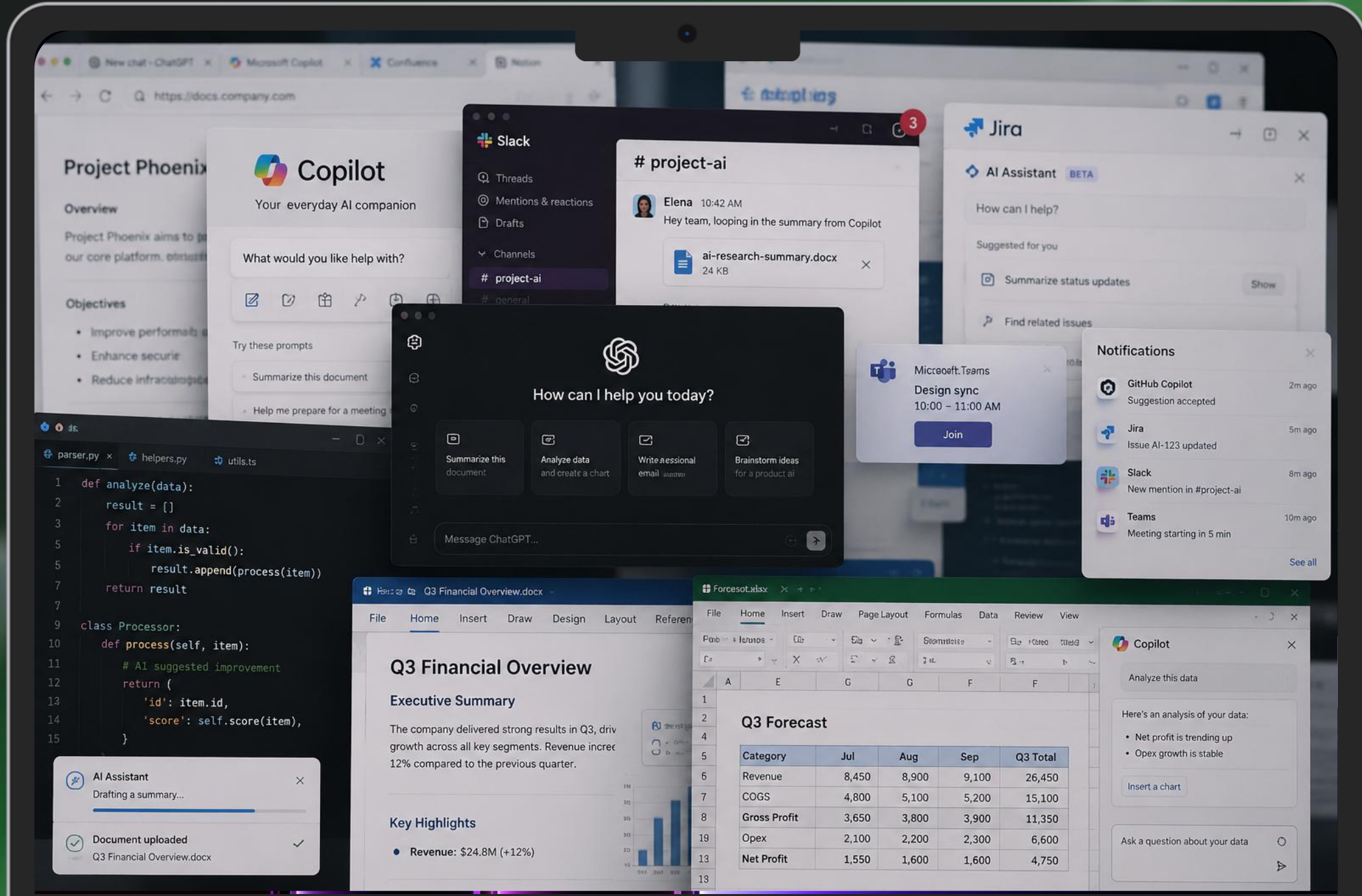


Shadow AI: пока CISO пишет политику, бизнес уже работает с ИИ

Лагоденко Андрей,
CISO Домклик
Май'26

Shadow AI



The image displays a central laptop screen filled with overlapping windows of various AI-powered productivity tools. At the top left, a browser window shows a document titled "Project Phoenix" with an overview and objectives. Overlaid on this is the Microsoft Copilot interface, which asks "What would you like help with?" and provides prompts like "Summarize this document" and "Help me prepare for a meeting". To the right, a Slack window for the "# project-ai" channel shows a message from Elena: "Hey team, looping in the summary from Copilot" with an attached file "ai-research-summary.docx". Further right, a Jira window features an "AI Assistant BETA" interface with suggestions like "Summarize status updates" and "Find related issues". In the foreground, a Microsoft Teams notification for a "Design sync" is visible. On the bottom left, a code editor window shows Python code for a data analysis function and a class. At the bottom center, a Microsoft Word document titled "Q3 Financial Overview.docx" is open, displaying an "Executive Summary" and a "Q3 Forecast" table. On the bottom right, another Copilot window is shown analyzing data from the financial overview, providing insights like "Net profit is trending up" and "Opex growth is stable". A notification tray at the bottom left shows "AI Assistant" drafting a summary and "Document uploaded" for the financial overview document.

