

Рассматривая вопрос защиты кода, нашел интересное обсуждение, суть которого хочу изложить ниже.

На самом деле от дизассемблера можно защититься, но эта защита весьма относительна... Помнится, когда-то читал книжку по ассемблеру, там предлагался вариант перезаписи точки входа в приложение и моментальный выход. Таким образом при запуске программа запускалась и работала, а дизассемблер считал, что программа тут же закрывается при старте. По крайней мере для IDA в то время это работало. И подобных приемов было много...

Это больше похоже на "я убегаю, ты догоняешь". Дизассемблеры постоянно развиваются, и против них постоянно придумывают новые препятствия... Тут однозначно можно сказать только одно: если нет желания посвятить этой гонке все свое время - лучше не соваться в это дело и воспользоваться сторонними решениями.

Что касается конкретно C# - это в каком-то роде неполноценный язык. Получаемый exe-файл не содержит нативного кода, в нем записаны инструкции, которые должны быть переданы .NET-среде для исполнения. Так написанную на C# программу можно очень просто открыть и просмотреть весь исходный код (с оригинальными названиями функций и переменных).

Я пишу на C# и так же столкнулся с проблемой защиты приложений. Для моих задач подошел бы **.NET Reactor**. По сути это обфускатор (делает код нечитаемым для человека), так же он может заменять некоторые участки кода нативными инструкциями (функция песко-bit, если не ошибаюсь). Как правило подобной защиты хватает. Если есть очень важные участки кода, их переписать на C++ и сделать нативную DLL-ку, которую можно будет защитить получше, и затем использовать в своей программе. Но мне такие извращения еще не требовались.

В рамках текущих реалий слову "защитить" дают новое определение... Защитить программное - это создать условия, при которых взлом будет экономически не выгоден. Это достигается двумя способами:

1. Усиление защиты софта
2. Снижение стоимости лицензии

Кстати в состав Visual Studio входит бесплатная версия Dotfuscator, называется Dotfuscator Community Edition распространяется как часть Visual Studio от Microsoft. Правда, указанная версия обфускатора делает чуть менее, чем ничего.

Из бесплатных решений, стоит обратить внимание только на Obfuscator, The Open Source Obfuscation Tool for .NET Assemblies, информация о котором доступна по ссылке: <https://obfuscator.codeplex.com/>

И в завершении.

Идеальной защиты нет, стремиться надо лишь к тому, чтобы стоимость взлома была выше стоимости лицензии.