



Реверс-инжиниринг

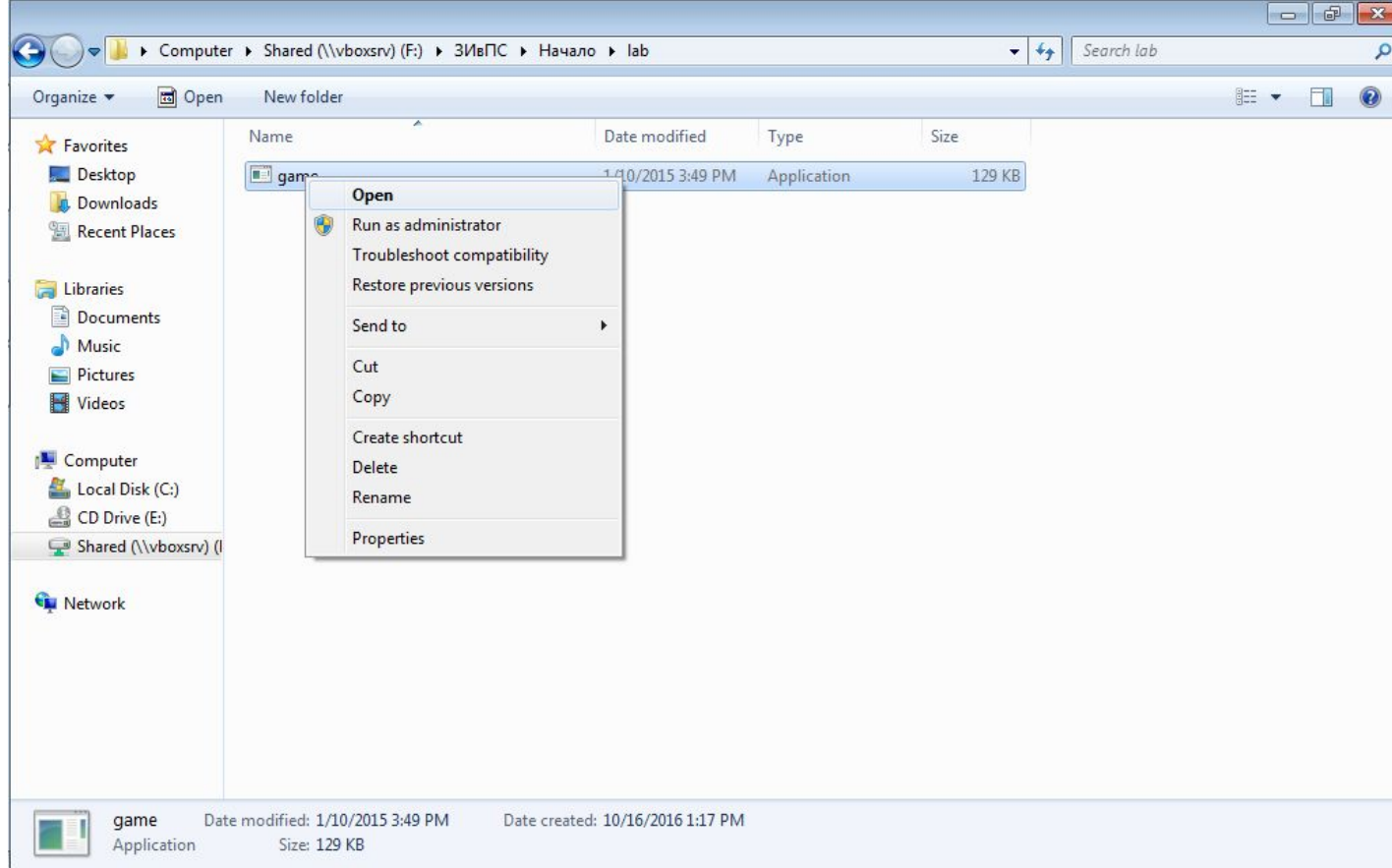
dotPeek



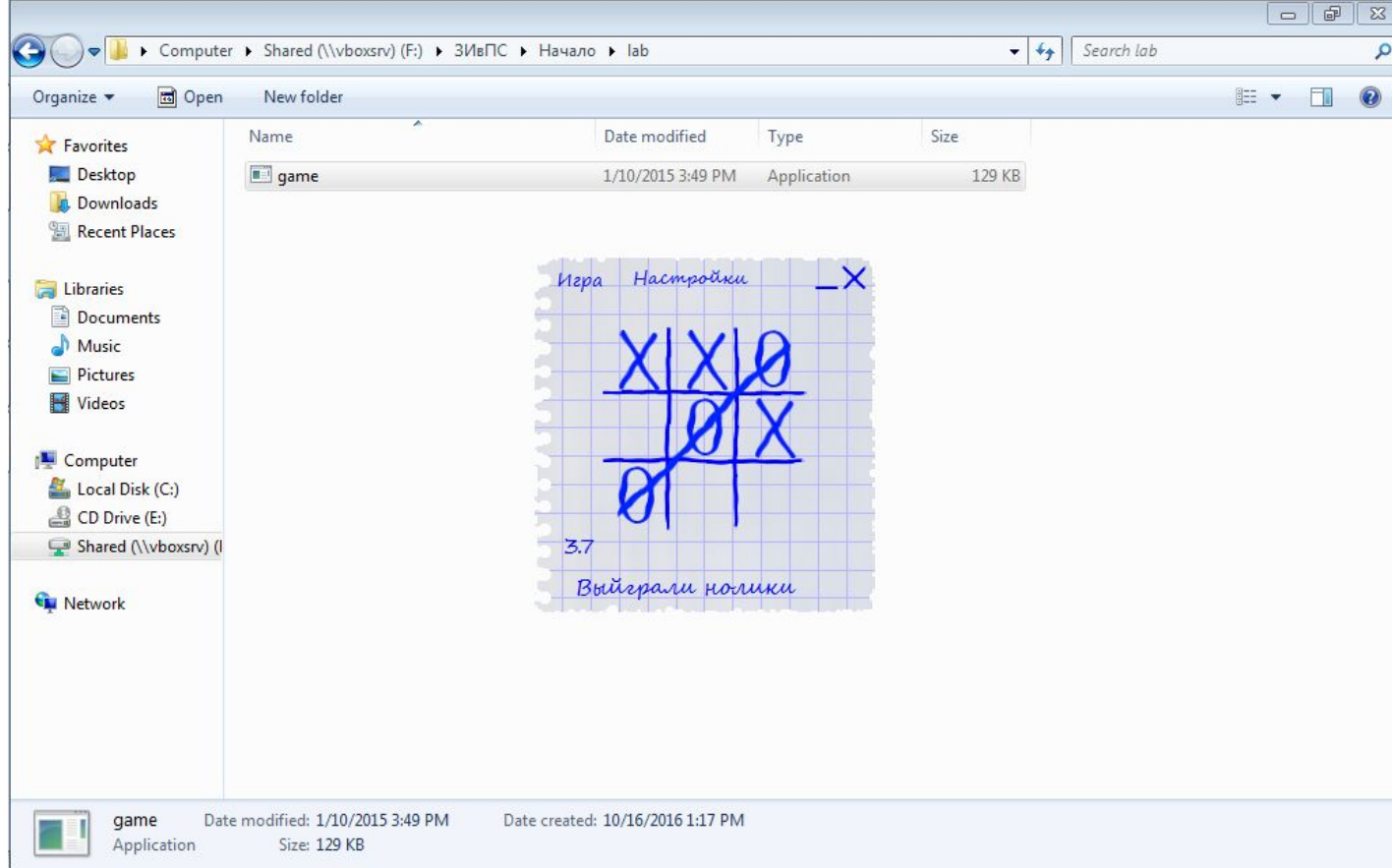
dotPeek

.Net decompiler

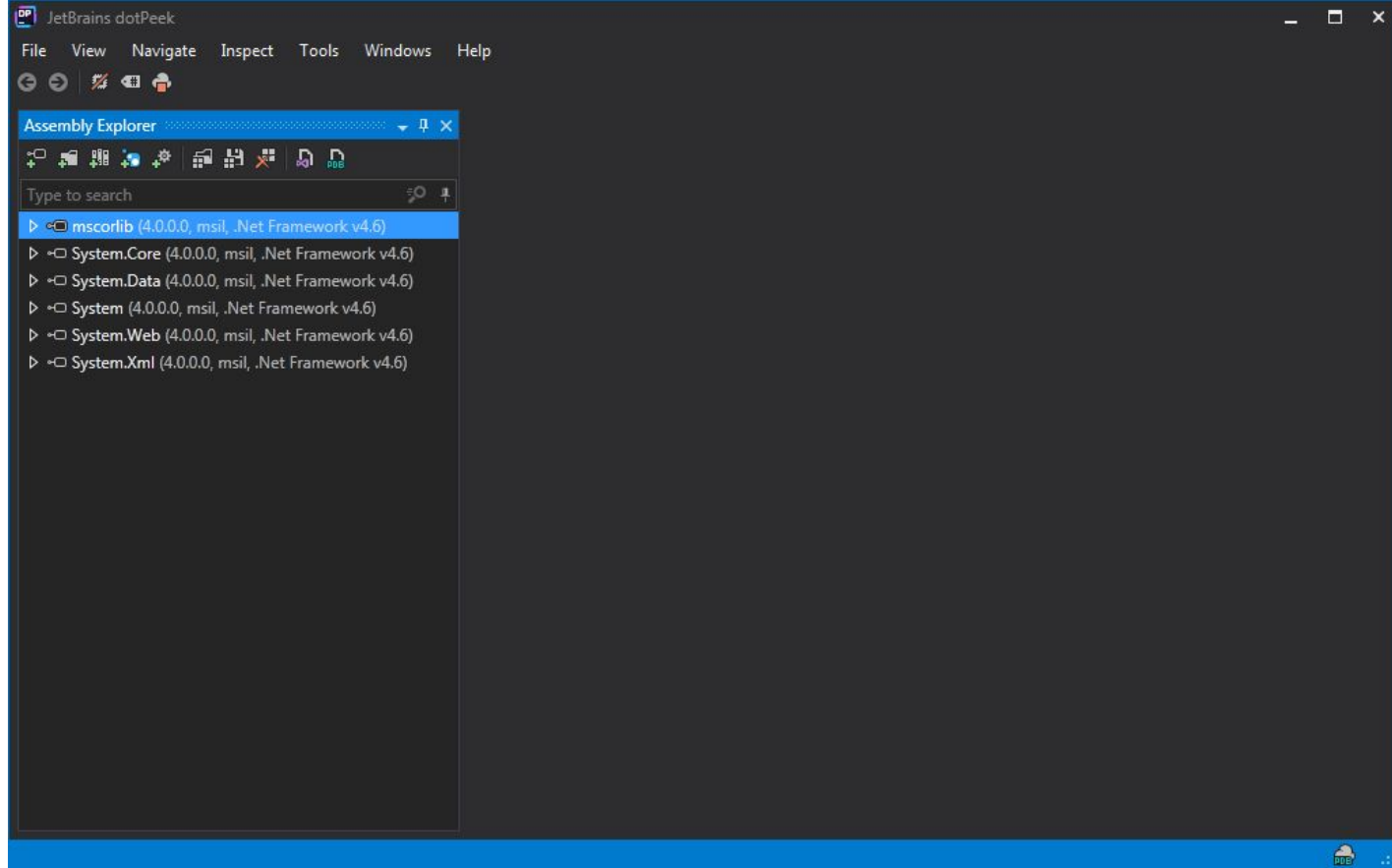
- Имеется .Net программа
- Исходный код недоступен
- Как внести изменения?



