# ТЕХНИЧЕСКОЕ ЗАДАНИЕ

# 1. Наименование

Программная реализация технологии внедрения DLL библиотеки в целевой процесс «Reflective DLL Injection.

**2. Основание для разработки**

В системном программировании внедрение кода в целевой процесс играет важную роль для решения прикладных задач по поддержке существующих приложений. Процесс внедрения стороннего кода, ожидает запуска конкретного приложения и вводит дополнительный код в запущенный процесс, чтобы изменить или дополнить его функциональные возможности. Например: программная платформа сценариев, такая как «AutoHotkey», с помощью добавления небольшого кода, предоставляет пользователям возможность создавать сценарии, которые запускаются в фоновом режиме с помощью комбинаций, предварительно заданных, горячих клавиш.

Для внедрения кода в целевой процесс существует технология Reflective dll injection. Для применения на практике необходимо разработать её программную реализацию, которая бы эффективно осуществляла внедрение полезной нагрузки и не обнаруживалась антивирусами как вредоносное программное обеспечение.

**3. Исполнитель**

Студент группы ИУК5-42Б Фролов Кирилл Дмитриевич

**4. Цель разработки**

Целью курсовой работы является формирование практических навыков по разработке и реализации программного приложения с использованием интерфейса прикладного программирования (АРI) операционных систем.

Задачи проектирования:

1. овладение первичными навыками ведения научно-исследовательской, проектной и производственно-технологической деятельности, развитие творческих способностей индивидуально для каждого студента;
2. подготовка к выполнению выпускной квалификационной работы;
3. усвоение методов грамотного ведения, оформления и редактирования технической документации.

Целью разработки является изучение принципов системного программирования и работы Windows API, а также программная реализация технологии Reflective dll injection для внедрения dll библиотеки в целевой процесс.

**5. Содержание работы**

**5.1. Задачи, подлежащие решению:**

исследование существующих методов внедрения программного кода в целевой процесс;

изучение методов работы системных библиотек и WinAPI функций;

реализация метода Reflective dll injection;

Тестирование реализованной технологии;

1. подготовка расчетно-пояснительной записки и графических листов;
2. подготовка презентации и речи для защиты курсовой работы;
3. защита курсовой работы.

**5.2. Требования к архитектуре АСОИ**

К архитектуре предъявляются следующие требования:

тип приложения – оконное;

модуль полезной нагрузки, представляющий из себя DLL библиотеку;

модуль загрузчика, представляющий из себя оконное приложение;

модуль загрузчика должен быть представлен в виде отдельного класса;

**5.3. Требования к составу программных компонентов**

Программный комплекс должен состоять из следующих программных компонентов:

1. исполняемый файл PE формата с расширением .exe, реализующий метод Reflective dll injection;
2. полезная нагрузка в виде динамической библиотеки .dll ;

**5.4. Требования к прикладным программам**

Для работы программного комплекса необходимы:

1. Microsoft Windows 8/10;
2. Microsoft Visual Studio 2019;
3. минимальный набор драйверов, обеспечивающих   
   работоспособность ПК.

**5.5. Требования к входным/выходным данным**

Входные данные:

1. PID процесса, в который будет производится внедрение;
2. путь к полезной нагрузке.

Выходные данные:

1. всплывающее окно типа «MessageBox» с сообщением об успешном внедрении.

**5.6. Требования к временным характеристикам**

Требования к временным характеристикам программы не предъявляются

**5.7. Требования к составу технических средств**

Для функционирования системы необходимы:

* Процессор: не менее 1 ГГц
* ОЗУ: 1 ГБ для 32-разрядной системы или 2 ГБ для 64-разрядной системы
* Место на жестком диске:16 ГБ для 32-разрядной ОС или 20 ГБ для 64-разрядной ОС
* Видеоадаптер: DirectX 9 или более поздняя версия с драйвером WDDM 1.0
* Экран: 800 x 600
* монитор;
* клавиатура;
* мышь.

**6. Этапы разработки**

1. создание пользовательского интерфейса;
2. реализация метода Reflective dll injection;
3. тестирование реализованной технологии;

**7. Техническая документация, предъявляемая по окончании работы**

По окончанию работы предъявлена расчетно-пояснительная записка в состав которой входят:

* техническое задание;
* научно-исследовательская часть;
* проектно-конструкторская часть;
* проектно-технологическая часть.

Также должна быть предоставлена графическая часть работы, выполненная формате А1 на 2 листах, в которую входят:

* демонстрационные чертежи;
* алгоритмические схемы.

**8. Дополнительные условия**

язык программирования С/С++;

использование Windows API функций для реализации метод внедрения программного кода в сторонний процесс;

интерфейс должен предоставлять пользователю текстовые поля для ввода PID в который необходимо внедриться и путь к полезной нагрузке, и кнопку «внедриться». По завершении работы должен появиться MessegeBox с информацией что внедрение произошло успешно.