**ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ**
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ**
**«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»**

Факультет компьютерных наук

Департамент программной инженерии

| | |
|---|---|
| СОГЛАСОВАНО<br>Приглашенный преподаватель<br>департамента программной инженерии,<br>к.т.н., доцент | УТВЕРЖДАЮ<br>Академический руководитель<br>образовательной программы<br>«Программная инженерия»<br>профессор, канд. техн. наук |
| _____ А.Д.Брейман<br>«___» _____ 2020 г. | _____ В.В. Шилов<br>«___» _____2020 г. |

| | |
|---|---|
| Подп. и дата | |
| Инв. № дубл. | |
| Взам. Инв. № | |
| Подп. и дата | |
| Инв. № подл. | |

**Программа для защиты исполняемого файла от уязвимости переполнения буфера на стеке путём переноса стека вызовов в кучу**
**Техническое задание**

**ЛИСТ УТВЕРЖДЕНИЯ**
**RU.17701729.02.13-01 ТЗ 01-1-ЛУ**

Исполнитель
Студент группы БПИ 184
_____/Новак В.А./
«___»_____2020 г.

**Москва 2020**

Утверждено
RU.17701729.02.13-01 ТЗ 01-1

# Программа для защиты исполняемого файла от уязвимости переполнения буфера на стеке путём переноса стека вызовов в кучу

## Техническое задание

## RU.17701729.02.13-01 ТЗ 01-1

## Листов 15

| Подп. и дата | |
|---|---|
| Инв. № дубл. | |
| Взам. Инв. № | |
| Подп. и дата | |
| Инв. № подл. | |

**Москва 2020**

# Содержание

# 1. Введение

## 1.1. Наименование программы:

Наименование программы: «Программа для защиты исполняемого файла от уязвимости переполнения буфера на стеке путём переноса стека вызовов в кучу» («Program for protecting an executable file from stack buffer overflow vulnerability by moving call stack to heap»).

## 1.2. Область применения программы

Программа может быть использована для защиты исполняемых файлов от внедрения вредоносного кода путём изменения адреса возврата через эксплуатацию уязвимости буфера на стеке.

# 2. Основания для разработки

Основанием для разработки является приказ декана факультета компьютерных наук НИУ ВШЭ И.В. Аржанцева от XX.XX.2019 г. № XXXXXX.

# 3. Назначение разработки

## 3.1. Функциональное назначение

Программа модифицирует поданный на вход исполняемый файл, так что получаемый в результате исполняемый файл при вызовах подпрограмм будет использовать кучу для хранения адресов возврата.

## 3.2. Эксплуатационное назначение

Программа может быть использована для защиты исполняемых файлов от внедрения вредоносного кода путём изменения адреса возврата через эксплуатацию уязвимости буфера на стеке.

# 4. Требования к программе

## 4.1. Требование к функциональным характеристикам

### 4.1.1. Требования к составу выполняемых функций

Программа должна позволять пользователю:

- Изменять в зависимости от выбранного пользователем значения из поддерживаемых программой следующие параметры:
  - Имена входного и выходного файлов;
  - Тип архитектуры исполняемого файла;
  - Размер стека вызовов.
- Отображать прогресс обработки исполняемого файла в виде списка обработанных функций

### 4.1.2. Требования к интерфейсу

- Программа должна получать через аргументы командной строки значения следующих параметров:
  - Имена входного и выходного файлов;
  - Тип архитектуры исполняемого файла;
  - Размер стека вызовов.
- Программа должна считывать входные данные и выводить результат через указанные в аргументах командной строки файлы.

### 4.1.3. Требования к формату входных данных

- Программа должна получать через аргументы командной строки значения следующих параметров:
  - Имена входного и выходного файлов;
  - Тип архитектуры исполняемого файла;
  - Размер стека вызовов.
- Программа должна считывать входные данные из указанного в аргументах командной строки файла для ввода.

### 4.1.4. Требования к выходным данным

- Программа должна выводить результат в указанный в аргументах командной строки файл для вывода.
- Во время работы программы прогресс обработки выводится в стандартный поток вывода в виде списка обработанных функций.