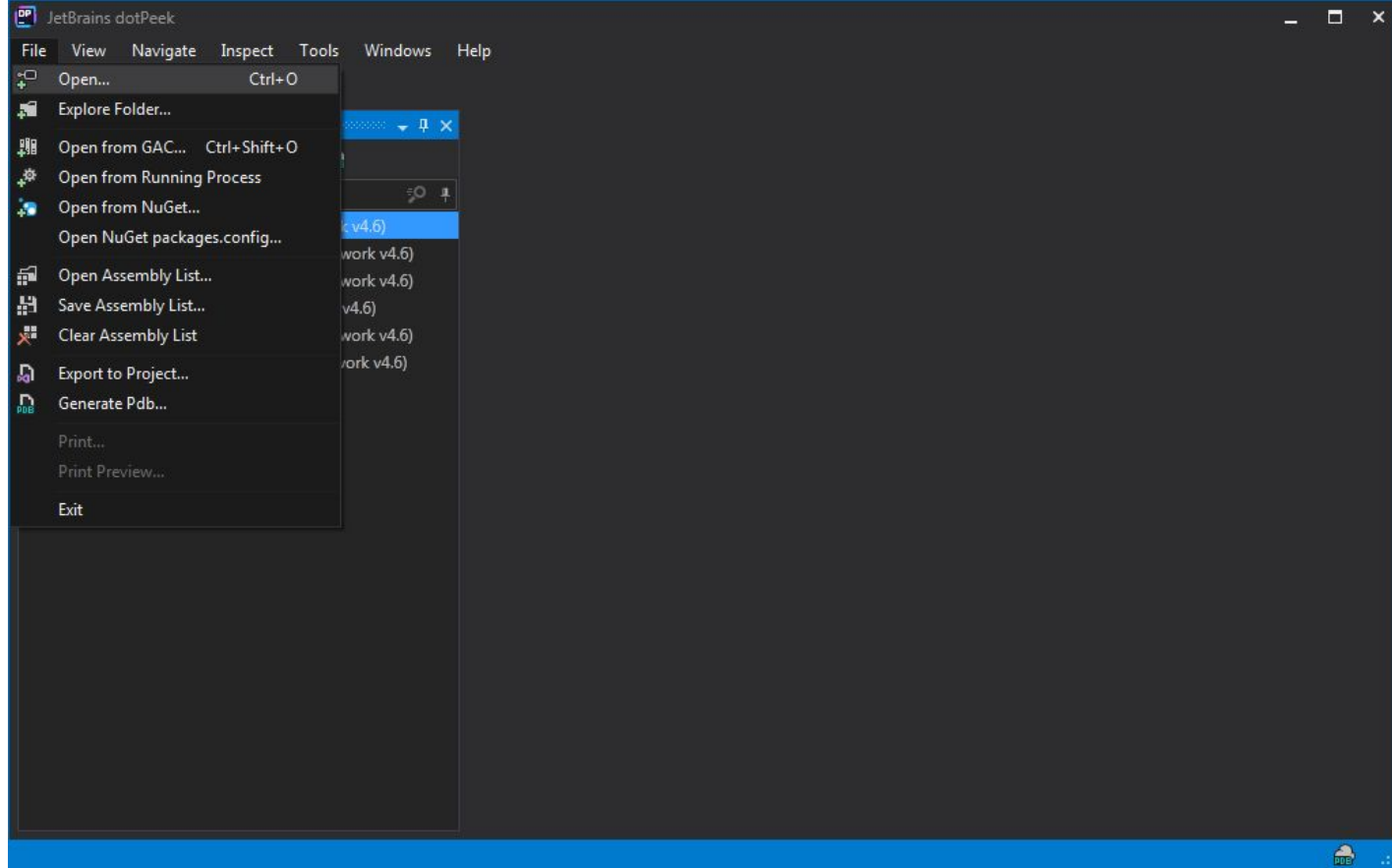
Проверим работоспособность



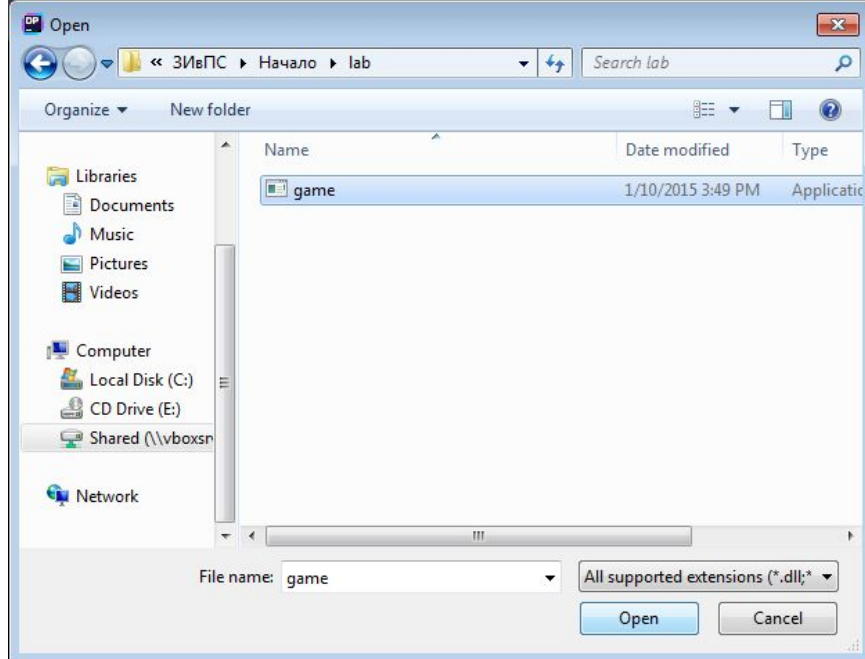
Работает корректно



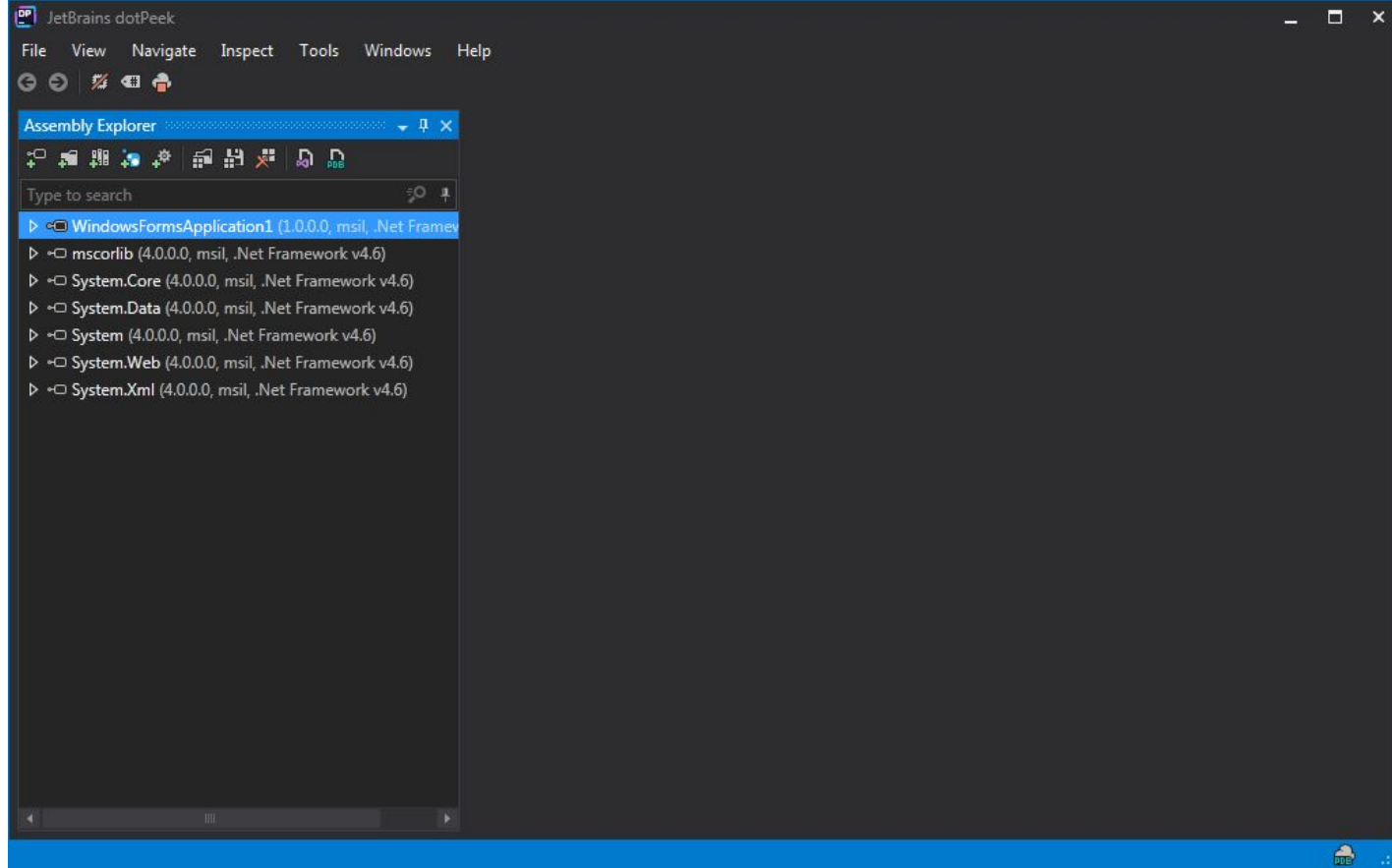
Интерфейс dotPeek



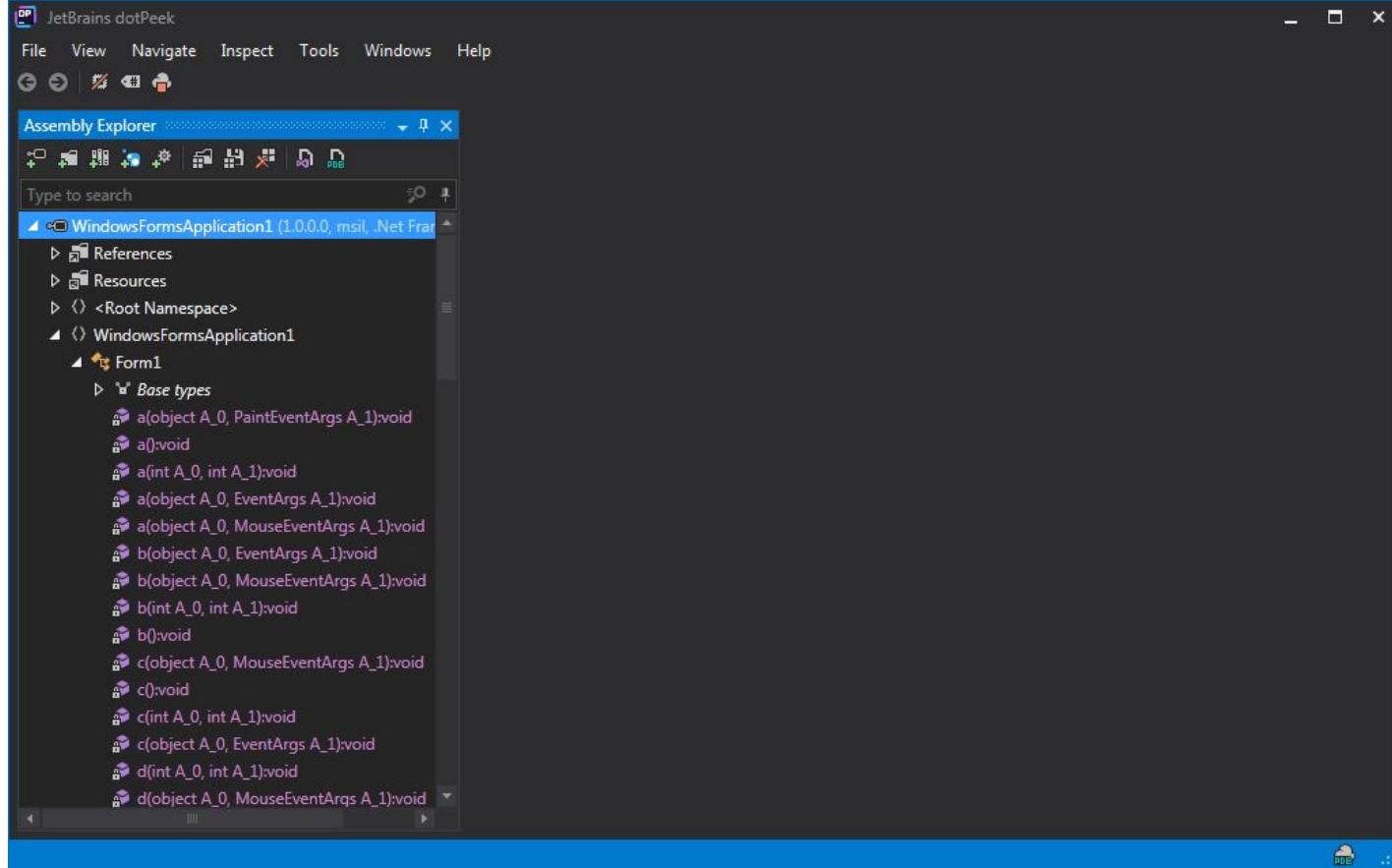
Добавим assembly



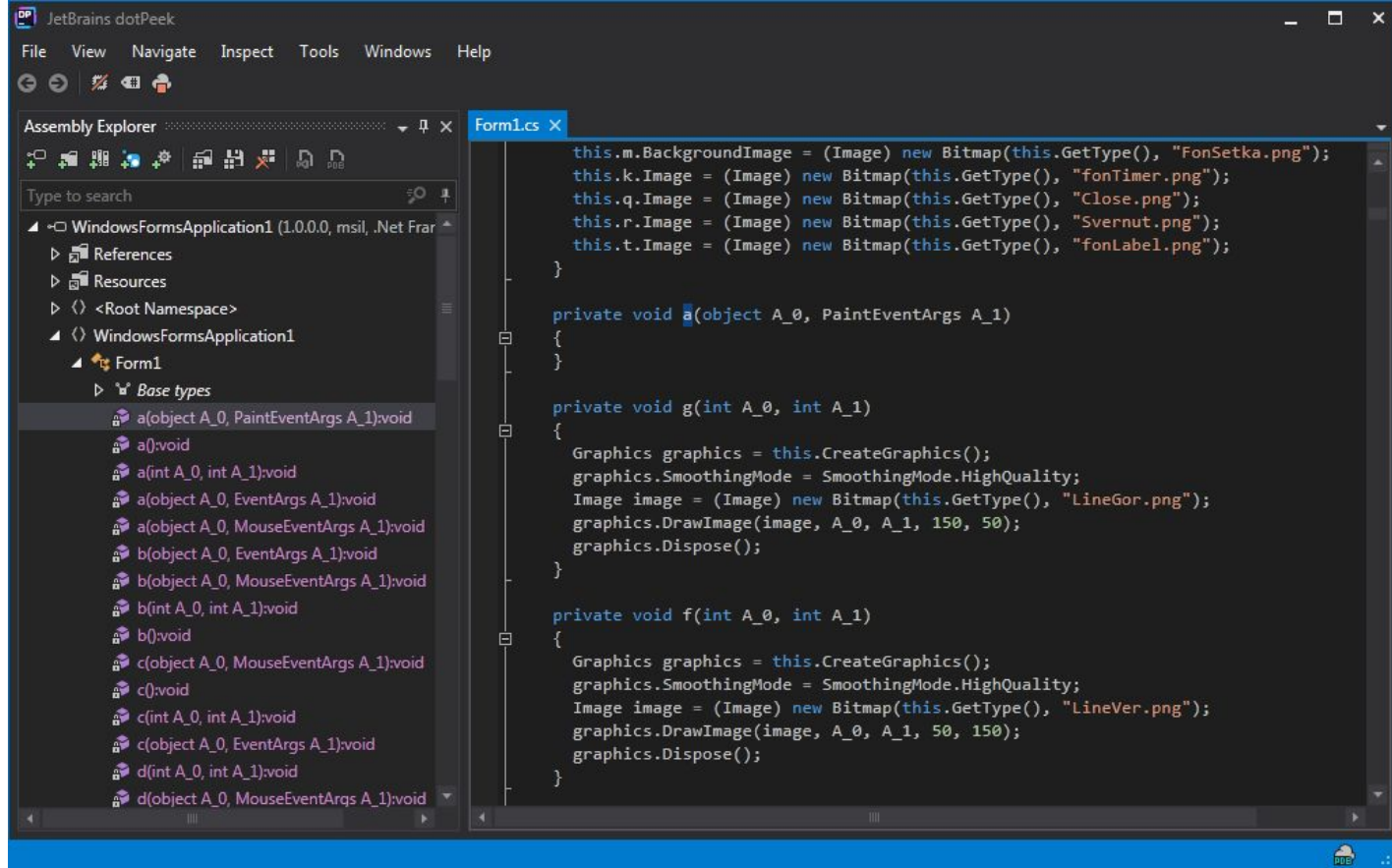
Загрузим исполняемый файл



