



АСТРА ИИ
[КОД]

Агентная система
для разработки
в защищённом
контуре



ИИ-напарник для инженера, который работает с ним на его рабочем месте

1

Инженер ставит задачу

Обычным текстом, как коллеге:
«Добавь авторизацию через
LDAP и напиши тесты»

Агент разбирается в коде,
составляет план, показывает
его для согласования
и только потом действует

2

Агент делает работу

Читает весь проект, пишет код,
запускает тесты, исправляет
ошибки

Защита от опасных действий
встроена: случайно удалить
базу или обнулить
репозиторий невозможно

3

Всё остаётся внутри

Ни строчки кода,
ни одного запроса
не уходит за периметр
организации

Модель, данные, история
запросов — всё в контуре
или в облаке «Группы Астры»

Запрещать нельзя легализовать

Что происходит на практике

Более 60% инженеров уже применяют ИИ, но вне контролируемого контура:

- / Через личные аккаунты и обходные каналы
- / Передавая данные на зарубежные серверы
- / Без логов, без аудит-следа

Регуляторные требования

- / Штраф (по 152-ФЗ) — **до ₽3 млн**
- / Ст. 274.1 УК РФ: личная ответственность руководителя при инциденте
- / Передача данных за рубеж без согласования **недопустима**

Операционный разрыв

- / Команды с легальным ИИ работают **в 1,5–2 раза быстрее**
- / Отставание по срокам вывода продуктов на ключевых направлениях
- / Повышенная текучка: люди уходят туда, где есть современные инструменты

Для КИИ, работы с персональными данными и компаний, которым важна безопасность

Нужен инструмент, при котором служба безопасности видит каждый запрос, код остаётся в периметре, а инженер работает без обходных каналов

Ни байта за периметр

Нулевая поверхность атаки снаружи. Полный аудит внутри
Путь сертификации ФСТЭК документирован

Изоляция

- / 0 исходящих соединений с кодом клиента
- / Модель работает в закрытой сети
- / Изолированный режим без внешних сетей — для контуров обработки защищаемой информации
- / Данные остаются в вашем ЦОДе физически и юридически

Безопасность «из коробки»

- / Правила блокировки опасных команд:
`rm -rf`, `git reset --hard`, `mkfs`,
`DROP DATABASE`
- / Режим планирования —
согласование плана перед исполнением
- / Полный журнал аудита всех запросов в системе мониторинга
- / Дочерние агенты — «только чтение» по умолчанию

Регуляторика

- / Открытые модели без зависимости от иностранных лицензий
- / Стек «Группы Астра» в реестре отечественного ПО
- / Сертификация ФСТЭК — план Q4 2027
- / Соответствие 152-ФЗ и требованиям КИИ

Директор по информационной безопасности получает все ИИ-запросы в системе мониторинга, никакого «теневого» ИИ, полный журнал аудита для регулятора

Возможности решения

Это система для автоматизации процессов разработки безопасного программного обеспечения с помощью искусственного интеллекта для критической информационной инфраструктуры

Написание, отладка и рефакторинг кода прямо из командной строки

1

Понимание больших кодовых баз — может читать и анализировать множество файлов в проекте

2

Автоматизация многошаговых задач, включая запуск команд и взаимодействие с файловой системой

3

Интеграция с внешними сервисами через MCP-серверы

4

Выполнение рутинных задач: исправление багов, написание тестов, комментариев, документации, обновление зависимостей

5

Нативная поддержка ПК СВ «Брест», ОС Astra Linux, платформ «Боецман» и GitFlic— интегрированы знания о функциях и возможностях решений

6

Агентная система — это полноценный помощник, способный взять на себя выполнение задач, а не только поговорить об их исполнении

Архитектура решения

Рабочее место инженера — локально

Клиент

Терминал, web, плагин OpenIDE, голос и изображения

Ядро агента

Оркестрация сессий, планирование, дочерние агенты, память и контекст, расширения (MCP, Hooks, Skills)

Корпоративная «песочница» — серверная часть в контуре заказчика

Шлюз и доступ

- / Единая точка входа (ГОСТ TLS)
- / Вход через ALD Pro, SSO
- / Роли и права (RBAC)
- / Профили доступа агента

