UZCLOUD

Теневой AI

в корпоративном контуре

как сотрудники уже отправляют секреты компании
на зарубежные серверы и что с этим делать

Дмитрий Некрасов
Chief Product Officer

Теневой AI - это использование внешних AI-инструментов вне утвержденного контура, логов и политик маскирования.

UZCLOUD

- Юрист вставил договор в личный ChatGPT
- Продавец загрузил КП в Claude для улучшения текста
- HR отправил резюме кандидатов в Gemini
- Аналитик загрузил финансовую таблицу в AI-сервис
- Разработчик отправил код во внешний AI-ассистент
- Менеджер подключил стороннего бота к встрече для саммари

Статистика

UZCLOUD

57% сотрудников скрывают использование AI на работе

48% загрузили данные компании в публичные AI-инструменты

54% нарушений связаны с регулируемыми данными

60% инцидентов фигурируют личные приложения

Теневой AI - проблема безопасности?

Нет - это симптом продуктового вакуума внутри компании.

UZCLOUD

> **Если у вас нет официального AI-инструмента, это не значит, что AI не используется; это значит, что вы не видите использование**
>
> Итан Моллик — профессор Wharton, автор книги «Co-Intelligence»

UZCLOUD

Почему это уже происходит?

68% не успевают за темпом работы

90% пользователей говорят, что AI экономит время

85% что помогает сосредоточиться на важном

84% что помогает быть креативнее

UZCLOUD

Что на самом деле утекает?

- Личные данные
- Финансы
- Интеллектуальная собственность
- Программный код
- Учётные данные
- Протоколы встреч

Что делать?

Может запретить?

UZCLOUD

90% организаций блокируют как минимум одно GenAI-приложение

47% пользователей всё равно используют личные неуправляемые аккаунты

Microsoft фиксирует массовый BYOAI

KPMG скрытое использование и загрузка корпоративных данных в public AI

Следствие: запрет сокращает видимость быстрее, чем реальное использование

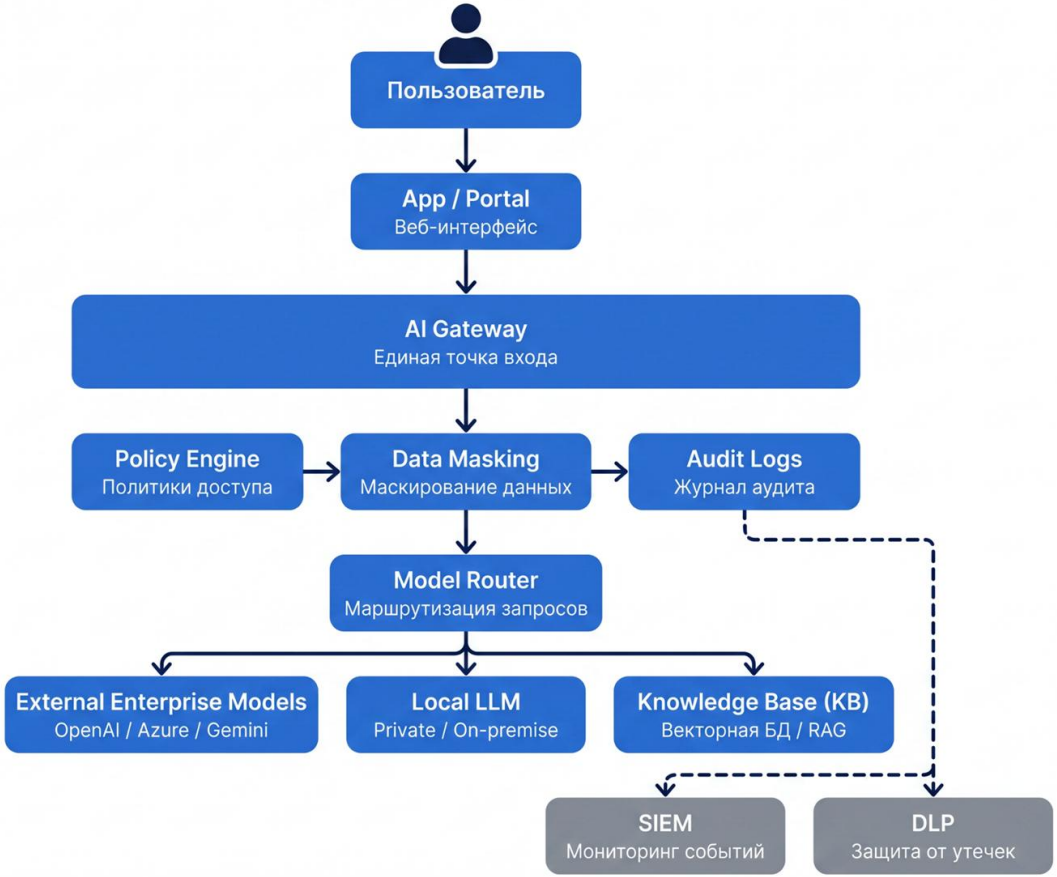
UZCLOUD

Какие способы контроля реально есть?