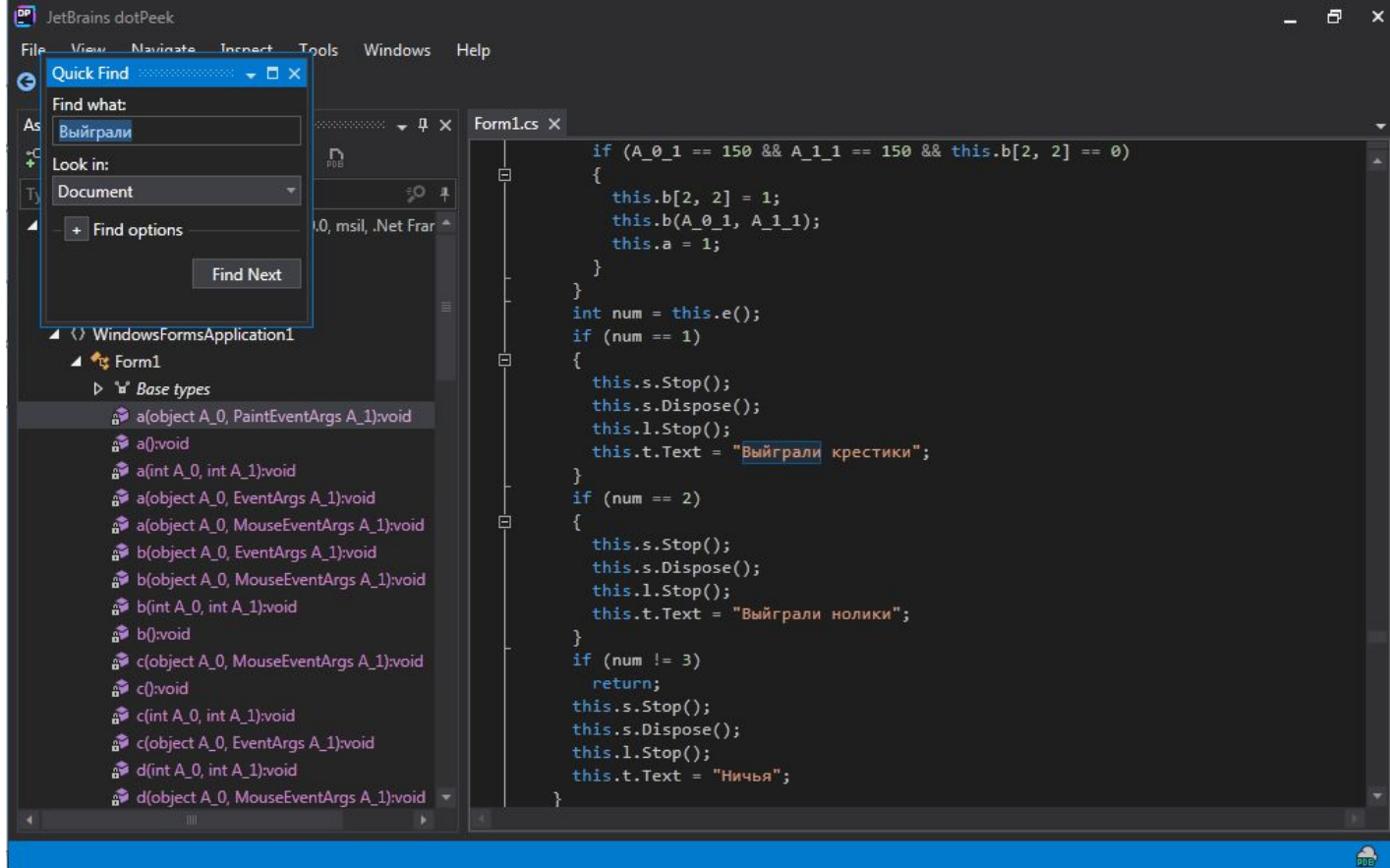
В списке появилось приложение



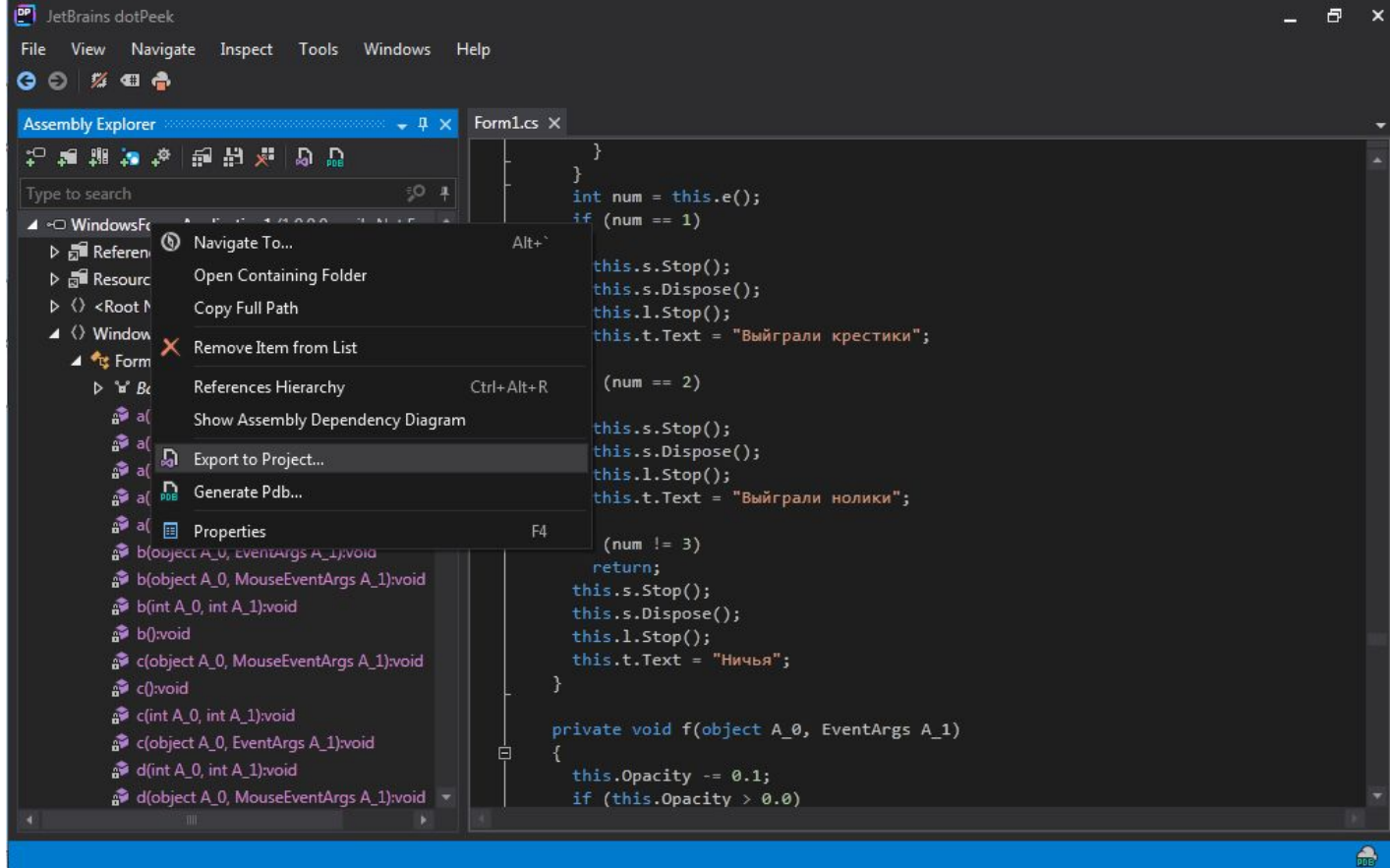
Внутри - декомпилированный код



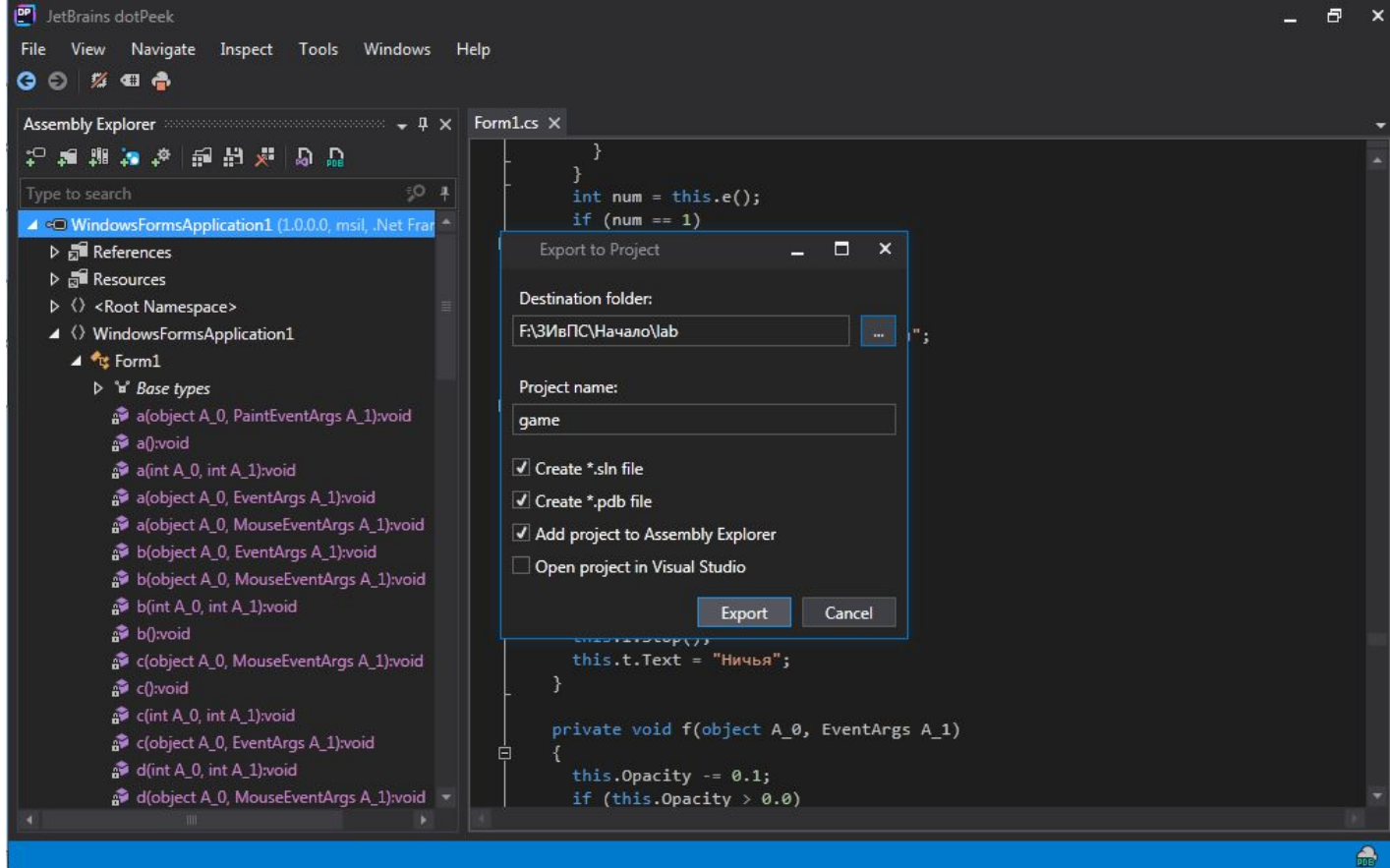
Клик на сущности - переход к коду



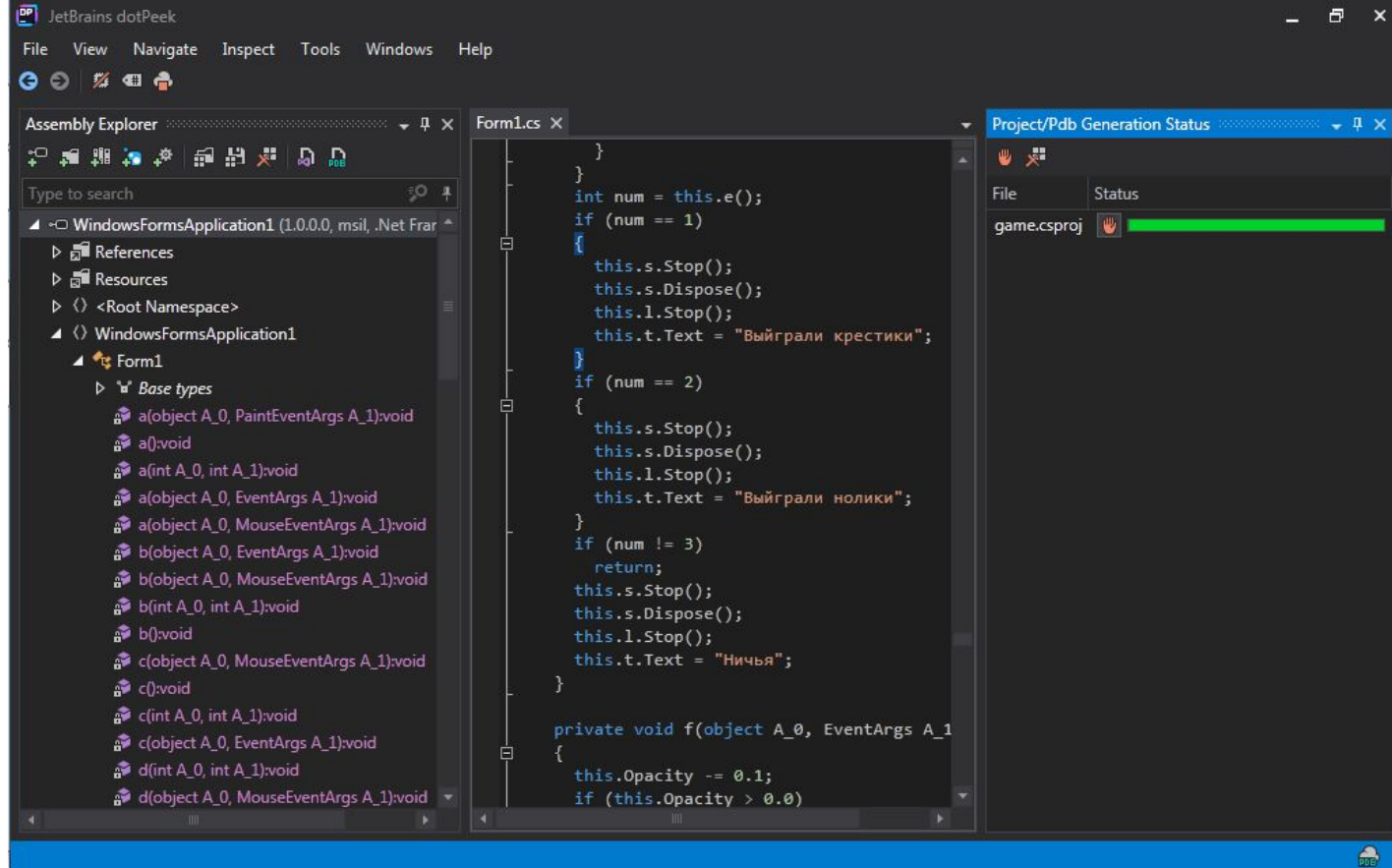
Нашли место результата игры



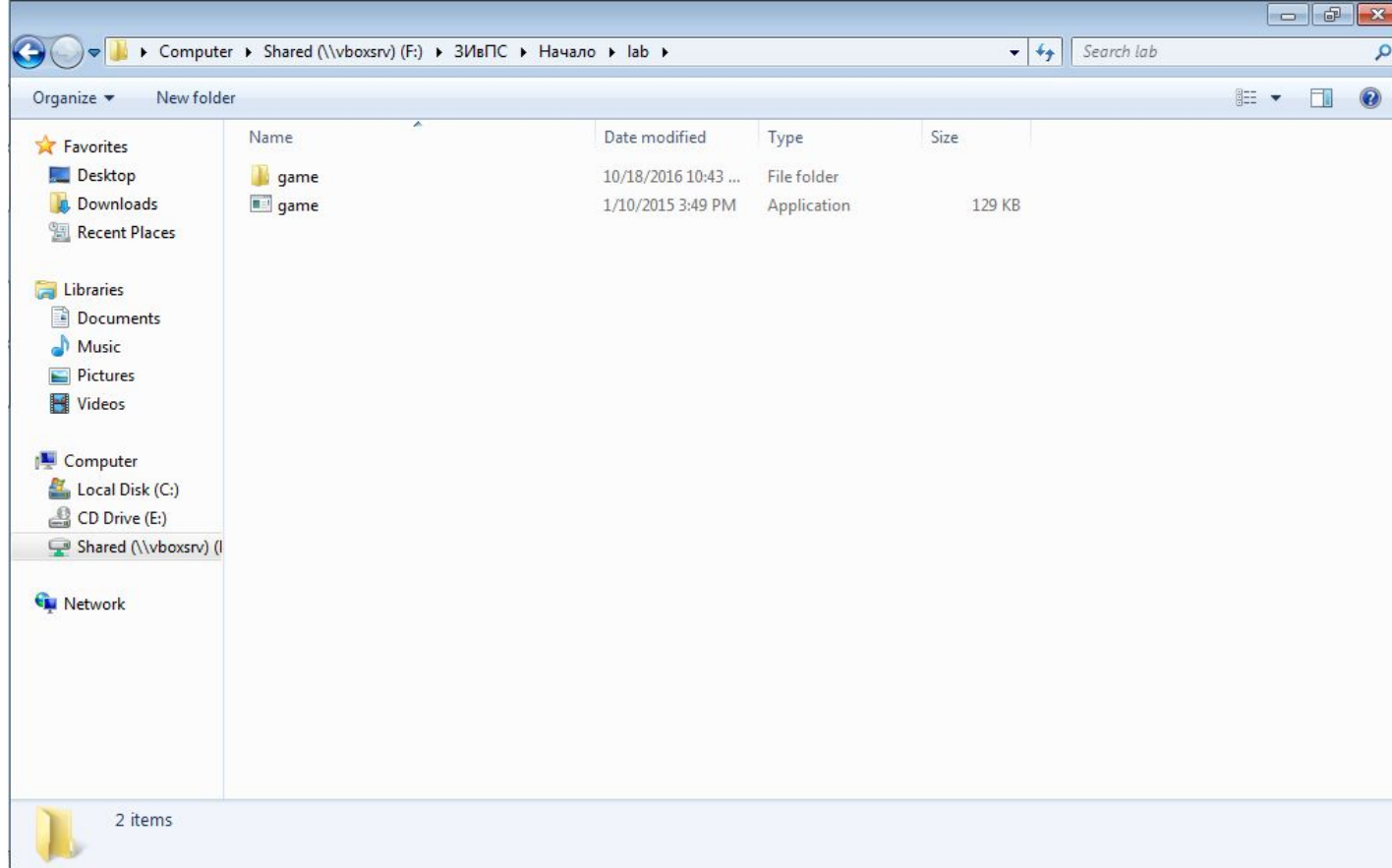
