издательства....17

О научном редакторе русского издания....17

Предисловие....18

Введение....21

Чем книга не является....22
О чем книга....22
Для кого эта книга....23
Предварительные условия....23
Что вы узнаете из книги....24
Структура книги....25
Часть I. Основные понятия....25
Часть II. Определение агентной экосистемы: agentic mesh....26
Часть III. Построение агентной сетки....26
Условные обозначения....27
Благодарности....27

ЧАСТЬ I
ОСНОВНЫЕ ПОНЯТИЯ

Глава 1. Agentic mesh: основы....31

Появление LLM....33
Эпоха агентов....35
Определение понятия «агент»....36
Агенты сегодня....37
Агенты корпоративного уровня....39
Агентная сетка: экосистема агентов....41
Проблемы при использовании агентов....44
Перспективы использования агентов....45
Итоги....47

Глава 2. Прошлое, настоящее и будущее агентов....48

История агентов....49
Происхождение искусственного интеллекта....49

Эра машинного обучения ... 51
Революция в области глубокого обучения ... 52
Агенты сегодня ... 52
Архитектура трансформера ... 53
Эпоха LLM ... 53
Будущее агентов ... 55
Краткосрочные перспективы: основа для агентов корпоративного уровня ... 55
Среднесрочные перспективы: появление агентной сетки — экосистемы агентов ... 58
Долгосрочные перспективы: создание агентных бизнесов ... 60
Итоги ... 61

Глава 3. Агенты и рабочие потоки ИИ ... 62

Определение рабочих потоков ИИ ... 62
Распространенные типы рабочих потоков ИИ ... 63
Цепочка промптов ... 63
Маршрутизация ... 65
Параллелизация ... 67
Оркестрация ... 68
Рефлексия ... 69
Проблемы с рабочими потоками ИИ ... 71
Проблема «черного ящика» ... 71
Проблемы масштабирования ... 72
Граничные случаи ... 73
Сравнение рабочих потоков ИИ и агентов ... 74
Агенты расширяют рабочие потоки ИИ ... 75
Итоги ... 77

Глава 4. Основы работы агентов ... 78

Аналогия: агенты и люди ... 79
От человека к агенту ... 79
От команд к флотам агентов ... 81
От организаций к агентным экосистемам ... 83
Архитектура агента ... 85
Планирование задач ... 87
Выполнение задач ... 89
Решение задач ... 92
Применение инструментов ... 94
Память и контекст ... 95
Обучение ... 98
Сотрудничество и коммуникации ... 100
Итоги ... 102

ЧАСТЬ II
ОПРЕДЕЛЕНИЕ АГЕНТНОЙ ЭКОСИСТЕМЫ: AGENTIC MESH

Глава 5. Архитектура агентов 105

Принципы агентов 106
Достоверность и подотчетность 108
Надежность и долговечность 111
Объяснимость и отслеживаемость 111
Сотрудничество и интеллектуальность 114
Агентные компоненты 116
«Мозг» агентов 117
Память агентов 118
Контекст-инжиниринг и агенты 120
Инструменты агентов 123
Управление задачами 124
Создание плана задачи 125
Идентификация инструментов и агентов-сотрудников 127
Подстановка параметров 127
Выполнение плана задачи 128
Взаимодействия с агентами и диалоги 129
Модель передачи сообщений 129
Управление диалогами 132
Управление состоянием 134
Рабочие пространства 136
Идентичности и роли агентов 137
Типы агентов 138
Агенты, ориентированные на задачу 138
Агенты, ориентированные на цель 140
Симуляционные агенты 142
Агенты-наблюдатели 143
Паттерны агентов 144
Коммуникационные паттерны 145
Ролевые паттерны агентов 147
Организационные паттерны 150
Конфигурация агента 153
Идентичность, описание и назначение 154
Стратегия выполнения задач 155
Конфигурация безопасности 156
Политики и сертификация 157
Видимость агентов и инструментов 157
Итоги 158

