

Министерство образования и науки Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ»

УТВЕРЖДАЮ

Зав. каф. компьютерных технологий

докт. техн. наук, проф.

_____ Васильев В.Н.

«__» _____ 20__ г.

ЗАДАНИЕ
НА МАГИСТЕРСКУЮ ДИССЕРТАЦИЮ

Студент Громаковский И.Е. **Группа** М4239 **Кафедра** компьютерных технологий
Факультет информационных технологий и программирования **Руководитель** Лукин М.А.,
канд. техн. наук, тьютор кафедры КТ Университета ИТМО

1 Наименование темы: Разработка алгоритмов статического поиска выходов за пределы динамического массива в C/C++ программах

Направление подготовки (специальность): 01.04.02 Прикладная математика и информатика

Направленность (профиль): Технологии проектирования и разработки программного обеспечения

Квалификация: Магистр

2 Срок сдачи студентом законченной работы: «31» мая 2017 г.

3 Техническое задание и исходные данные к работе.

Требуется разработать и реализовать алгоритм статического поиска выходов за пределы динамического массива в C/C++ программах. Необходимо обрабатывать промышленные программы больших размеров (состоящие из сотен тысяч строк) за разумное время (порядка нескольких десятков минут). Анализатор должен находить как можно больше ошибок с как можно меньшим числом ложных срабатываний. На сегодняшний день известно множество свободно распространяемых анализаторов, решающих аналогичную или более общую проблему. В данной работе необходимо также произвести сравнение с другими анализаторами.

4 Содержание магистерской диссертации (перечень подлежащих разработке вопросов)

- а) Обоснование актуальности задачи, описание предметной области, обзор существующих решений.
- б) Теоретическое исследование задачи поиска выходов за пределы динамического массива в C/C++. Разработка алгоритма.
- в) Описание практической реализации алгоритма, результаты экспериментов, сравнение с другими анализаторами.

5 Перечень графического материала (с указанием обязательного материала)

Не предусмотрено

6 Исходные материалы и пособия

- а) Li, Lian, Cristina Cifuentes, and Nathan Keynes. "Practical and effective symbolic analysis for buffer overflow detection." Proceedings of the eighteenth ACM SIGSOFT international symposium on Foundations of software engineering. ACM, 2010.
- б) Shahriar, Hossain, and Mohammad Zulkernine. "Classification of static analysis-based buffer overflow detectors." Secure Software Integration and Reliability Improvement Companion (SSIRI-C), 2010 Fourth International Conference on. IEEE, 2010.
- в) Le, Wei, and Mary Lou Soffa. "Marple: a demand-driven path-sensitive buffer overflow detector." Proceedings of the 16th ACM SIGSOFT International Symposium on Foundations of software engineering. ACM, 2008.
- г) Ding, Sun, et al. "Detection of buffer overflow vulnerabilities in C/C++ with pattern based limited symbolic evaluation." Computer Software and Applications Conference Workshops (COMPSACW), 2012 IEEE 36th Annual. IEEE, 2012.

7 Календарный план

№№ пп.	Наименование этапов магистерской диссертации	Срок выполнения этапов работы	Отметка о выполнении, подпись руков.
1	Ознакомление с основами статического анализа	до 15.11.2015	
2	Изучение существующих подходов к решению данной проблемы	до 28.02.2016	
3	Разработка и реализация прототипа анализатора	до 30.06.2016	
4	Исследование преимуществ и недостатков прототипа, разработка теоретических улучшений	до 20.11.2016	
5	Реализация улучшенной версии анализатора	до 25.01.2017	
6	Проведение экспериментов, сравнение с другими анализаторами	до 26.02.2017	
7	Написание пояснительной записки	до 31.05.2017	

8 Дата выдачи задания: «01» сентября 2015 г.

Руководитель _____

Задание принял к исполнению _____ «01» сентября 2015 г.