Экспорт в MS VS для модификации



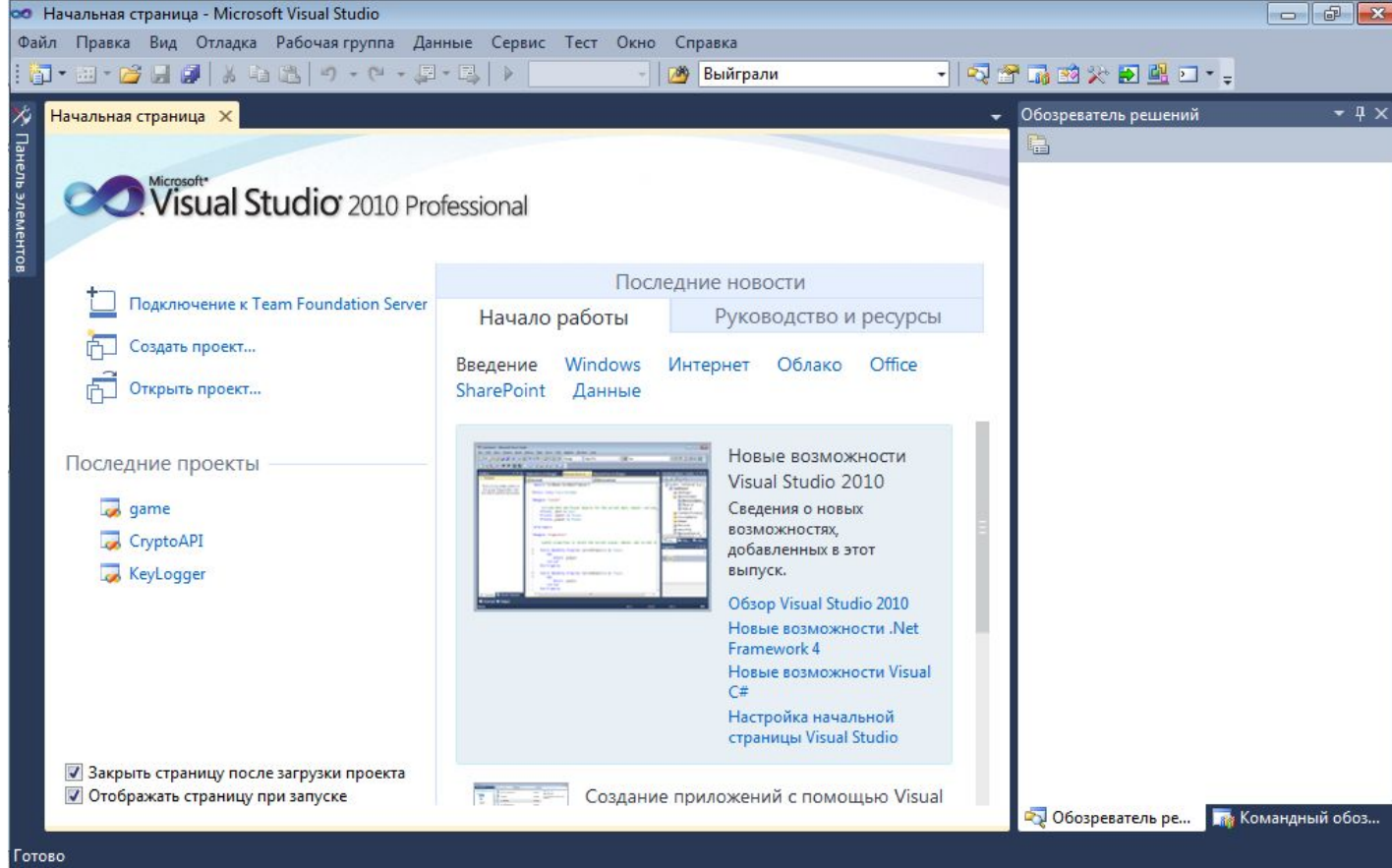
Настройка экспорта



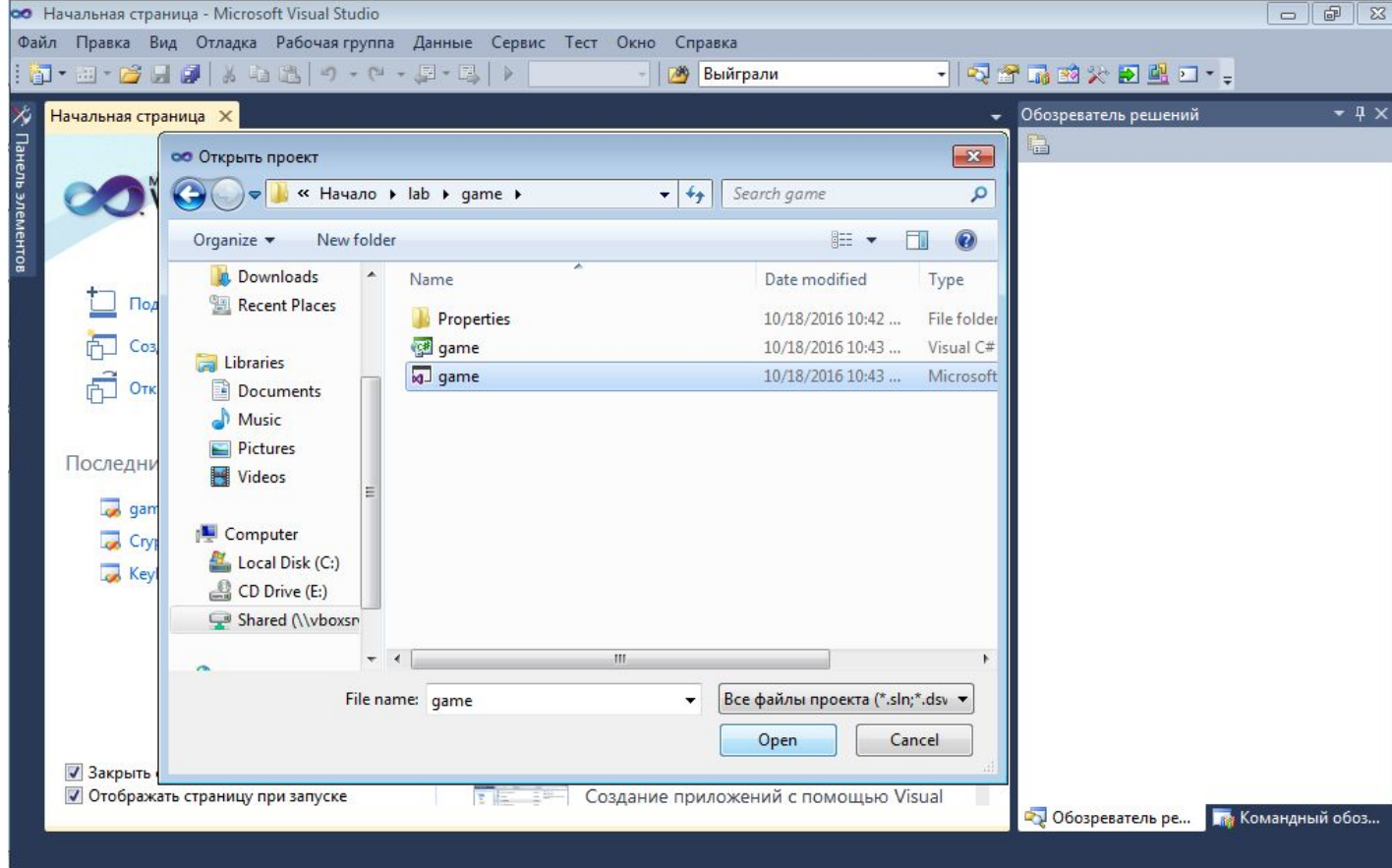
Дождемся завершения экспорта



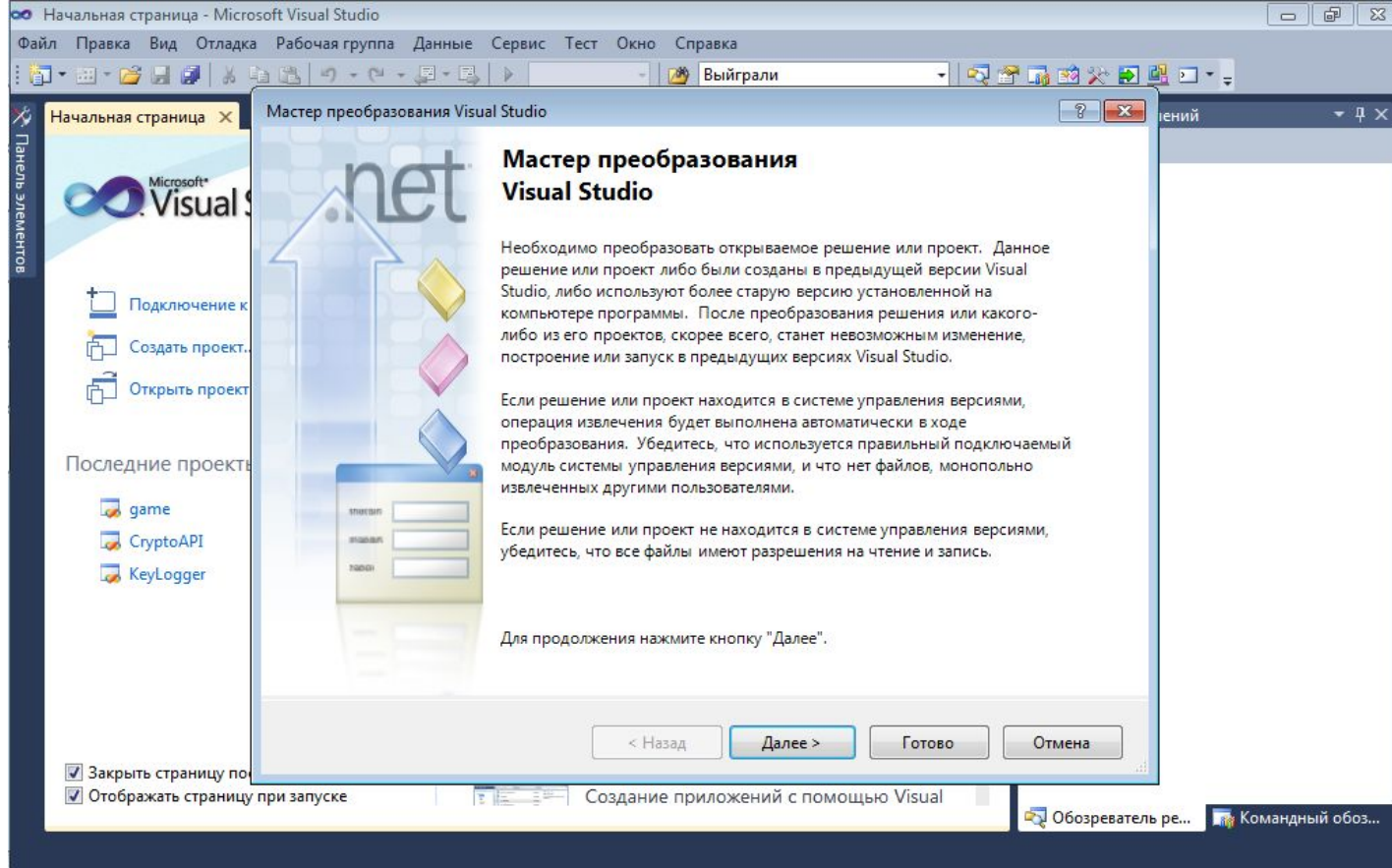
Появилась папка с проектом



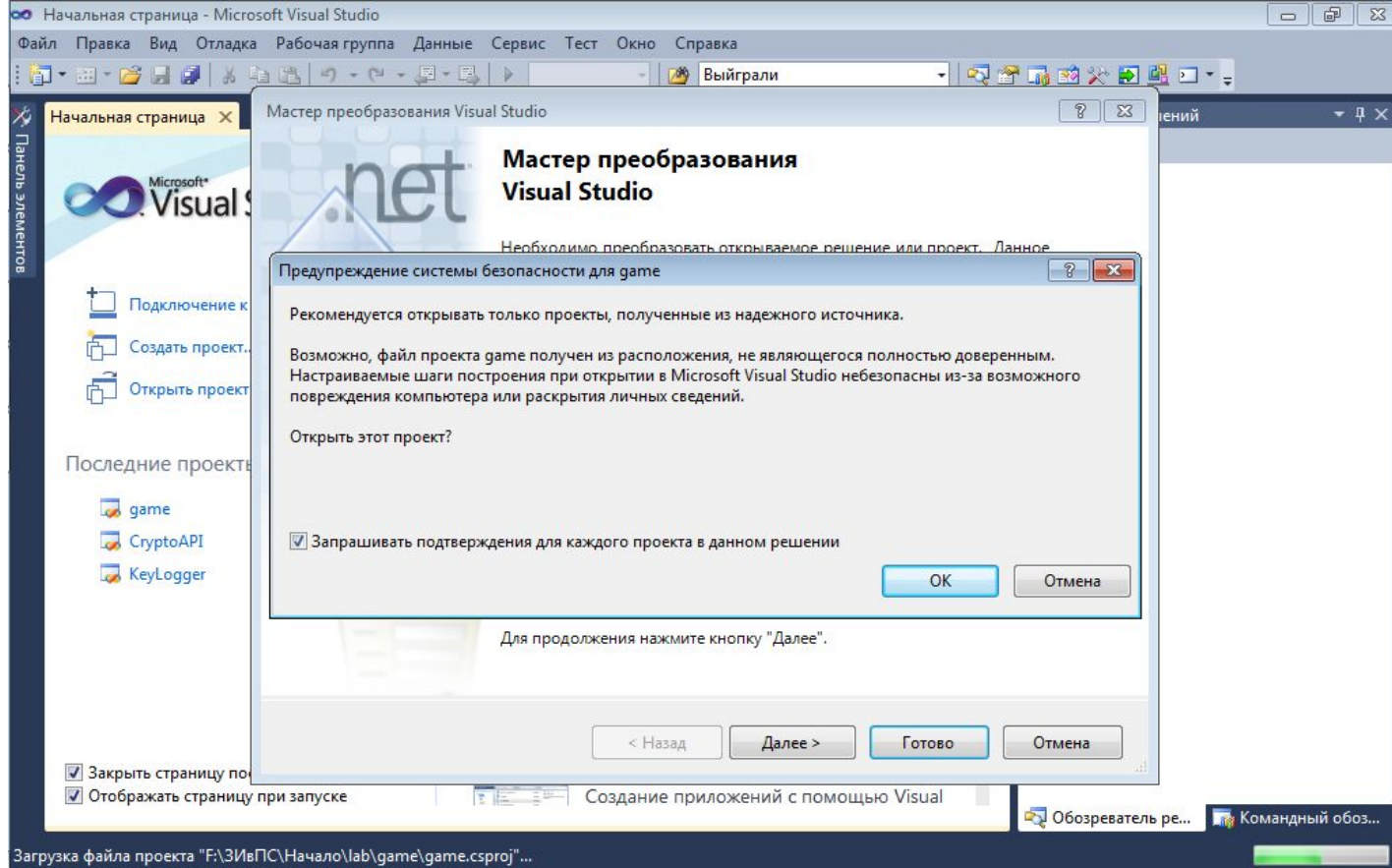
Переходим в Visual Studio



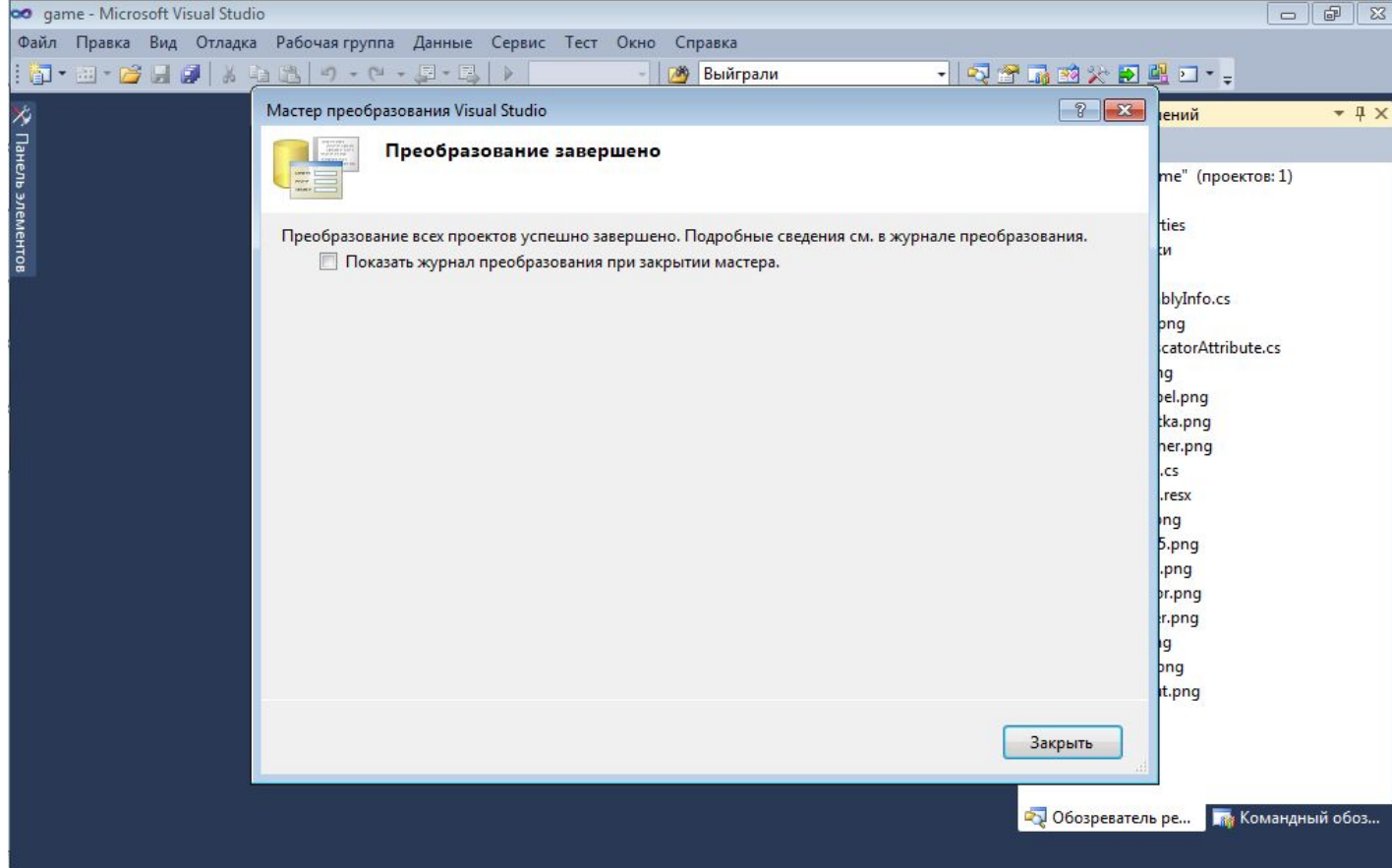