Выглядит как обычная работа

1 Dev



“Напиши SQL для отчёта”



2 HR



“Сделай summary интервью”



3 Analyst



“Проанализируй Excel”



4 PM



“Подготовь Jira update”



5 Sales



“Сделай follow-up клиенту”



6 Support



“Суммаризируй тикеты”



А что же с потоками данных?

1. ДАННЫЕ КОМПАНИИ

То, с чем мы работаем каждый день



Документы



Код



Excel



Звонки



HR



Jira

2. ДЕЙСТВИЯ СОТРУДНИКОВ

Повседневные запросы к ИИ



Сделай summary



Напиши SQL



Подготовь письмо



Проанализируй Excel

3. КУДА УХОДЯТ ДАННЫЕ

Внешние AI-ресурсы



Public AI Chats

ChatGPT, Claude,
Gemini и другие



AI-enabled SaaS

Microsoft 365 Copilot,
Notion AI, Slack AI,
Jira AI и другие



Agents & Plugins

AI-агенты, плагины,
интеграции, расширения
браузера и IDE

Shadow AI побеждает за счет скорости



Отчёт

2 часа → 20 минут



Анализ Excel

1 час → 10 минут



Ответ клиенту

30 минут → 5 минут



Запрет AI не контроль – а потеря видимости

ЧТО ДЕЛАЕТ КОМПАНИЯ



AI policy



Access denied



Firewall block

ЧТО ПРОИСХОДИТ РЕАЛЬНО



Личный телефон



Личный аккаунт



Браузер AI

Shadow AI прорастает в бизнес