## 4.2. Требования к надёжности

При любом вводе пользователя программа не должна завершаться аварийно. При неправильном формате вводимых данных программа должна завершаться с сообщением о некорректных входных данных.

## 4.3. Условия эксплуатации

### 4.3.1. Климатические условия

Климатические условия эксплуатации, при которых должны обеспечиваться заданные характеристики, должны удовлетворять требованиям, предъявляемым к персональным компьютерам.

Персональный компьютер предназначен для работы в закрытом отапливаемом помещении со стабильными климатическими условиями согласно [1].

1) влажность от 20% до 70%;
2) температура от 5°C до 30°C;
3) атмосферное давление — от 84 до 106,7 кПа (от 630 до 800 мм рт. ст.).

### 4.3.2. Требования к квалификации оператора

Не требует специального обслуживания. Требуемая квалификация – продвинутый пользователь.

## 4.4. Требования к составу и параметрам технических средств

Минимальные требования программы для работоспособности.

- Процессор архитектуры AMD или Intel с частотой не менее 2,10 ГГц;
- Не менее 150мб ОЗУ;
- Не менее 80мб на жёстком диске;
- Клавиатура.

## 4.5. Требования к информативной и программной совместимости

- Windows 7 или более поздняя версия операционной системы (32-разрядные или 64-разрядные).

## 4.6. Требования к маркировке и упаковке

При хранении на физическом носителе на нём должны быть указаны ФИО Исполнителя, название продукта и год окончания разработки.

## 4.7. Требования к транспортировке и хранению

Программное изделие может храниться и транспортироваться на флэш-носителе и распространяться через облачное хранилище.

# 5. Требования к программной документации

## 5.1. Состав программной документации

В рамках данной работы должна быть разработана следующая программная документация в соответствии с ГОСТ ЕСПД:

- «Программа для защиты исполняемого файла от уязвимости переполнения буфера на стеке путём переноса стека вызовов в кучу». Техническое задание (ГОСТ 19.201-78) [2];
- «Программа для защиты исполняемого файла от уязвимости переполнения буфера на стеке путём переноса стека вызовов в кучу». Программа и методика испытаний (ГОСТ 19.301-79) [3];
- «Программа для защиты исполняемого файла от уязвимости переполнения буфера на стеке путём переноса стека вызовов в кучу». Текст программы (ГОСТ 19.401-78) [4];
- «Программа для защиты исполняемого файла от уязвимости переполнения буфера на стеке путём переноса стека вызовов в кучу». Пояснительная записка (ГОСТ 19.404-79) [5];
- «Программа для защиты исполняемого файла от уязвимости переполнения буфера на стеке путём переноса стека вызовов в кучу». Руководство оператора (ГОСТ 19.505-79) [6].

## 5.2. Специальные требования к программной документации

Документы к программе должны быть выполнены в соответствии с ГОСТ 19.106-78 и ГОСТами к каждому виду документа (см. п. 5.1);

Пояснительная записка должна быть загружена в систему «Антиплагиат» через LMS «НИУ ВШЭ». Лист, подтверждающий загрузку пояснительной записки, сдается в учебный офис вместе со всеми материалами не позже, чем за день до защиты курсовой работы;

Вся документация также воспроизводится в печатном виде, она должна быть подписана исполнителем и руководителем разработки и утверждена академическим руководителем образовательной программы 09.03.04 «Программная инженерия» перед сдачей курсовой работы в учебный офис не позже одного дня до защиты;

Документация и программа также сдается в электронном виде в формате .pdf или .docx. в архиве формата .zip или .rar;

За один день до защиты комиссии все материалы курсового проекта:

– техническая документация,

– программный проект,

– исполняемый файл,

– отзыв руководителя

должны быть загружены одним или несколькими архивами в проект дисциплины «Курсовой проект 2019-2020» в личном кабинете в информационной образовательной среде LMS (Learning Management System) НИУ ВШЭ.

# 6. Технико-экономические показатели

В рамках данной работы расчет экономической эффективности не предусмотрен.