Открываем проект



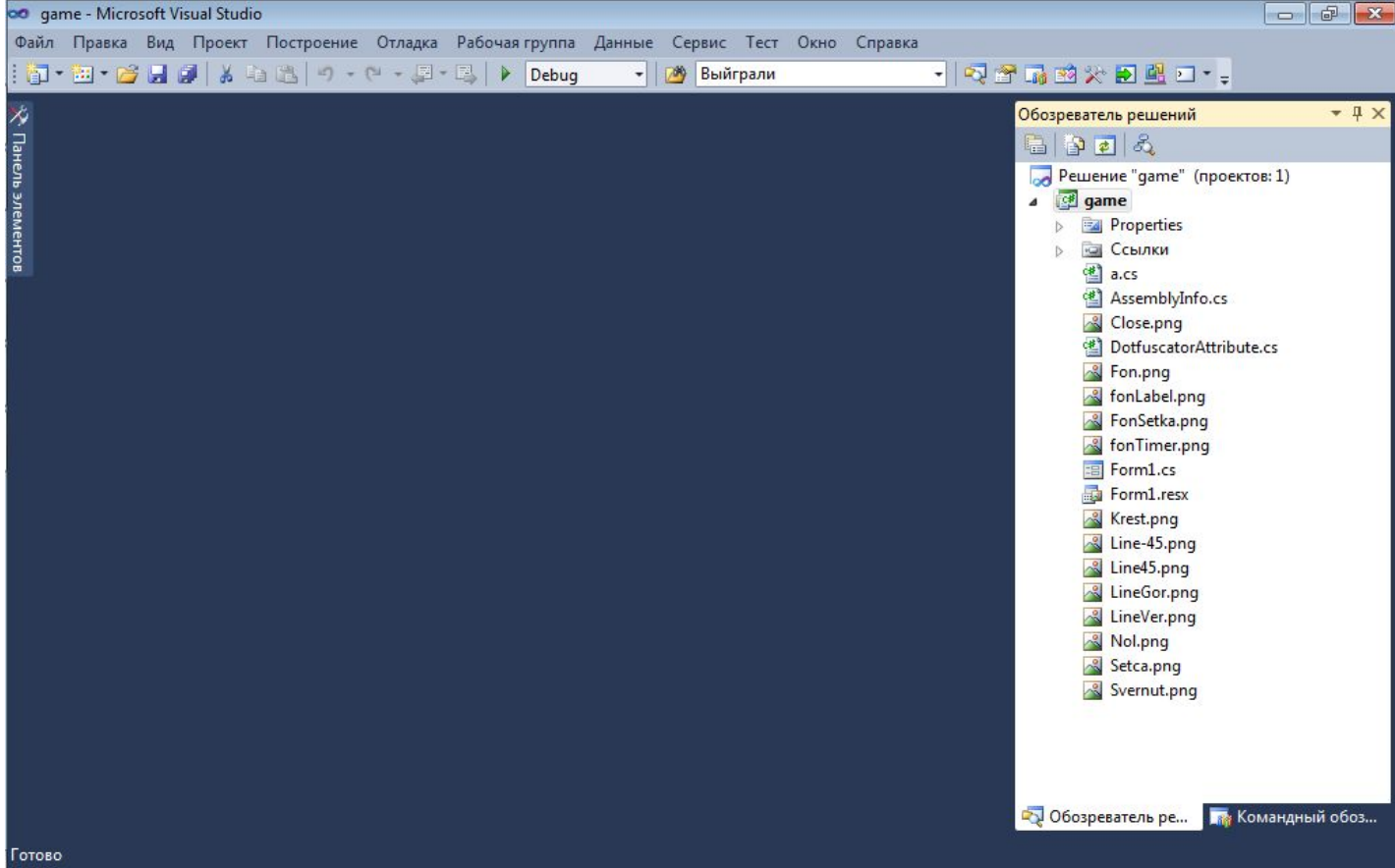
MS VS конвертирует в нужный формат



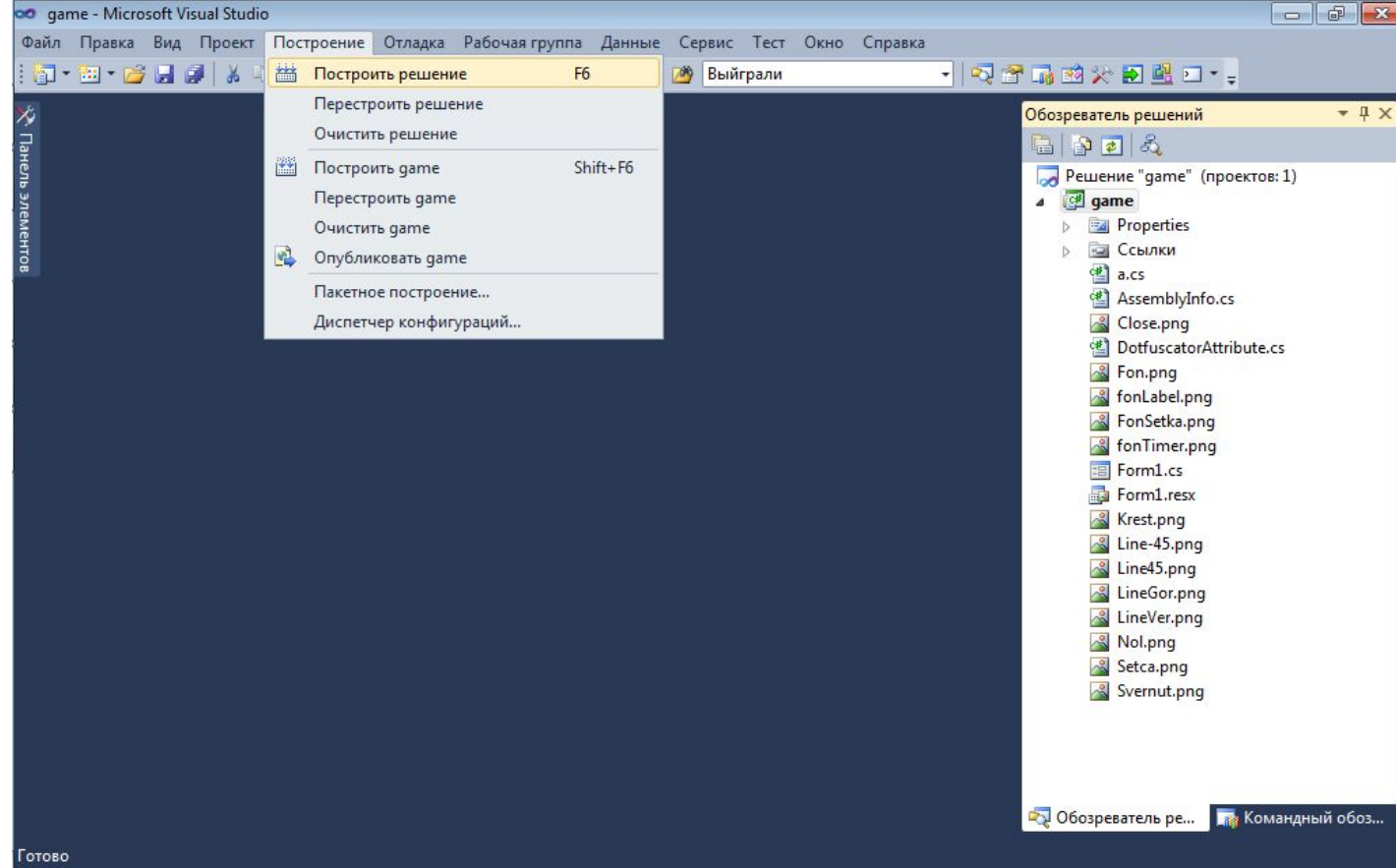
Предупреждение о безопасности



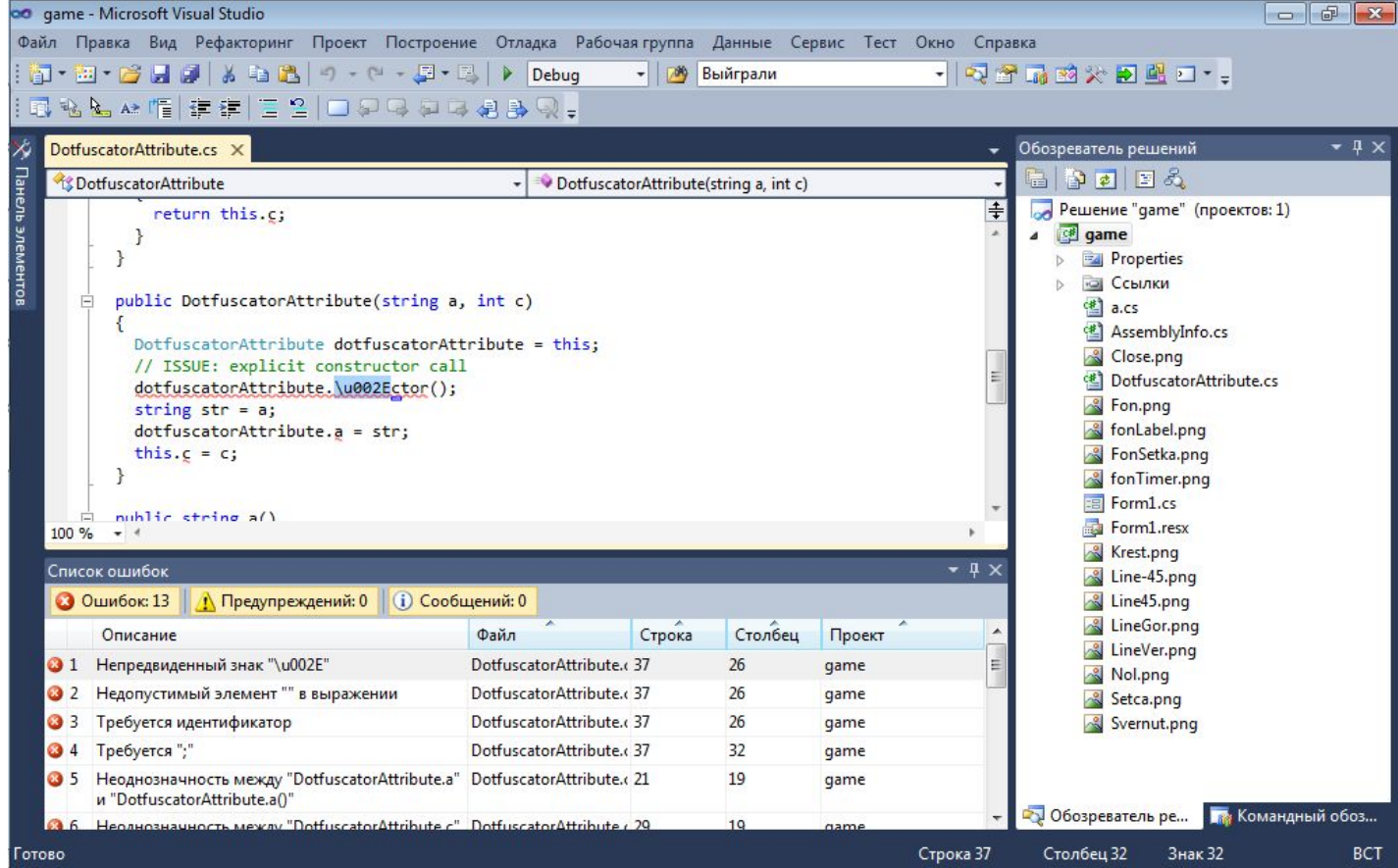
Преобразование успешно



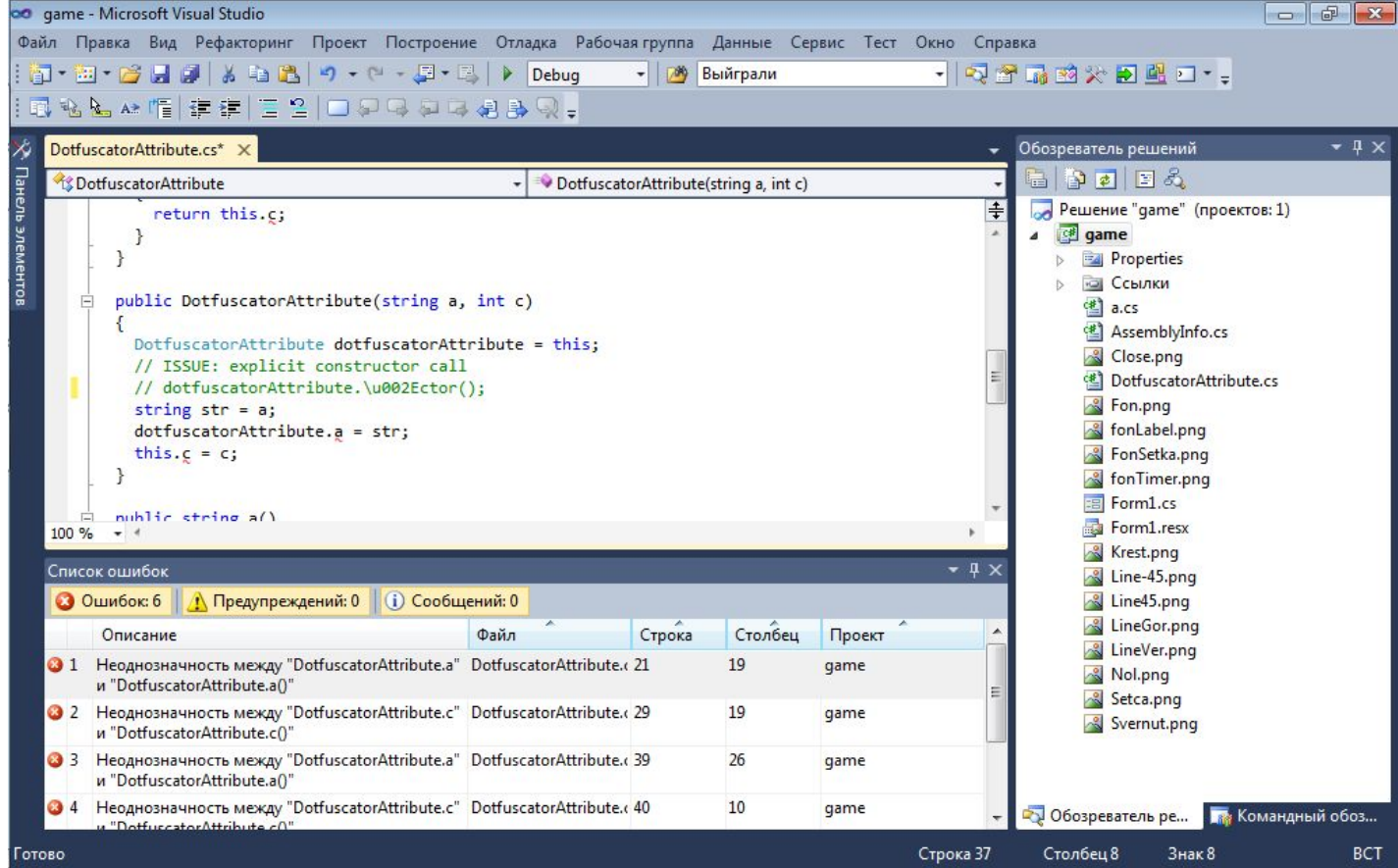
Проект в Visual Studio



