УДК 004

Создание с помощью Microsoft Visual Studio приложения вызывающего BSOD

Маринчук Александр Сергеевич
Приамурский государственный университет им. Шолом-Алейхема
Студент

Аннотация
В данной статье рассмотрен инструмент Microsoft Visual Studio для создания консольного приложения, вызывающего синий экран смерти. Рассмотрен принцип вызова, а также последствия после имитирования BSOD.
Ключевые слова: C++, MVS, консольное приложение.

Creating an application that calls BSOD using Microsoft Visual Studio

Marinchuk Alexander Sergeevich
Sholom-Aleichem Priamursky State University
Student

Abstract
This article describes the Microsoft Visual Studio tool for creating a console application that causes a blue screen of death. The principle of the call, as well as the consequences after simulating the BSOD, are considered.
Keywords: C++, MVS, console application.

1. Введение

1.1 Актуальность исследования

Стремительное развитие информационных технологий и их проникновение во все сферы человеческой деятельности привело к развитию информационной или киберпреступности, направленной против информационной безопасности. Ежегодно миллионы людей и компаний теряют ценную информацию и данные в результате вирусных атак, действия троянов и других вредоносных программ. Часто информация бывает утеряна безвозвратно. Информация в современном обществе является ценным достоянием и подлежит защите, но в то же время информация должна быть доступной для определенного круга пользователей. На сегодняшний день угрозы безопасности для компьютера могут принять любую форму и масштаб.

1.2 Обзор исследований

В статье В. А. Староверова статье рассматривается работа компьютерных вирусов, какой ущерб могут вызвать вирусные программы для нормального функционирования ПК. Какие основные методы защиты

существуют от вредоносных программ и как работают антивирусные программы [1]. Разработан метод распространения вирусов в компьютерных сетях на основе цепи Маркова. Рассмотрены модели на основе цепи Маркова для всей сети и для отдельных узлов. Построена компьютерная сеть в виде графа в статье А. А. Емельянова [2]. Рассмотрела основные виды компьютерных вирусов и методы их действия в своей статье Т. С. Санникова [3]. В статье Н. А. Бородиной и других рассматривается применение персональных компьютеров, в которых пользователь имеет свободный доступ ко всем ресурсам машины, защита компьютера от вирусов, основные пути проникновения вирусов в компьютерную сеть, заражение жесткого диска вирусами [4]. Е. А. Семененко рассмотрела способы распространения компьютерных вирусов и внесла некоторые предложения по защите своего компьютера. [5].

1.3 Цель исследования

Целью данной статьи является создание консольного приложения вызывающего BSOD с помощью Microsoft Visual Studio.

2. Методы исследования

Инструментом для достижения цели станет Microsoft Visual Studio. Microsoft Visual Studio — линейка продуктов компании Microsoft, включающих интегрированную среду разработки программного обеспечения и ряд других инструментальных средств [6].

Для начала работы следует скачать и установить Microsoft Visual Studio с официального сайта (рис. 1).