## 6.1. Предполагаемая потребность

Данная программа будет полезна для защиты исполняемых файлов от внедрения вредоносного кода путём изменения адреса возврата через эксплуатацию уязвимости буфера на стеке.

## 6.2. Экономические преимущества разработки по сравнению с отечественными и зарубежными аналогами

На момент начала разработки найдены следующие аналоги:

- GCC StackGuard;
- Компилятор Microsoft Visual Studio (имеет встроенную защиту от описанной уязвимости).

Сравнение характеристик данной программы с аналогами будет выполнено после завершения разработки.

# 7. Стадии и этапы разработки

## 7.1.Стадии разработки

| Стадии разработки | Этапы работ | Содержание работ |
|---|---|---|
| **1. Техническое задание** | Обоснование необходимости разработки программы | Постановка задачи |
| | | Сбор теоретического материала. |
| | Научно-исследовательские работы | Определение структуры входных и выходных данных. |
| | | Предварительный выбор методов решения поставленной задачи. |
| | | Определение требований к техническим средствам. |
| | | Обоснование возможности решения поставленной задачи |
| | Разработка и утверждение технического задания | Определение требований к программе. |
| | | Определение стадий, этапов и сроков разработки программы и документации на неё. |
| | | Выбор языка программирования и платформы разработки. |
| | | Согласование и утверждение технического задания. |
| **2. Рабочий проект** | Разработка программы | Реализация программного интерфейса |
| | | Отладка программы |
| | Разработка программной документации | Разработка программных документов в соответствии с требованиями ЕСПД (ГОСТ 19.101-77). |
| | Испытания программы | Разработка, согласование и утверждение порядка и методики испытаний. |
| | | Проведение предварительных приемо-сдаточных испытаний. |
| | | Корректировка программы и программной документации по результатам испытаний. |
| **3. Внедрение** | Подготовка и защита программного продукта. | Подготовка программы и программной документации для презентации и защиты. |
| | | Утверждение дня защиты программы. |
| | | Презентация программного продукта. |
| | | Передача программы и программной документации в архив НИУ ВШЭ. |

## 7.2.Сроки разработки и исполнители

Разработка должна закончиться к 22 мая 2020 года.

Исполнитель: **Новак Василий Андреевич**, студент группы БПИ184 факультета компьютерных наук НИУ ВШЭ.

# 8. Порядок контроля и приемки

Контроль и приемка разработки осуществляются в соответствии с программным документом «Программа для защиты исполняемого файла от уязвимости переполнения буфера на стеке путём переноса стека вызовов в кучу». Программа и методика испытаний [3].

# 9. Список литературы

1. ГОСТ 15150-69 Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды. – М.: Изд-во стандартов, 1997.
2. ГОСТ 19.201-78 Техническое задание. Требования к содержанию и оформлению. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
3. ГОСТ 19.301-79 Программа и методика испытаний. Требования к содержанию и оформлению. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
4. ГОСТ 19.401-78. ЕСПД. Текст программы. Требования к содержанию и оформлению. – М.: ИПК Издательство стандартов, 2001.
5. ГОСТ 19.404-79. ЕСПД. Пояснительная записка. Требования к содержанию и оформлению. – М.: ИПК Издательство стандартов, 2001.
6. ГОСТ 19.505-79. ЕСПД. Руководство оператора. Требования к содержанию и оформлению. – М.: ИПК Издательство стандартов, 2001.

# 10. Лист регистрации изменений

| Изм. | Номера листов (страниц) | | | | Всего листов (страниц) в документе | № документа | Входящий № сопроводительного документа и дата | Подпись | Дата |
|---|---|---|---|---|---|---|---|---|---|
| | измененных | замененных | Новых | аннулированных | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

| | | | | |
|---|---|---|---|---|
| Изм. | Лист | № докум. | Подп. | Дата |
| RU.17701729.02.13-01 ТЗ 01-1 | | | | |
| Инв. № подл. | Подп. и дата | Взам. Инв. № | Инв. № дубл. | Подп. и дата |