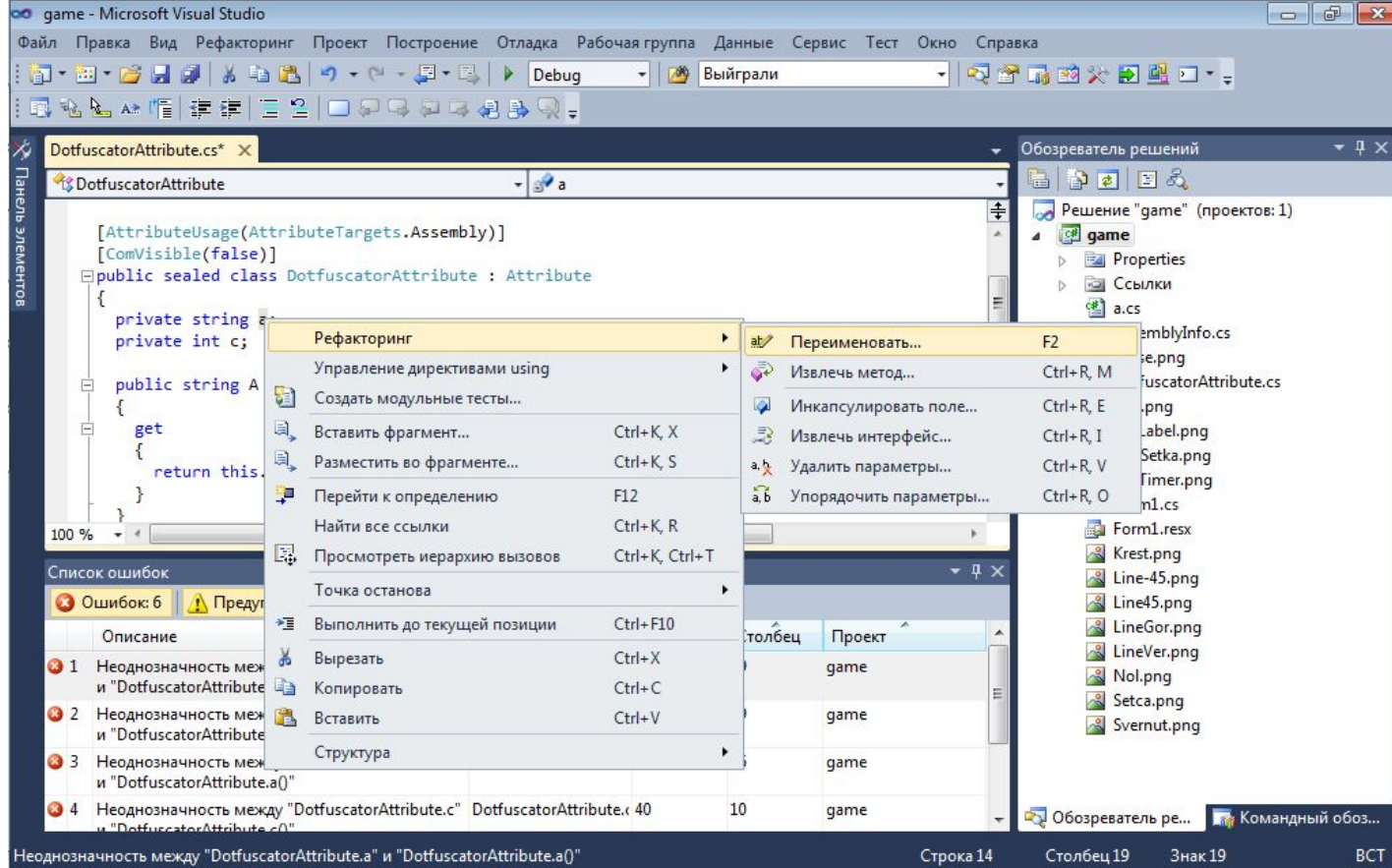
Пытаемся собрать



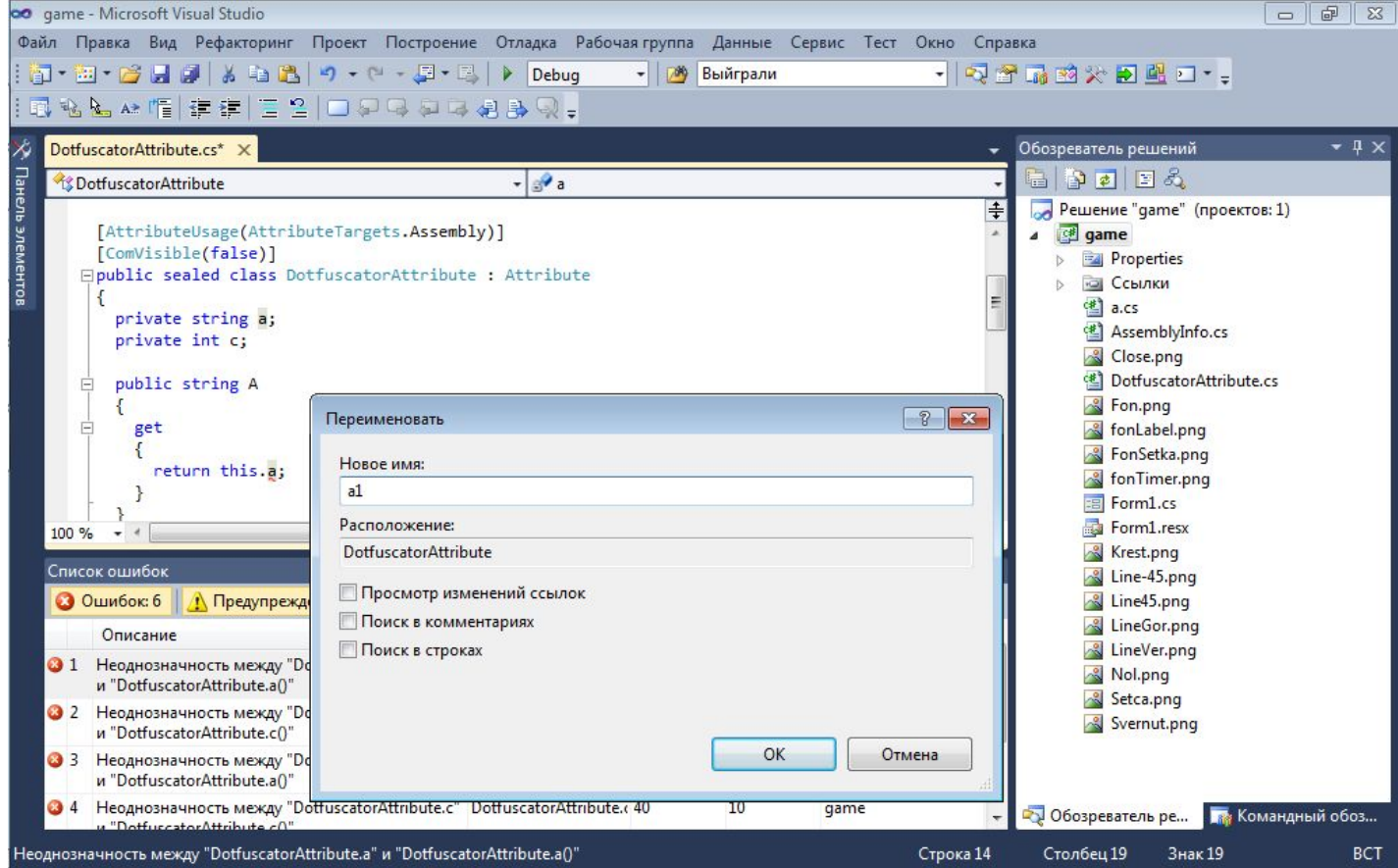
Есть ошибки - нужны правки



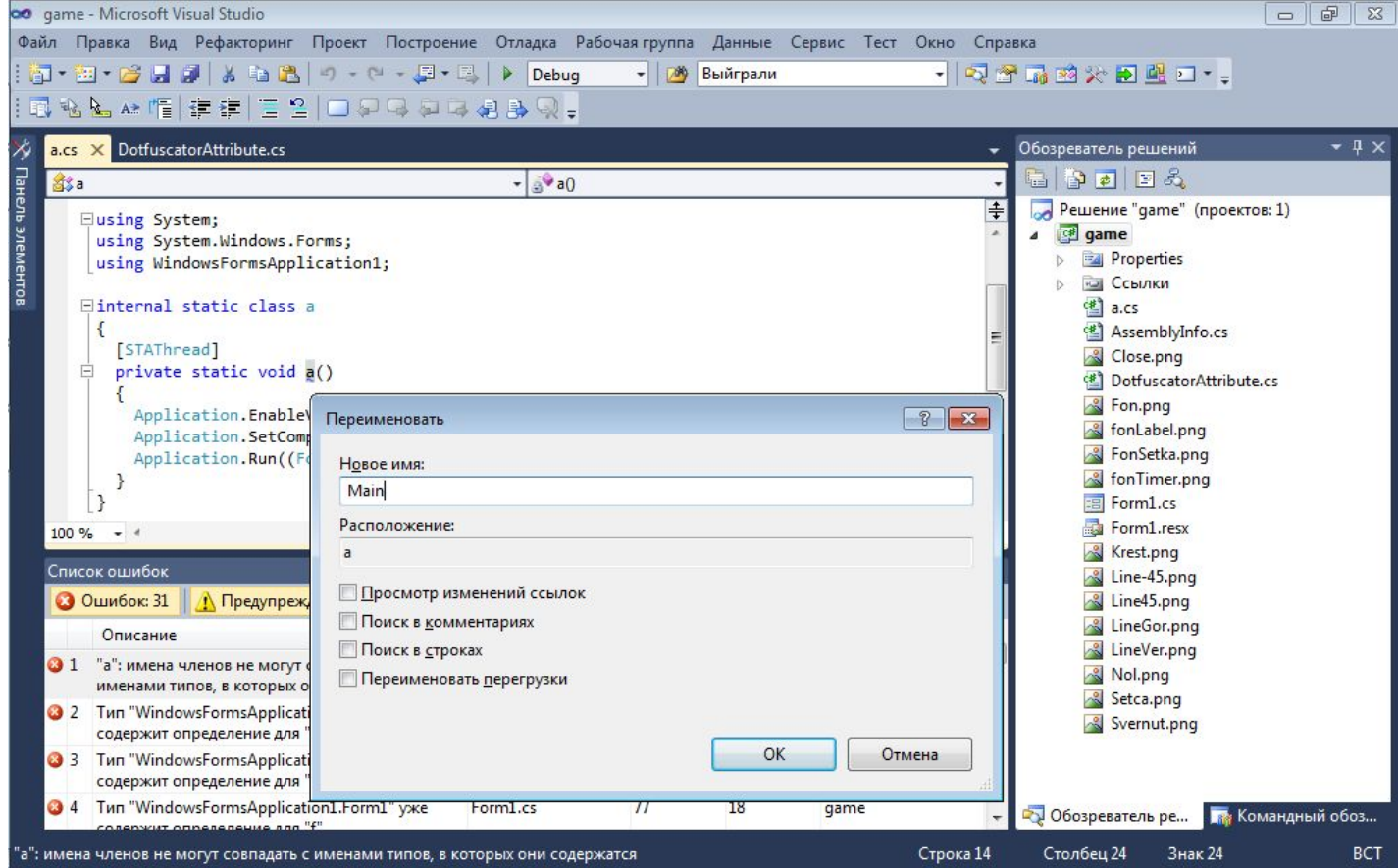
Комментируем



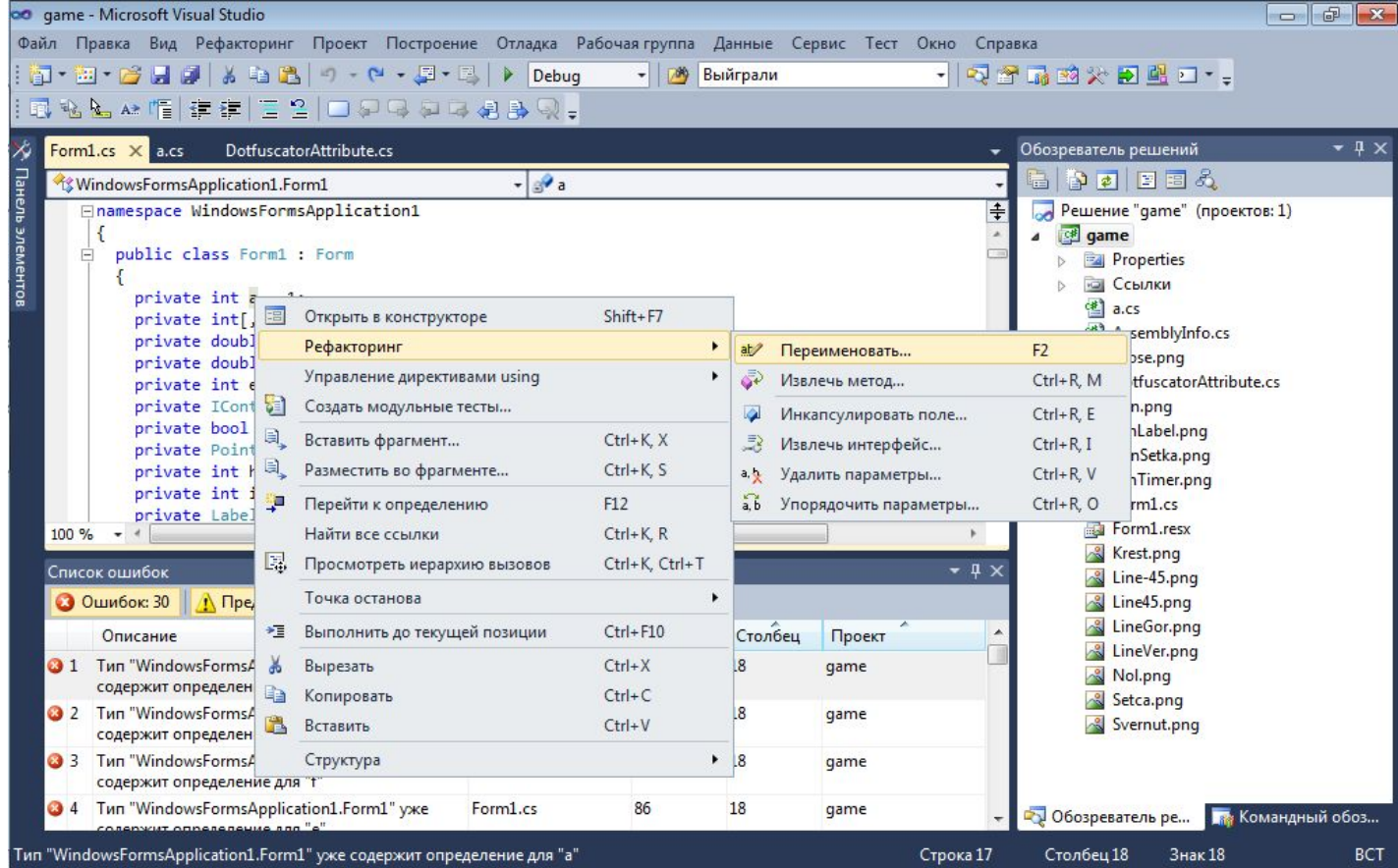
Необходимо устранить конфликты



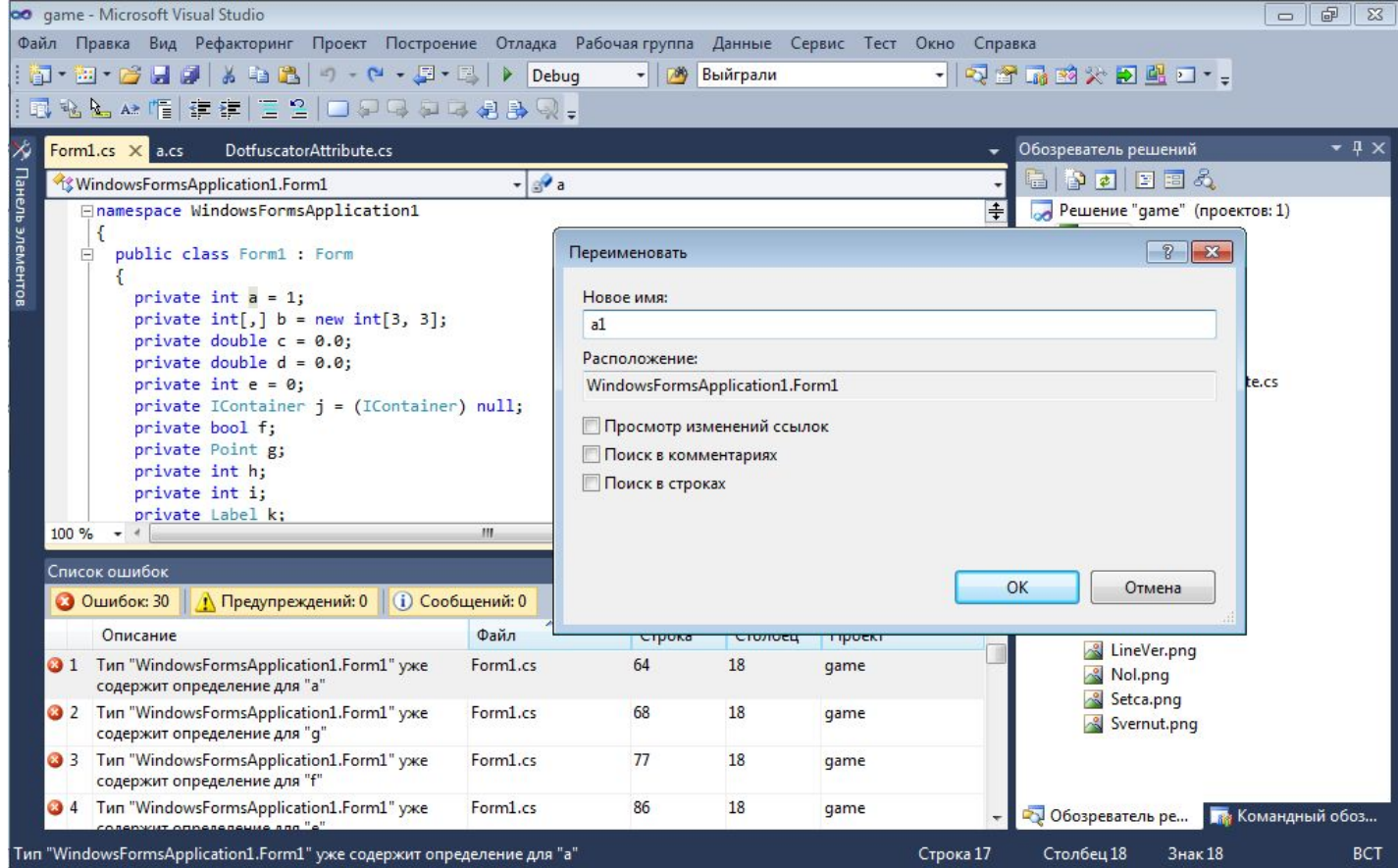
Даем другое имя