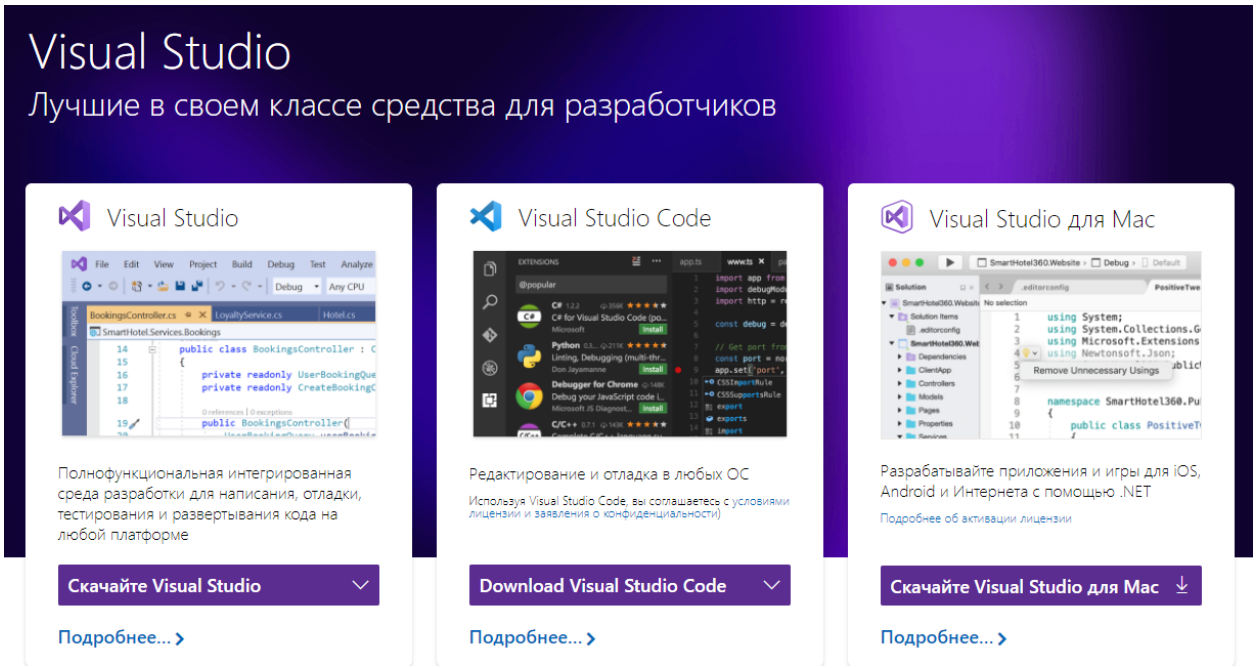

Рисунок 1 – Скачивание приложения

После установки программы следует создать новый проект консольного приложения C++ (рис. 2).

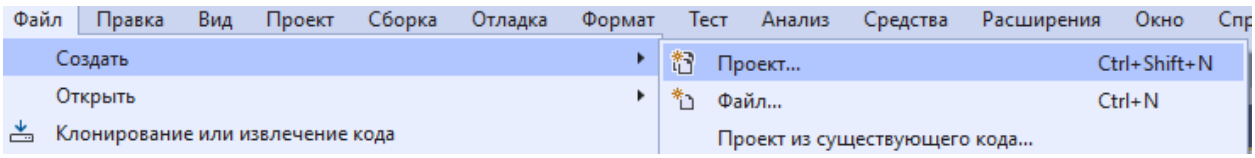

Рисунок 2 – Создание проекта

Далее пишем необходимый код для работы приложения (рис. 3).

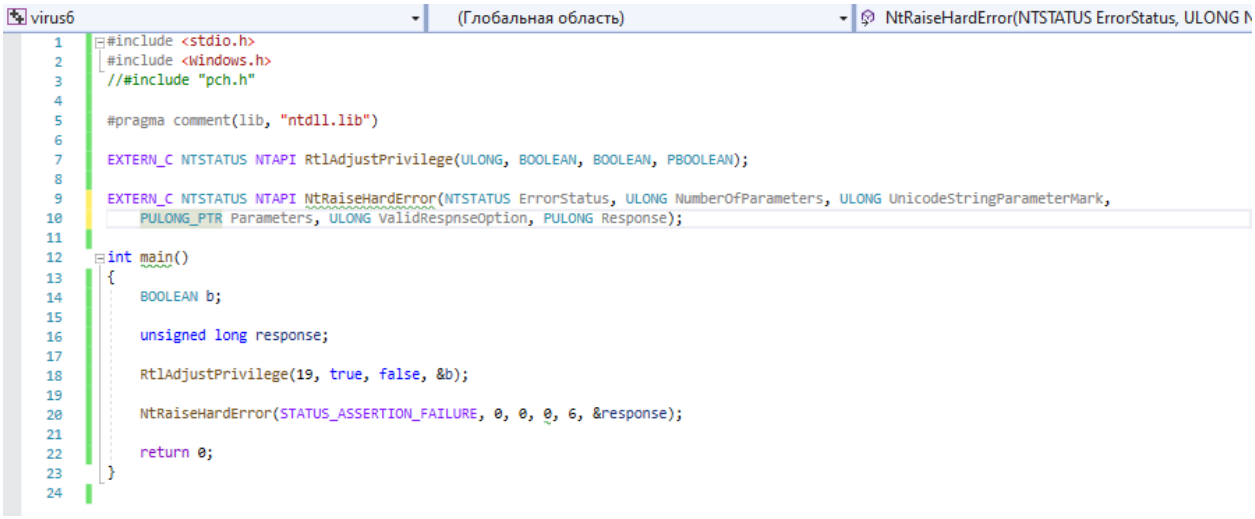

Рисунок 3 – Код приложения

Первая функция RtlAdjustPrivilege дает или забирает доступ к определенным правам, без которых некоторые функции не получится вызвать. Первый аргумент: 19 - номер привилегии, с которым будем работать, в данном случае это SE_SHUTDOWN_PRIVILEGE. Второй аргумент: true – означает выдать привилегию. Третий: false – привилегия выдается для всего процесса. Четвертый аргумент возвращает предыдущее состояние привилегии, то есть, была ли она выдана или нет.

