

Чек-лист пилота Claude Code: контроль IDE-контекста

Сохраните этот список как PDF-памятку для пилота. Он не заменяет внутреннюю политику ИБ, но помогает проверить конкретные настройки, доступ к файлам и наблюдаемые следы в сессии.

Подготовьте тестовый контур

- Создайте отдельный тестовый репозиторий.
- Добавьте искусственные секреты, тестовые конфиденциальные документы и реалистичные имена файлов.
- Не используйте реальные секреты и персональные данные для первой проверки.
- Определите, какие пути должны быть недоступны Claude Code.

Проверьте подключение к IDE

- Зафиксируйте способ запуска Claude Code: внешний терминал или интегрированная среда.
- Проверьте effective value параметра autoConnectIde.
- Проверьте влияние переменной CLAUDE_CODE_AUTO_CONNECT_IDE.
- Повторите одинаковую задачу при активной IDE и без неё.

Проверьте доступ к файлам

- Настройте deny-правила Read для тестовых чувствительных путей.
- Убедитесь, что политика охватывает все определённые в пилоте места хранения чувствительных артефактов.
- Проверьте, что агент не читает защищённый файл по прямому запросу.
- Проверьте, что IDE-сигналы для защищённого пути не появляются в сессии.

Зафиксируйте результаты

- Сравните transcript до и после применения настроек и правил.
- Запишите итоговую конфигурацию и окружение запуска.
- Отметьте компромиссы для удобства разработчика.
- Определите владельца политики, порядок доставки настроек и разбор исключений.