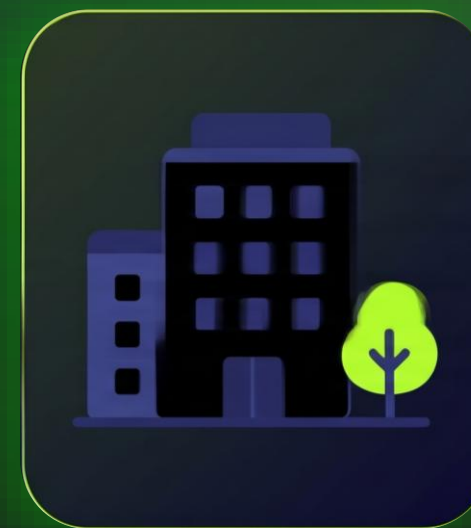
Личное
использование
AI



Делимся
с командой

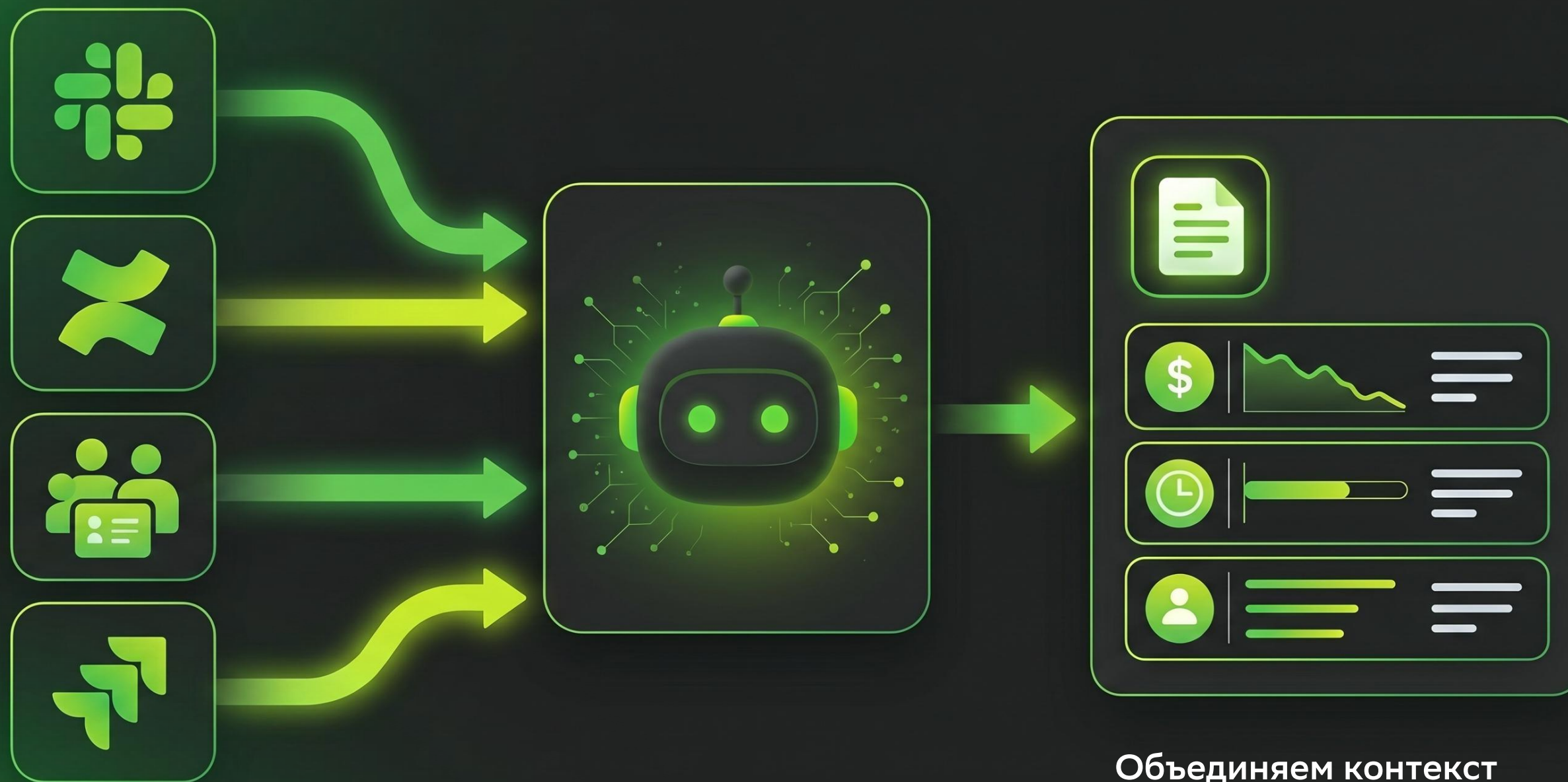


С интеграциями
еще удобней



Часть бизнес-
процесса

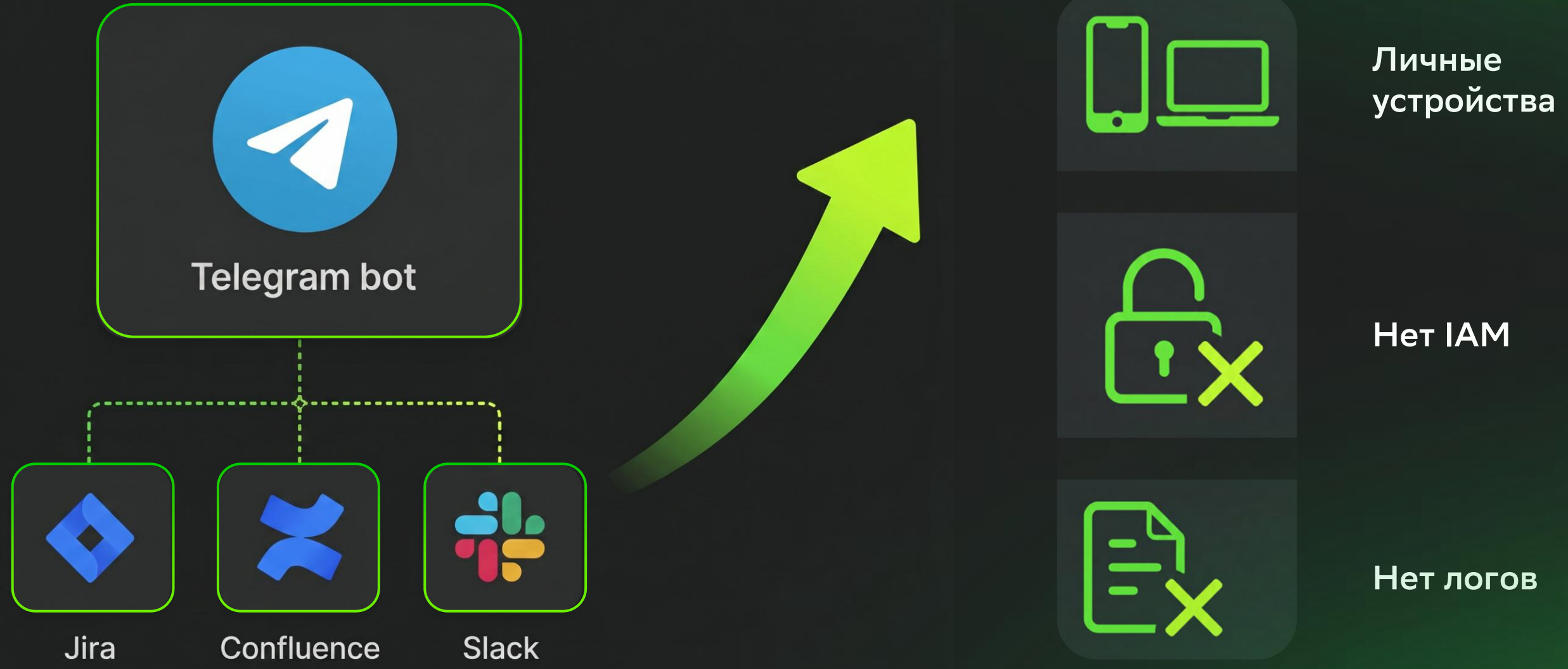
КЕЙС #1 Саммаризация



Объединяем контекст

(раскрывая конфиденциальные данные)

Кейс #2. Телеграм-бот



Главная ошибка

политики

ревью

риски

согласования

AI-платформа

AI шлюз

процессы

Реестр моделей

регламенты

red teaming

compliance

архитектура



Понять, где уже используют?



Дать согласованный AI



Ввести простые правила

Как реально найти Shadow AI

Браузер и расширения

ГДЕ СМОТРЕТЬ

Proxy / EDR / NGFW / Logs

ЧТО ИСКАТЬ

ChatGPT, Claude, Gemini, etc.



Teams / Slack / Telegram

ГДЕ СМОТРЕТЬ

Чаты, боты, каналы

ЧТО ИСКАТЬ

LLM-, summary-, search- боты



Загрузка данных во внешние AI

ГДЕ СМОТРЕТЬ

Proxy / DLP / Logs

ЧТО ИСКАТЬ

Документы, Excel, Code



Интервью с командами

Что спрашивать

где AI уже экономит время?

без каких AI инструментов неудобно?

что используют “временно”?

где хотелось бы начать использовать?



Как дать сотрудникам согласованный AI