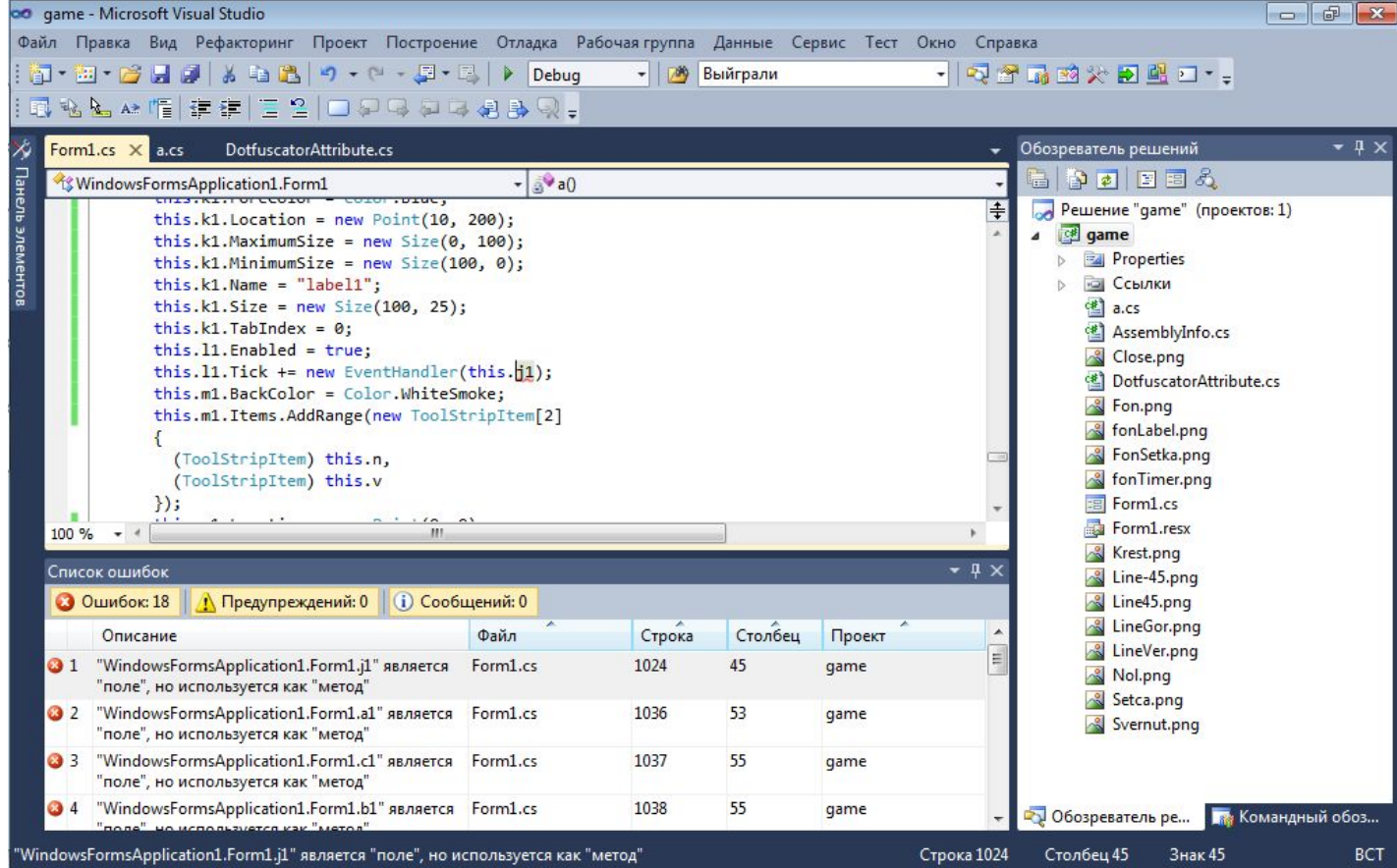
Находим Main - точку входа



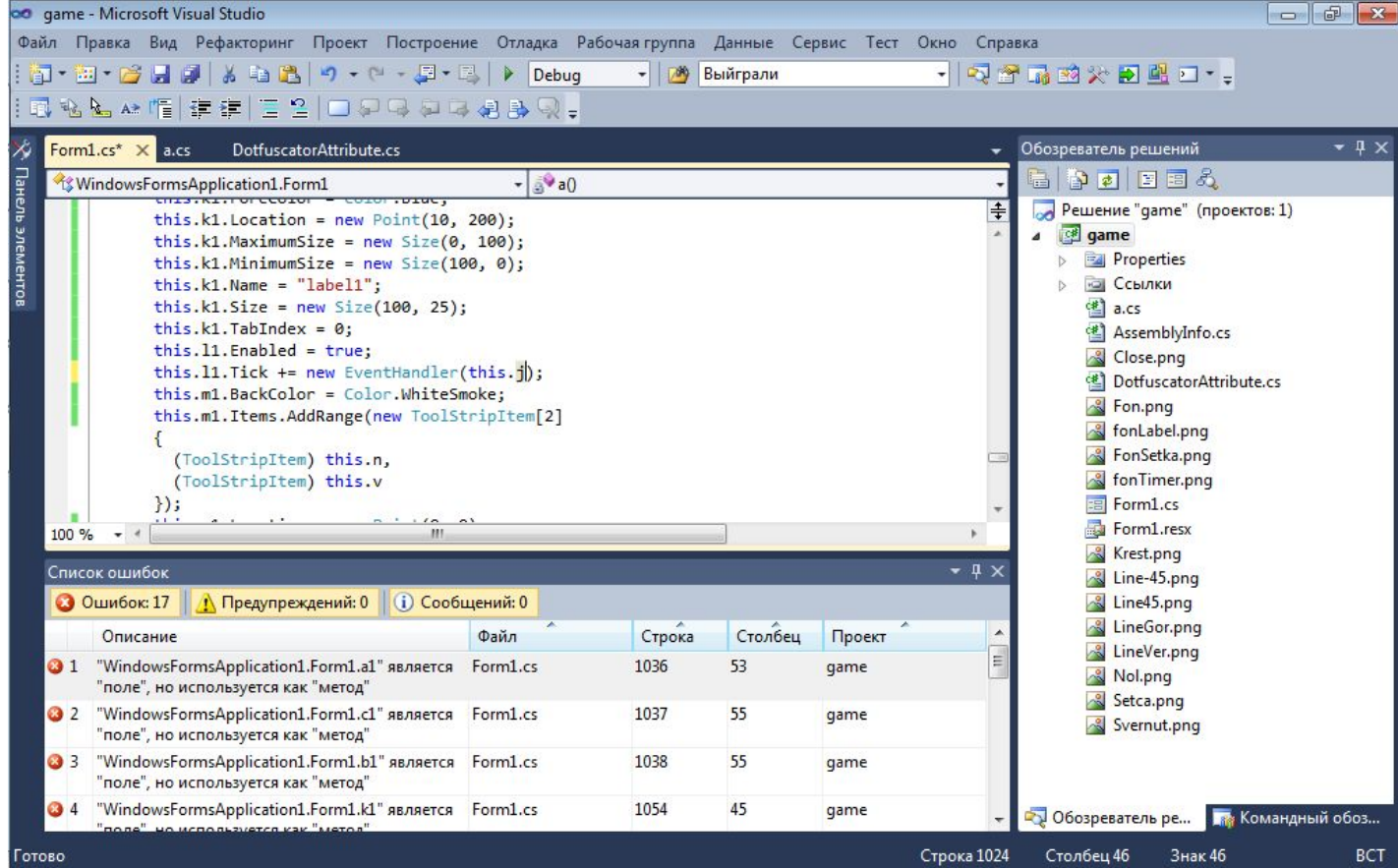
Меняем все конфликтные поля



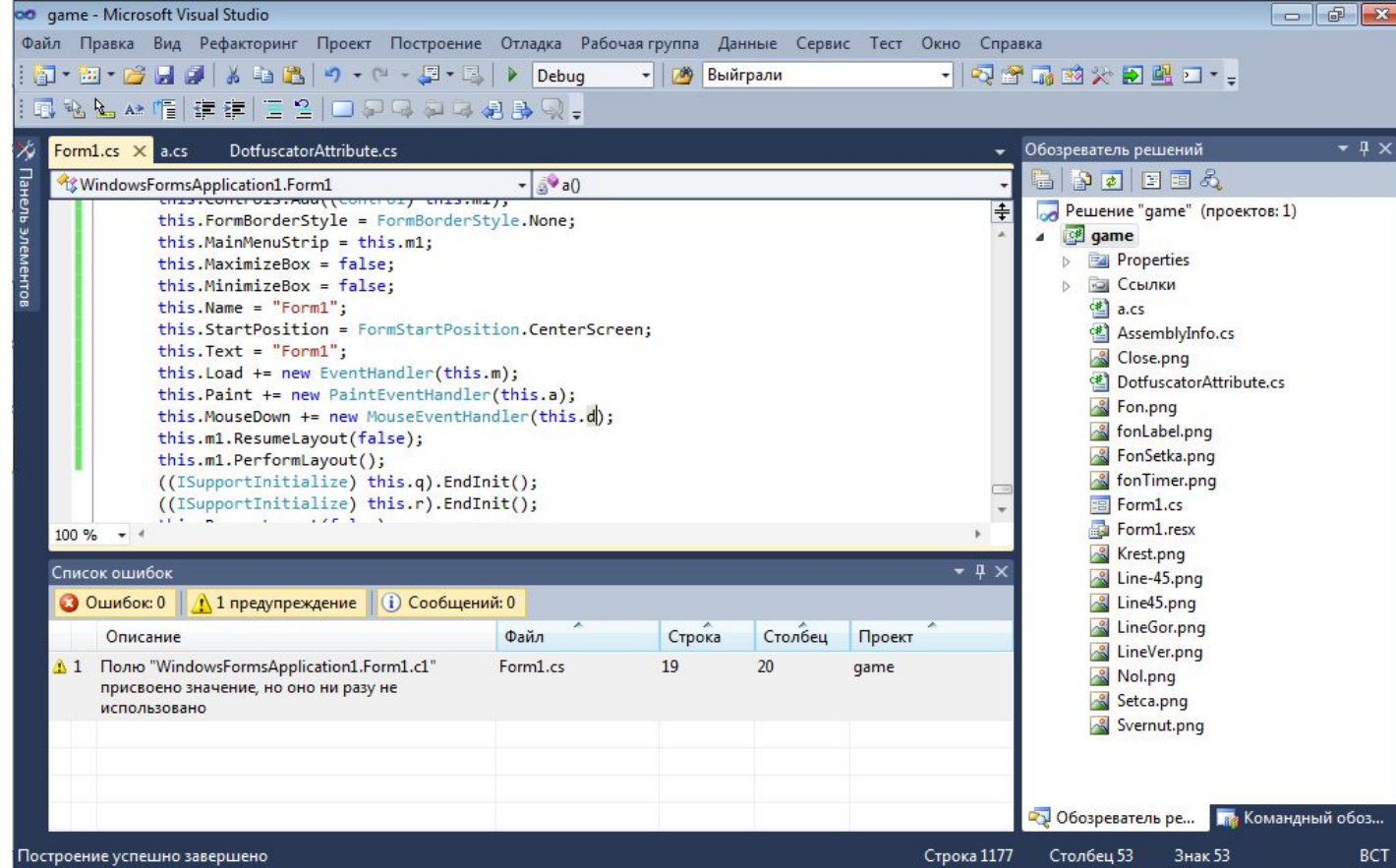
Имя значения не имеет



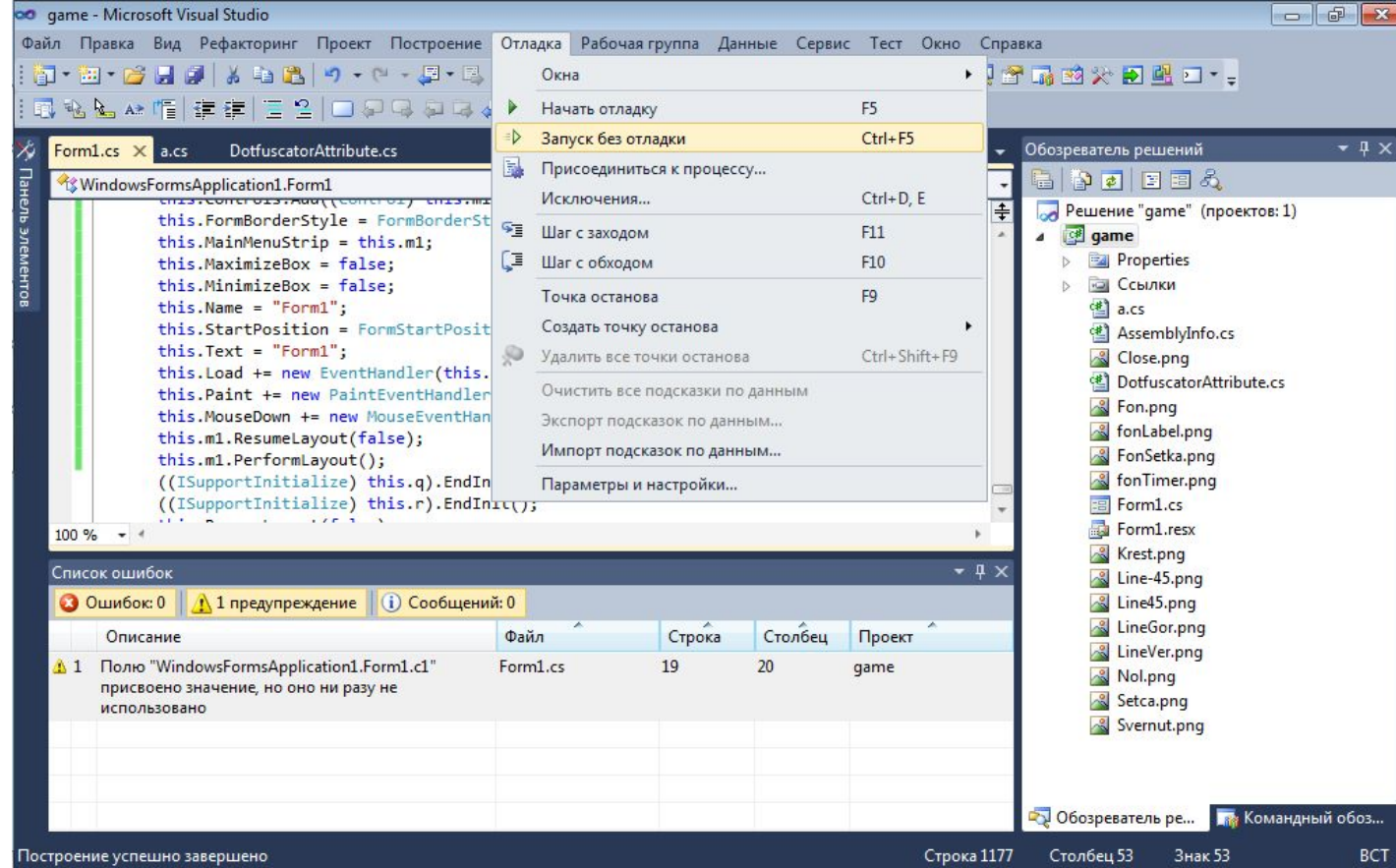
Не все переименования верны



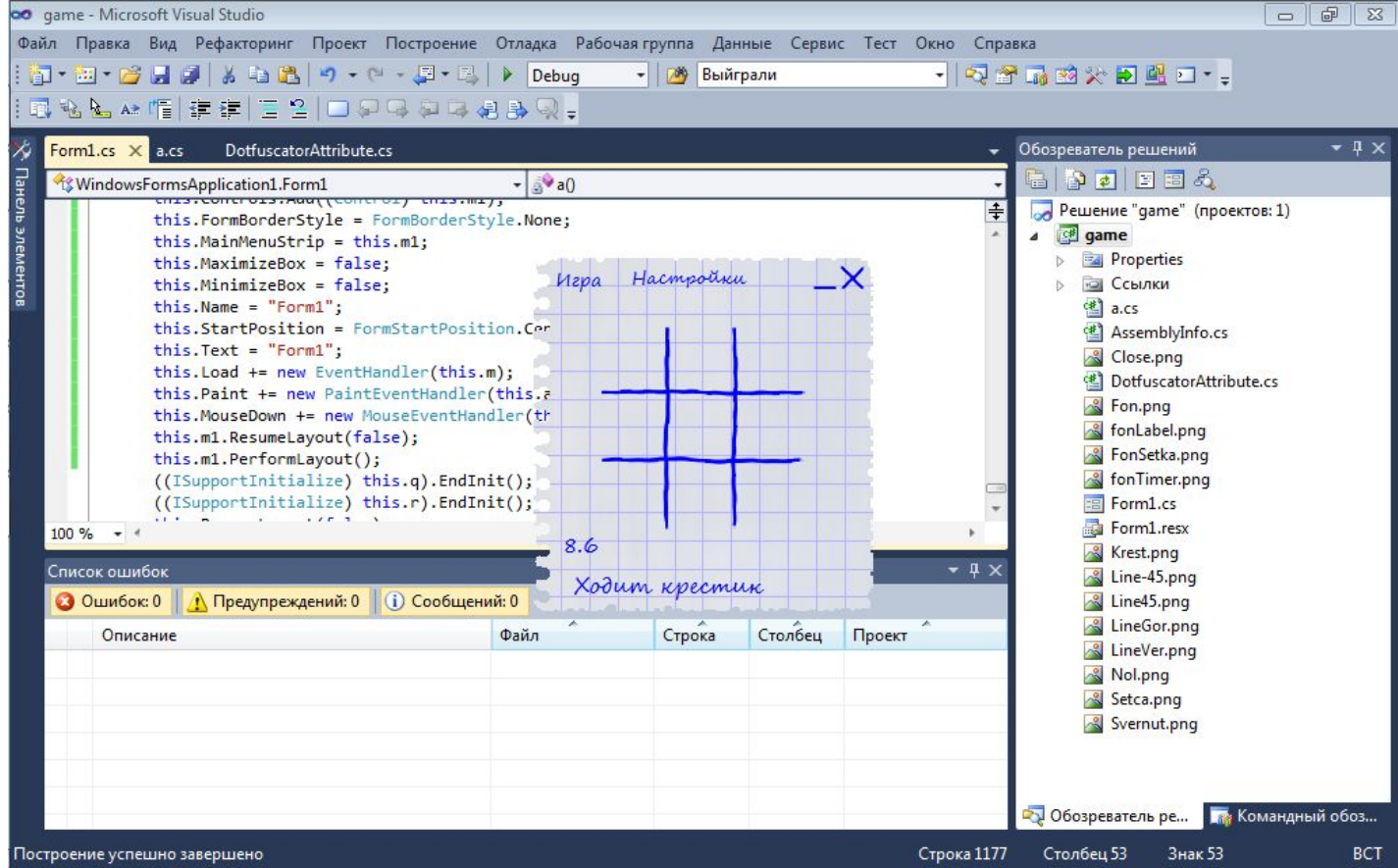
В таких случаях делаем откат