Инференс и исполнение

- / Шлюз моделей + ИИ-фильтр
- / Изоляция инструментов в «песочнице»
- / Правила блокировки опасных операций
- / Маскирование секретов

Аудит и контроль

- / Журнал в SIEM (ГОСТ Р 59548)
- / Политики и соответствие требованиям ФСТЭК
- / Консоль администрирования
- / Управление обновлениями в контуре

Экосистема «Группы Астра» — нативные интеграции



Модели [MLOps / LLMOps]



Код, CI/CD, ASOC



Каталог и вход



Monitoring + SIEM

Менеджер секретов

Как это работает в жизни?

Три проверяемых сценария с измеримым эффектом на пилоте

Больше результата без роста штата



Рутинная «съедает» время команды: шаблонный код, тесты по спецификации, конфигурации



Ускоряем генерацию рутинных, хорошо специфицированных задач, освобождаем инженеров для сложной работы



Сокращение времени цикла на рутинном сегменте при контроле переделок и дефектов

Снятие зависимости от инженеров эксплуатации



Новый сервис простаивает 3–7 дней в очереди к перегруженному сотруднику



Готовим сценарии сборки, контейнеры, манифесты развёртывания и конфигурации — инженеру остаётся проверка, а не написание с нуля



Время ожидания сокращается с дней до часов

Работа с унаследованным кодом



Унаследованный код никто не понимает; адаптация нового сотрудника занимает недели, ~58% времени уходит на понимание кода.



Объясняем логику модулей, отвечаем на вопросы по коду, ускоряем первый самостоятельный вклад нового сотрудника



Сокращение времени до первого изменения с обязательной проверкой ответов агента

Потенциал экономии от ИИ-инструментов

Расчёт: ФОТ × доля автоматизируемых задач × ускорение на них

Для команды в 150 разработчиков

270 млн ФОТ команды

Пессимистичный сценарий

43,2 млн

Оптимистичный сценарий

82,3 млн

от 45%

Рутинных задач, которые
могут быть автоматизированы

от 35%

Минимальное ускорение,
получаемое от автоматизации



до 61%

Рутинных задач, которые
могут быть автоматизированы

до 50%

Оптимальное ускорение,
получаемое от автоматизации

Как мы считаем эффект

Мы не обещаем единый процент на всю команду — он не выдерживает проверки
Эффект измеряется на пилоте по каждому сценарию отдельно и с контролем качества: ускорение «засчитывается», только если переделки, дублирование и частота отказов не растут относительно исходных показателей



Экосистема безопасных ИИ-решений

АСТРА ИИ [КОД]

Агентная система для разработки
в защищённом контуре

- / Создание сложных агентных систем
- / Работа с готовыми агентами на уровне кода

АСТРА ИИ [ПЛАТФОРМА]

Система для создания
ИИ-решений в режиме low-code

- / Визуальное отображение и доработка готовых агентов на уровне принципиальных схем
- / Минимальный срок запуска новых агентных сервисов
- / Безопасная среда исполнения пайплайнов

АСТРА ИИ [ЦИФРОВОЙ ОФИС]

Корпоративное ИИ-приложение
для каждодневных бизнес-задач

- / Работа пользователей в удобной и полностью контролируемой внутренней ИИ-среде

АСТРА ИИ [ХАБ]

Единый корпоративный
центр управления ИИ,
основанный на
инференс-платформе
«Боцман»