Вторая функция вызывает BSOD путем передачи OptionShutdownSystem в предпоследний аргумент, но вызвать её можно только имея определенные права, а именно SE_SHUTDOWN_PRIVILEGE, который как раз и выдается предыдущей командой.

Далее скомпилируем проект, нажав на нем ПКМ и кликнув «Собрать» (рис. 4).

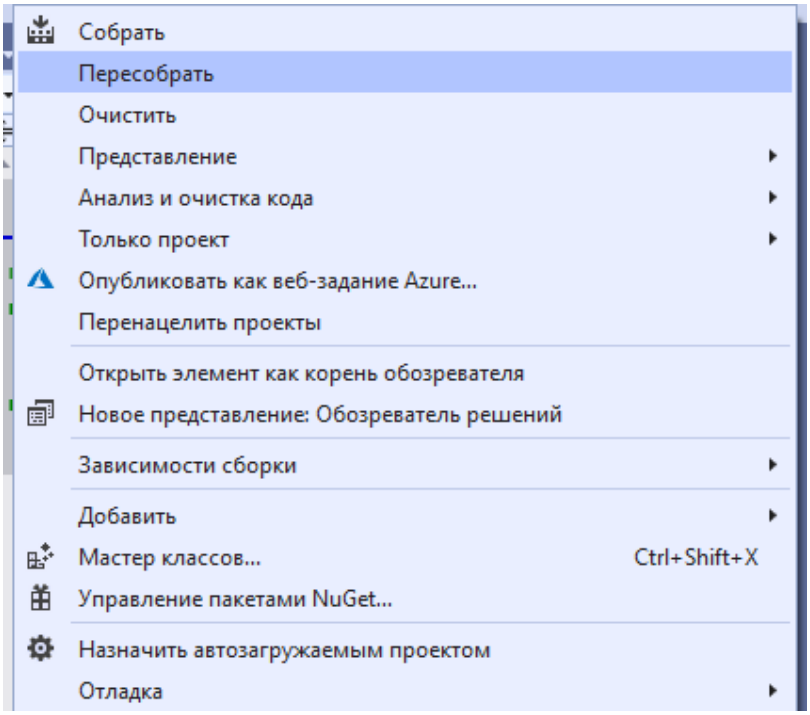

Рисунок 4 – Сборка приложения

Для того чтобы перейти к созданному exe-файлу кликнем по проекту ПКМ и нажмем «Открыть папку в проводнике» (рис. 5).

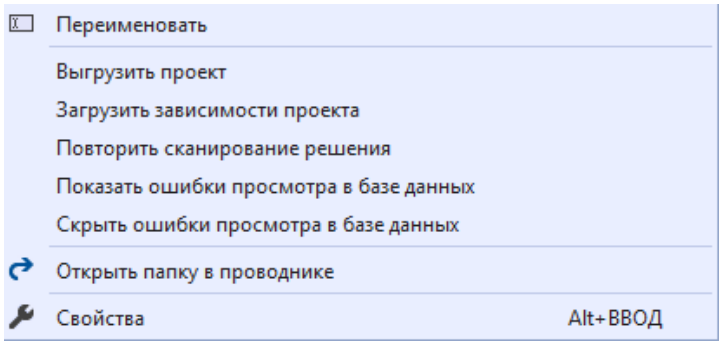

Рисунок 5 – Открытие папки с проектом

Далее переходим на уровень вверх, а затем в папки x64 и Release соответственно. Здесь будет лежать exe-файл с названием аналогичным названию проекта (рис. 6).