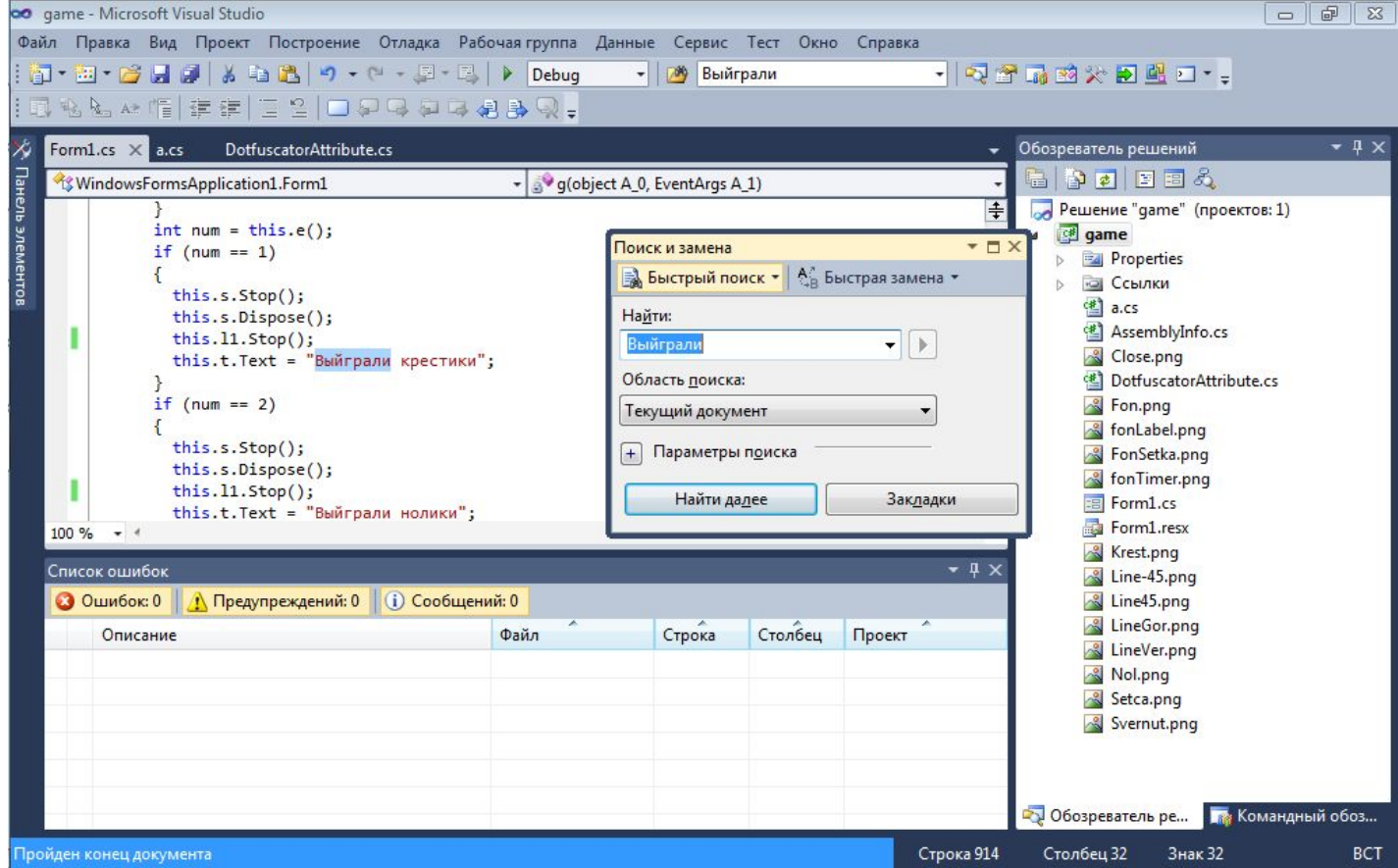
Добились успешной сборки



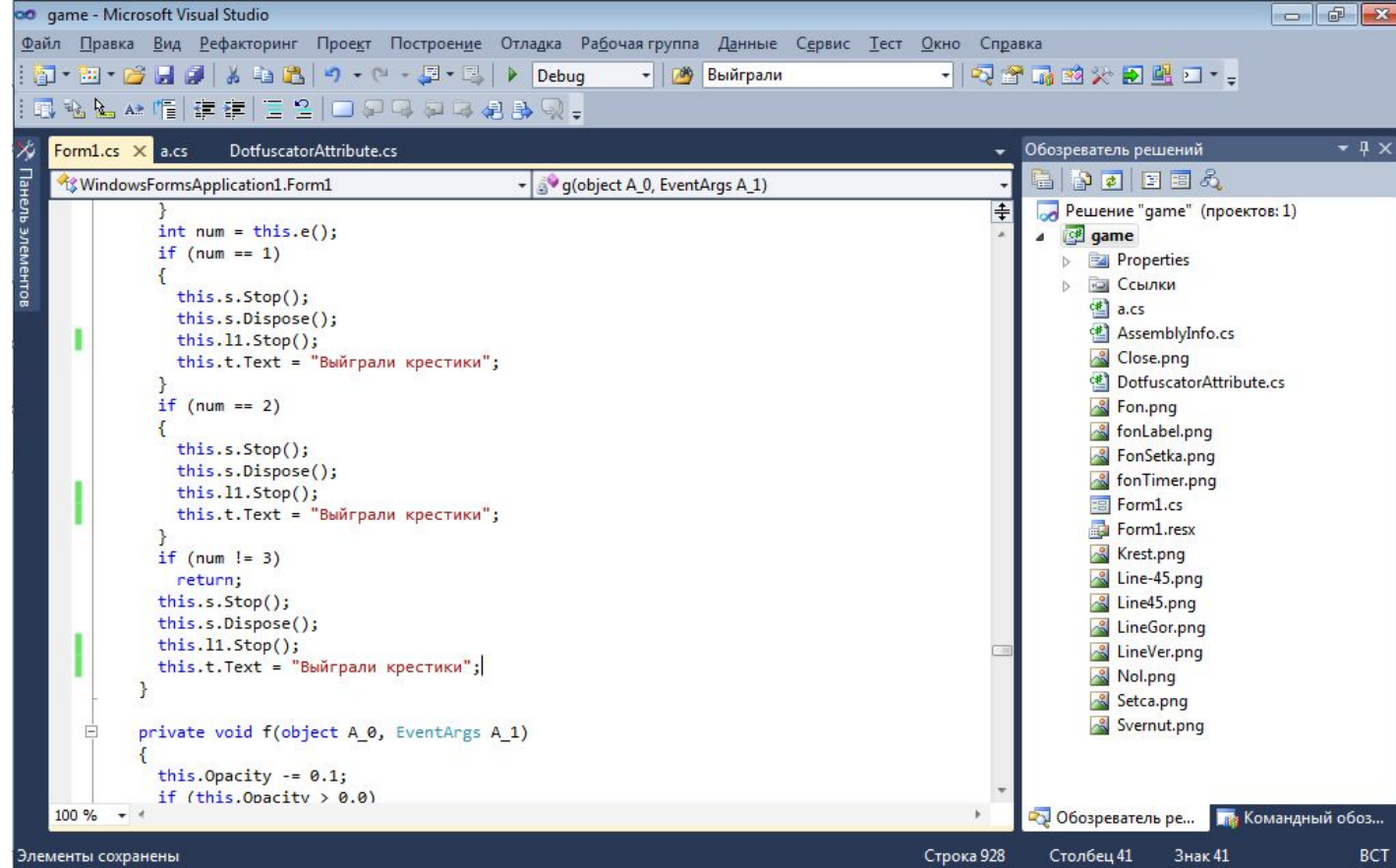
Проверим работоспособность



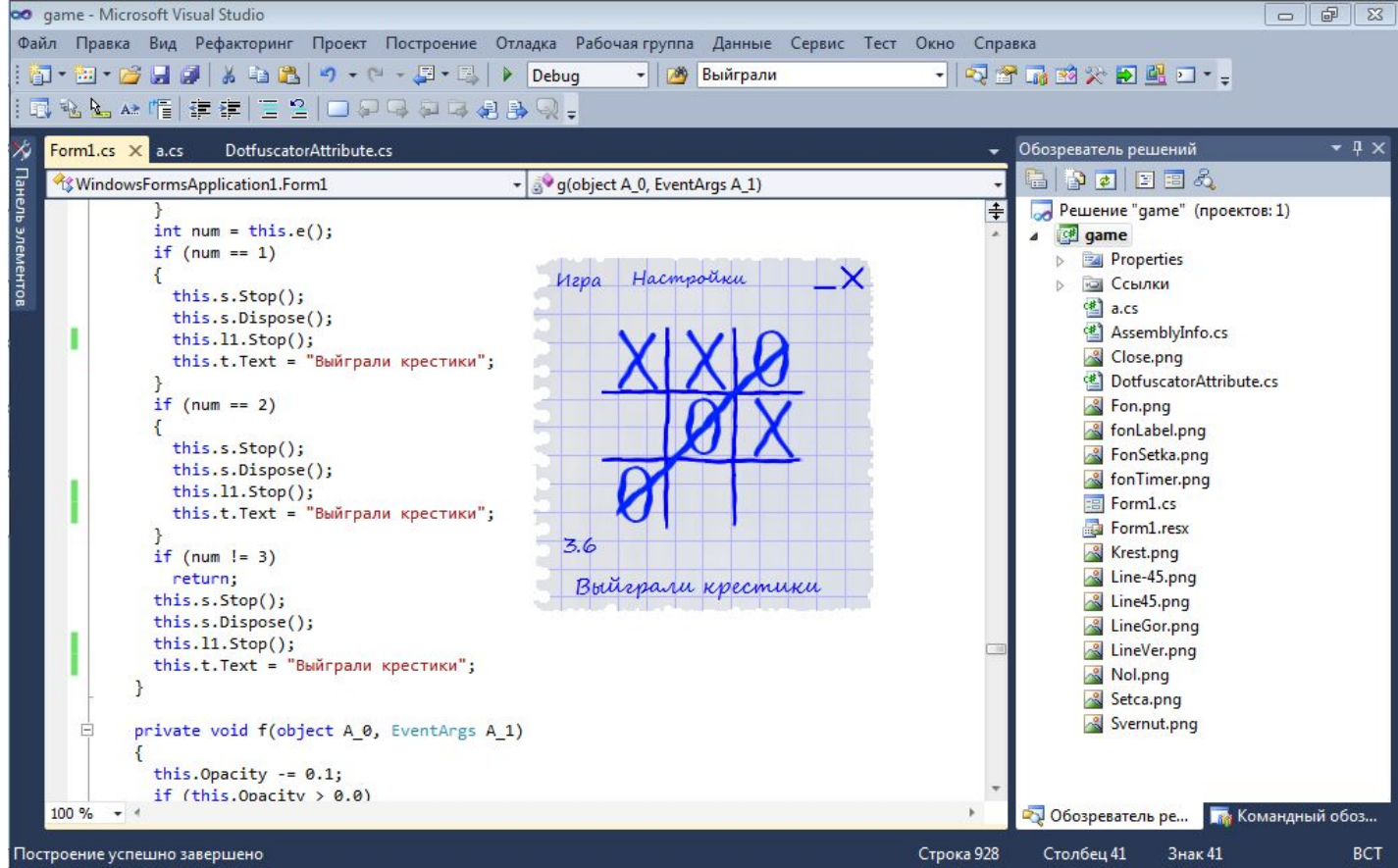
Работает



Ищем результат игры



Меняем результат на желаемый



Программа взломана

Спасибо за внимание

<mailto:vyacheslav.bezborodov@gmail.com>