Глава 6. Агенты корпоративного уровня 159
Микроагенты (микросервисные агенты) 160
Безопасность агентов 162
Базовая безопасность микросервисов 163
Безопасность контейнеров 164
Безопасность Kubernetes 165
Надежность агентов 166
Проблема надежности 166
Первопричина проблемы надежности 167
Потенциальные решения 169
Декомпозиция задач 171
Детерминированное выполнение 172
Специализация 172
Объяснимость агентов 175
Недостаток доверия 175
Объяснимость: уроки реального мира 176
Объяснение объяснимости 177
Объяснимые агенты 180
Масштабируемость агентов 180
Проблема масштабируемости 181
Распределенные архитектуры 184
Стандартные методы сотрудничества 186
Управление диалогом и состоянием 188
Возможности корпоративной агентной платформы 190
Агенты как кванты повторного использования 191
Масштабирование фундамента LLM 192
Обнаружение агентов 193
За пределами проблемы поиска 194
Поиск подходящего агента 195
Наблюдаемость и отслеживаемость агентов 197
Управляемость агентов 198
Тестирование агентов 199
Тестирование LLM 199
Переход к тестированию агентов 200
Тестирование микроагентов: детерминированность в вероятностной модели 201
AgentOps: DevOps для агентов 202
Итоги 203

Глава 7. Agentic mesh: агентная экосистема корпоративного уровня 204
Экосистемы и масштаб 205
Флоты агентов 206
Структура и композиция 206

Координация и операции ... 208
Плоскость управления экосистемой ... 209
Компоненты агентной сетки ... 210
Реестр ... 211
Монитор ... 214
Сервер взаимодействий ... 215
Маркетплейс ... 216
Рабочая среда ... 218
Прокси ... 219
Возможности сетки ... 219
Схема доверия ... 219
Операции ... 221
Управление жизненным циклом агента ... 221
Итоги ... 223

Глава 8. Agentic mesh: опыт пользователя ... 224

UX агентной сетки ... 226
Вход ... 228
Главный экран ... 229
Маркетплейс ... 229
Что такое агентный маркетплейс? ... 230
Сервисы маркетплейса ... 231
Поиск нужного агента ... 235
Рабочая среда потребителя: взаимодействие с агентом ... 236
Общие рабочие пространства для агентов ... 237
Чат-интерфейсы для агентов ... 241
Рабочая среда создателя ... 243
Регистрация метаданных агентов ... 244
Связывание агентов с маркетплейсом ... 244
Использование рабочих сред для управления жизненным циклом агентов ... 245
Сходство между рабочей средой создателя и PyPI ... 246
Рабочая среда доверия ... 246
Конфигурация политик ... 246
Закрепление политик за агентами ... 247
Сертификация агентов ... 248
Внутренняя и сторонняя сертификация ... 248
Управление жизненным циклом сертификации ... 249
Рабочая среда оператора ... 249
Наблюдаемость агентов ... 250
Диагностика и устранение неисправностей ... 250
Контроль за выполнением ... 251
Итоги ... 251

Глава 9. Agentic mesh: реестр ... 252
Реестр агентной сетки ... 253
Агенты ... 254
Диалоги ... 256
Взаимодействия ... 258
Рабочие пространства ... 260
Политики ... 263
Пользователи ... 265
Замечания по реализации ... 267
Итоги ... 268

Глава 10. Управление взаимодействиями ... 269
Управление взаимодействиями в агентной сетке ... 270
Коммуникации, управляемые событиями ... 271
HTTP vs коммуникации, управляемые событиями ... 271
Очереди сообщений: надежная доставка и персистентность ... 272
Pub/sub: динамическое и масштабируемое распределение ... 273
Воспроизведение событий ... 274
Мониторинг очередей ... 276
Коммуникации «пользователь — агент» ... 276
Жизненный цикл взаимодействий ... 279
Диалоги ... 281
Эндпоинты диалогов и взаимодействий ... 281
Коммуникации «агент — агент» ... 282
Агенты как шаги плана ... 282
Отправка сообщений ... 282
Оповещения для пользователей ... 284
Рабочие пространства ... 285
Решение об ответе ... 286
Действия с сообщениями в рабочем пространстве ... 287
Цели рабочего пространства ... 288
Рабочие пространства как суперконтекст ... 290
Итоги ... 292

Глава 11. Безопасность ... 293
mTLS ... 295
Аутентификация и авторизация ... 296
Управление секретами ... 299
Промпт-инъекция ... 301
Пример промпт-инъекции ... 303

Методы промпт-инъекций ... 305
Противодействие промпт-инъекции ... 306
Джейлбрейк ... 308
Мониторинг поведения ... 309
Аварийное восстановление ... 310
Итоги ... 311