Подход	Где применять	Что учесть
Корпоративные аккаунты у коммерческих AI	Быстрый старт и хороший UX	Логирование, SSO, использование данных для дообучения
On-prem модели	Чувствительные данные, RAG	Качество моделей, GPU/Инфраструктура, TCO
AI Gateway	Контролировать разные AI-сервисов	Логирование, контроль файлов

Правила, которые люди **реально** читают

Не отправлять
секреты и креды

Не загружать
персональные данные
(особенно клиентские)

Всегда проверять
ответ модели, прежде
чем использовать

Внешний AI для
неконфиденциальных
данных

В работе
использовать только
согласованный AI

Не все AI-риски одинаково опасны

Клиентские данные

Персональные данные,
договоры, обращения



ИТ/ИБ-архитектура

Репозитории, скрипты, внутренняя
логика, архитектура и СЗИ



Доступ к внутренним данным

Jira, Confluence, Slack, CRM,
базы знаний



Агенты

Боты, автоматизация, агенты
и мультиагентные системы

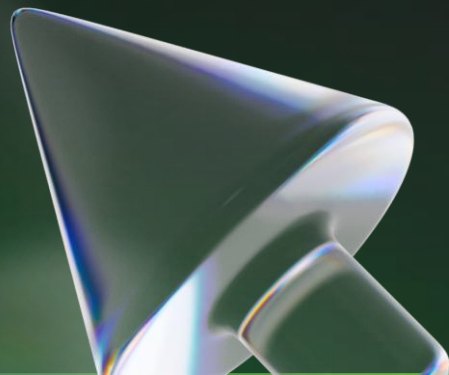


Управляемость в повторяемости

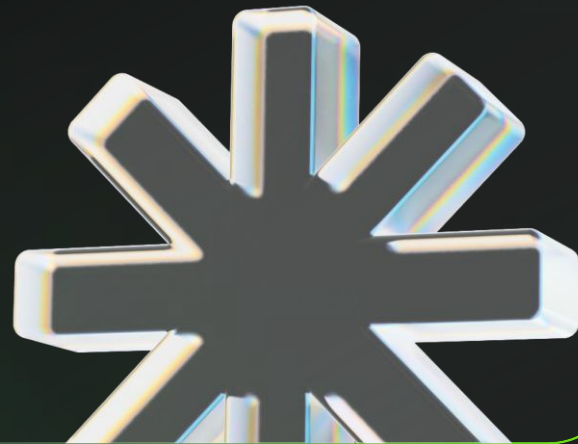


Вместо выводов

AI с нами
надолго



Заборы
не помогут



Управляемость
возможна