Конкурентные преимущества — чего нет у других

Главное — безопасность и встроенные практики ИБ

Преимущество	Экосистемный вендор А	Экосистемный вендор Б	облачный ИИ-сервис	Нишевый ИИ-ассистент	«Астра ИИ [КОД]»
Killer-функции — ядро продукта					
Безопасность «из коробки» — практики ИБ «Группы Астра» в процессе	—	—	—	—	✓
Готовый процесс под ФСТЭК / ГОСТ Р 56939 «под ключ»	—	—	—	—	✓
Фабрика разработки ПО (АСТРА ИИ [КОД] + АСТРА ИИ [ТРАЕКТОРИЯ])	—	—	—	—	✓
Сквозные интеграции со стеком «Группы Астра» (Astra Linux, «Боцман», ПК СВ «Брест», GitFlic)	—	—	—	—	✓
Дифференциаторы — нет у конкурентов					
Полный журнал каждого ИИ-запроса в SIEM заказчика	—	—	—	—	✓
Работа без интернета (изолированный контур, air-gap)	—	—	—	—	✓
Нейтральный поставщик: «Группа Астра» — не конкурент клиенту	—	—	Частично	Да	✓
Полнота решения — единый комплекс					
Полноценная агентная система: терминал + инференс-платформа	Частично	Частично	—	—	✓
Вендорная поддержка всего решения — единый SLA на весь стек	—	—	Частично	—	✓
Профильные скиллы под ГОЗ, банковский комплаенс, отраслевой стек	—	—	—	—	✓

Почему «Группа Астра»

Нейтральный поставщик

Покупать у конкурента ключевой инструмент разработки — стратегический риск.

«Группа Астра» не конкурирует с клиентами.

Мы уже внутри периметра

18 500+

организаций

Встроенное доверие

76% Отечественных ОС


В тысячах организаций продукты «Группы Астра» уже прошли проверку временем.



Нативно работает с другими продуктами компании

1 экосистема

1 договор

1 точка ответственности

Поддержка от вендора

Почему не «сделать самим на OpenCode»:

Открытый код — не продукт.

Развернуть, настроить и поддерживать его в закрытом контуре — это отдельный инженер по ИИ.

Его зарплата за год больше, чем подписка на «Астра ИИ [КОД]» для всей команды.

Обновления, безопасность, совместимость с новыми моделями обычно «ложатся» на клиента.

Мы берём всё это на себя.

«Астра ИИ» — это не только экосистема решений, но и центр компетенций, который помогает заказчикам встраивать ИИ в продукты, процессы и решения

Формируем единый центр экспертизы по LLM, ML и безопасному внедрению

1

Обучаем и адаптируем сотрудников к ИИ-среде

3

Помогаем находить сценарии, где ИИ усиливает уже существующие компетенции

2

Обеспечиваем единый подход к безопасным и доверенным ИИ-решениям

4

Ключевой принцип взаимодействия —
поддержка и экспертиза на каждом этапе внедрения и эксплуатации экосистемы



АСТРА ИИ



Источники и методология

Все цифры в расчётах опираются на независимые исследования, а не на маркетинг поставщиков

Производительность и эффект ИИ

McKinsey, 2024 — «The economic potential of generative AI»

Ускорение генерации кода на 35–45%, документирования – на 45–50%, рефакторинга – на 20–30%

GitHub Copilot RCT — Peng, Kalliamvakou, Cihon, Demirer
(Microsoft Research / GitHub / MIT Sloan), arXiv:2302.06590
+55,8% на изолированной задаче

METR, 2025 — Becker, Rush, Barnes, Rein, arXiv:2507.09089
На знакомом legacy эффект может быть отрицательным (–19%)

DORA, 2024–2025 — Google, State of DevOps Report
Связь ИИ с пропускной способностью и стабильностью доставки

Качество и безопасность кода

GitClear, 2025 — анализ 211 млн строк
Рост дублирования ×8, code churn 3,1% → 5,7%

USENIX Security, 2025 — Spracklen et al., arXiv:2406.10279
19,7% рекомендованных ИИ пакетов не существует
(риск подмены зависимостей)

Stack Overflow Developer Survey, 2025 — 49 000 респондентов
66% жалуются на «почти правильные» ответы ИИ

Xia et al., 2018 — IEEE TS
Разработчики тратят ~58% времени на понимание кода

Методологическая основа

Каркасы SPACE (Forsgren et al., ACM Queue, 2021) и DevEx (Noda et al., ACM Queue, 2023)
Продуктивность многомерна: каждой метрике скорости придаётся встречная метрика качества
Эффект измеряется на пилоте на уровне отдельных задач, а не сравнением групп

Ссылки на все
источники



Расчёт эффекта построен на рецензируемых контролируемых экспериментах и отраслевых отчётах
Цель ставится по типу задачи, с учетом сохранения контролем качества