Стратегия	Ценность и возможности	Риски и барьеры	Сфера применения
Полный запрет	Снижение формального риска	Игнорирование реальности, уход сотрудников в тень	Только как экстренная мера
Политики и обучение	Фундамент культуры безопасности	Отсутствие контроля над исполнением	Базовый уровень для всех
Корпоративные лицензии	Управляемый доступ и защита данных	Ограниченная видимость сценариев	Массовые рабочие задачи
Частные модели (Private LLM)	Изоляция критических данных	Высокая стоимость, сложность поддержки	Работа с гостайной/критикой
AI-шлюз (Gateway)	Единая точка контроля и аудита	Требует настройки инфраструктуры	Операционная модель ★ Быстрый выбор
Гибридная схема	Баланс безопасности и скорости	Высокая сложность архитектуры	Целевой стандарт компании ★ Лучший выбор

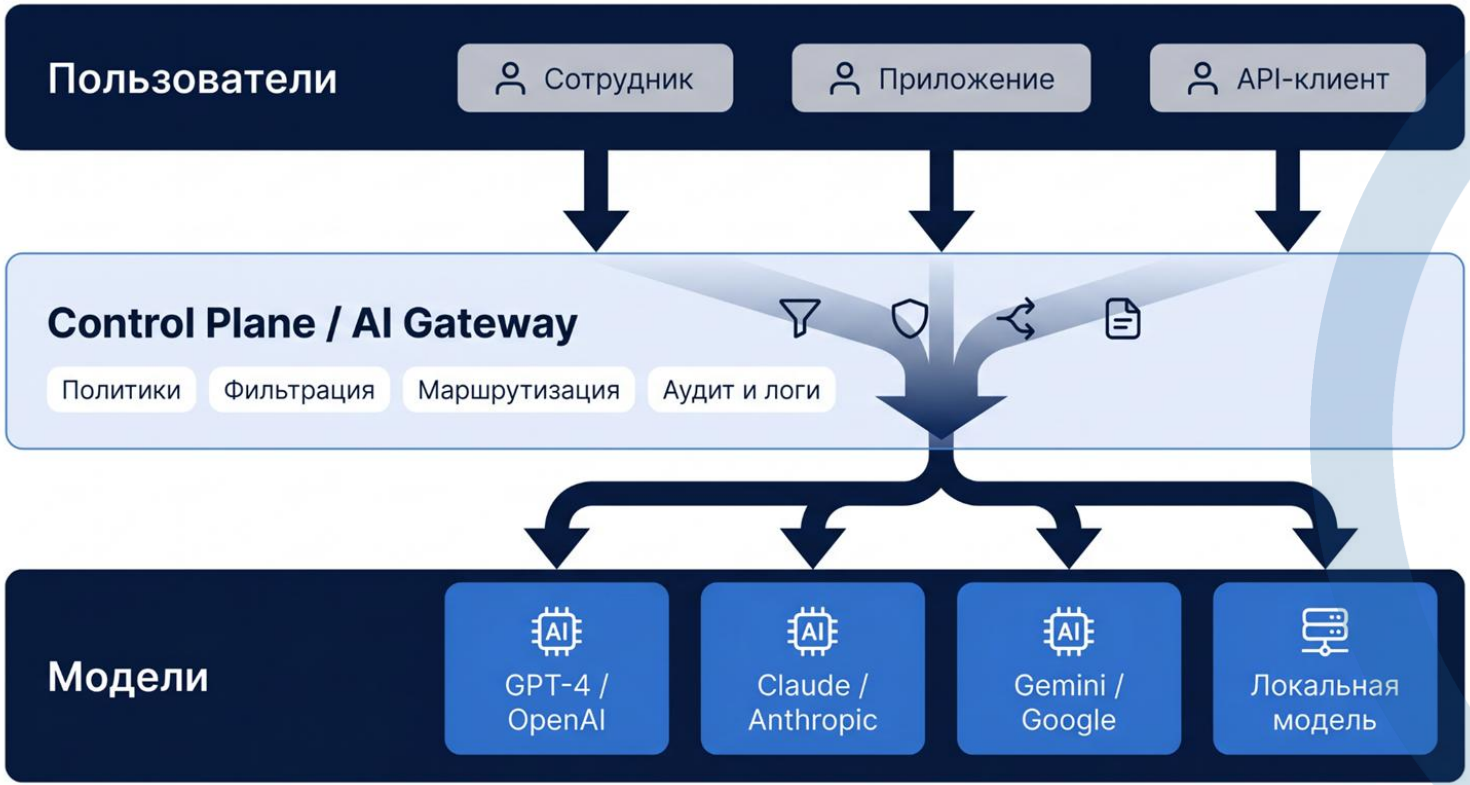
UZCLOUD

Целевая архитектура безопасного AI-шлюза



UZCLOUD

AI шлюз как Control Plane



UZCLOUD

В каких сценариях это работает?

Классификация данных | Проверка прав доступа (ACL) | Маскирование | Журналирование | Запрет на экспорт

AI шлюз - большой брат?

Вы можете спросить:

"Как же приватность?

Ведь если мы видим все запросы,

мы превращаемся в слежку".

UZCLOUD

Как вернуть контроль над AI за 5 шагов?

UZCLOUD

Что проверить в своей компании

- [x] Знаем ли мы, какие AI-инструменты реально используют сотрудники?
- [x] Можем ли мы отличить личные аккаунты от корпоративных?
- [x] Какие данные сотрудники отправляют в AI?
- [x] Есть ли список разрешённых и запрещённых AI-сценариев?
- [x] Есть ли классификация данных для AI?
- [x] Есть ли технический контроль, а не только политика в PDF?
- [x] Есть ли официальный AI-инструмент, которым удобно пользоваться?
- [x] Логируются ли AI-запросы и ответы?
- [x] Есть ли модель управления затратами?
- [x] Есть ли план перевода теневых сценариев в управляемый контур?

Спасибо за внимание!

UZCLOUD

Дмитрий Некрасов

Chief Product Officer

- ✓ ex. Samolet Development
- ✓ ex. MWS
- ✓ ex. MTS

Telegram

LinkedIn