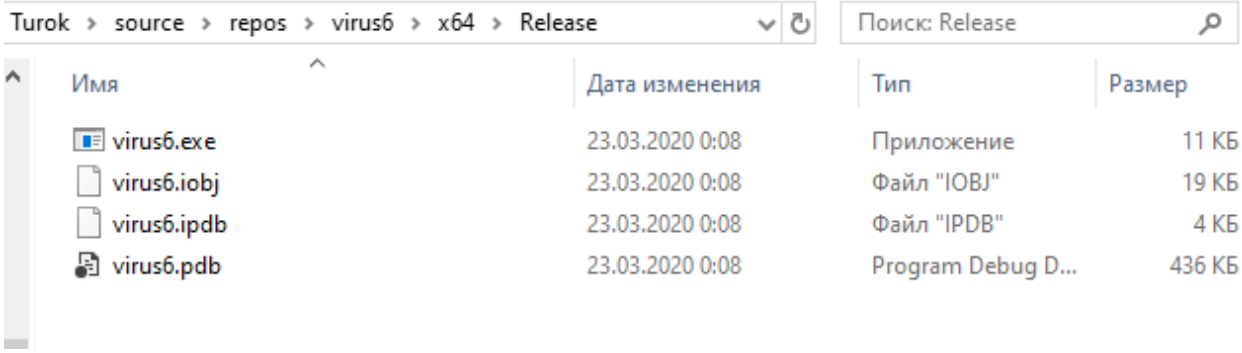

Рисунок 6 – exe-файл

Запустив данный файл появится синий экран смерти после чего компьютер перезагрузится. (рис. 7).

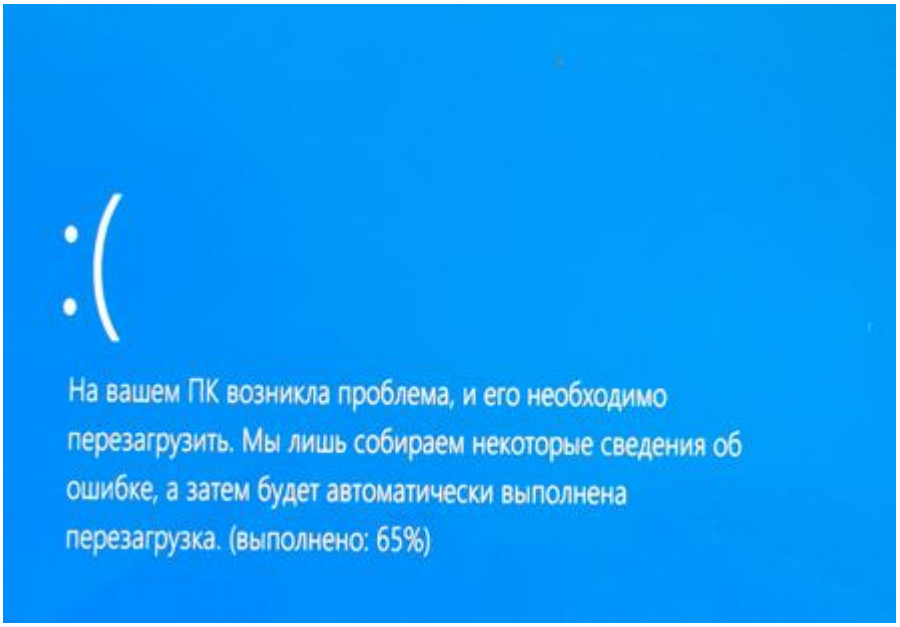

Рисунок 7 – Синий экран смерти (BSOD)

Данный вызов BSOD может печально отразиться на состоянии компьютера из-за затрагивания различных системных библиотек, служащих для стабильной работы ПК.

3. Выводы

В настоящее время с развитием информационных технологий и интернета начинают все активнее распространяться всевозможные компьютерные вирусы, которые как могут причинить вред компьютеру, так и украсть конфиденциальную информацию. Стать жертвой можно, как и простого вируса, который является шуточным и не причинит большого вреда, так и достаточного серьёзного вируса, который может вывести из строя ваше устройство. Для того чтобы не стать добычей киберпреступников следует соблюдать ряд мер в числе которых может присутствовать изучение принципов действия различных компьютерных вирусов.

В данной статье были рассмотрен инструмент Microsoft Visual Studio для создания приложения вызывающего BSOD.

Библиографический список

1. Староверов В. А. Защита информации от компьютерных вирусов // Информатизация образования - 2015. Казань: Частное образовательное учреждение высшего профессионального образования "Академия социального образования, 2015. С. 364-369.
2. Емельянов А. А. Анализ распространения вирусов в компьютерных сетях на основе цепи Маркова // Молодежный научно-технический вестник. 2015. №8 . С. 35.

3. Санникова Т. С. Компьютерные вирусы // Экономика и социум. 2015. № 6-1. С. 883-886.
4. Бородина Н. А., Контарева Н. И., Акользин В. В. Компьютерные вирусы // Теория и практика современной науки. 2016. №1. С. 43-45.
5. Семененко Е. А. Способы распространения компьютерных вирусов // Будущее науки-2016. Курск: Закрытое акционерное общество "Университетская книга, 2016. С. 72-75.
6. Microsoft Visual Studio // Википедия URL: https://ru.wikipedia.org/wiki/Microsoft_Visual_Studio (дата обращения: 25.01.2020).