Глава 12. Инфраструктура доверия и управление ... 312

Семиуровневая инфраструктура доверия ... 313
Уровень 1: идентификация и аутентификация ... 316
Жизненный цикл идентичности ... 316
Делегирование и область действия ... 317
Масштабирование идентичности ... 317
Мониторинг и аудит идентичностей ... 317
Доверие и идентичности ... 317
Уровень 2: авторизация и контроль доступа ... 318
Основы контроля доступа ... 318
Модель с нулевым доверием для агентов ... 319
Контроль, минимальные привилегии и управление жизненным циклом ... 319
Интеграция идентичности и федеративное управление ... 319
Практическая реализация безопасности при проектировании ... 320
Уровень 3: назначение и политики ... 321
Назначение: определение того, что делает агент ... 321
Политики: определение операционных ограничений ... 321
Уровень 4: планирование задач и объяснимость ... 323
Проблема: непрозрачные рассуждения в современных агентах ... 323
Выбор инструментов и сотрудников ... 323
Параметризация и выполнение шагов ... 324
Уровень 5: наблюдаемость и отслеживаемость ... 324
Видимость активности агентов ... 325
Сохранение мультиагентных контекстов задач ... 325
Операционный мониторинг и наблюдаемость системного уровня ... 326
Уровень 6: сертификация и комплаенс ... 327
Сертификация как структурированное предоставление гарантий ... 327
Оценка, надзор и повторная сертификация ... 328
Реестры доверия, метаданные и обнаруживаемость ... 328
Циклы обратной связи, контроль и долгосрочное доверие ... 329
Уровень 7: управление и контроль жизненного цикла ... 330
Управление агентами на практике ... 330
Жизненный цикл агента ... 331
Итоги ... 334

ЧАСТЬ III
ПОСТРОЕНИЕ AGENTIC MESH

Глава 13. Операционная модель и структура команд 337

Структура, процессы, технологии, политики и метрики 338
Структура (люди и агенты) 339
Процесс 339
Технология 339
Метрики 340
Политика 340
Другие аспекты 341
Структура флотов агентов 342
Флот как единица масштабирования сетки 343
Динамическая принадлежность и гибкие границы 344
Базовые сервисы как связующее звено 344
Ориентация на миссии 345
Ключевые роли в управлении флотами 346
Организационные паттерны для флотов 346
Структура команды агента 347
Владелец агента 349
Инженер агентов 350
Агентный *SRE* *351*
Руководитель по управлению и сертификации 351
Оценщик и наблюдатель в контуре управления 352
Ответственный по политикам и этике 352
Менеджер релизов 353
Факторы перехода 353
Последствия для людей и этика 354
Коммуникации, доверие и культурная адаптация 355
Структурированный переход: переподготовка, поддержка и управление 356
Будущее сферы труда 358
От автоматизации к автономности 360
Неравные последствия и поляризация персонала 361
Появление гибридных профессий и операционных моделей 362
Назначение человека, адаптируемость и непрерывное обучение 364
Итоги 365

Глава 14. Фабрика агентов: построение агентов в масштабе 366

Цикл разработки агентов 367
Построение агентов в масштабе 369
Флоты 370

Организация флотов ... 372
Построение флота ... 375
Организация работы агентов в масштабе ... 376
Развертывание флота ... 377
Мониторинг флота: агенты-наблюдатели ... 377
Обновление флота и вывод его из эксплуатации ... 378
Более отдаленное будущее ... 379
Агенты создают агентов ... 380
Бóльшие абстракции ... 380
Итоги ... 382

Глава 15. Практический план реализации ... 383

Стратегические основы ... 385
Фаза 1: формулировка стратегии ... 385
Фаза 2: проектирование архитектуры ... 386
Фаза 3: пайплайн кандидатов на идентификацию ... 386
Фаза 4: выбор MVP ... 387
Технологическая сборка и масштабирование ... 387
Построение технологической основы ... 389
Технологическая основа масштабирования ... 390
Технологическая основа безопасности ... 391
Управление моделями и операциями ... 392
Фабрики агентов и флотов ... 393
Построение агентной схемы корпоративного уровня ... 395
Построение флота агентов/экосистемы корпоративного уровня ... 397
DevSecOps для агентов/флотов ... 399
Создание фабрики агентов ... 401
Создание фабрики флотов ... 403
Организационная и операционная модель ... 404
Создание новой операционной модели ... 406
Управление изменениями ... 407
Обучение персонала и формирование навыков ... 408
Управление и сертификация ... 408
Создание схемы управления и сертификации для агентов ... 410
Создание схемы управления и сертификации для флотов ... 410
Итоги ... 411

Об авторах ... 413

Иллюстрация на обложке ... 414