**Министерство образования и науки Российской Федерации**

**федеральное государственное автономное образовательное учреждение высшего образования**

**“САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ**

**УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ,**

**МЕХАНИКИ И ОПТИКИ”**

**АнНотация**

**ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**

**Студент** Просочкина Дарья Андреевна .

(ФИО)

**Наименование темы ВКР:** «Поиск уязвимостей нарушения целостности динамическим анализом программ на языке JavaScript» .

**Наименование организации, где выполнена ВКР** Университет ИТМO .

**ХАРАКТЕРИСТИКА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**

1 Цель исследования: разработка средства поиска уязвимостей нарушения целостности, доступного любому разработчику и позволяющего сократить время, затрачиваемое на локализацию уязвимости. .

2 Задачи, решаемые в ВКР: обзор существующих средств поиска уязвимостей; разработка нового средства; тестирование разработанного средства, подтверждение корректности его работы. .

3 Число источников, использованных при составлении обзора\_\_\_\_\_\_\_\_9\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4 Полное число источников, использованных в работе \_\_\_\_\_\_\_\_\_\_\_\_\_21\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

5 В том числе источников по года

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Отечественных** | | | **Иностранных** | | |
| Последние 5 лет | От 5 до 10 лет | Более 10 лет | Последние  5 лет | От  5 до 10 лет | Более 10 лет |
| 1 | 1 | 2 | 12 | 1 | 4 |

6 Использование информационных ресурсов Internet\_\_\_\_\_\_\_\_\_\_\_\_\_Да, 10\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Да, нет, число ссылок в списке литературы)

7 Использование современных пакетов компьютерных программ и технологий (Указать, какие именно, и в каком разделе работы)

Обзор существующих средств: статический анализатор кода ScanJs; разработка нового средства: платформа Node.js, парсер Esprima, библиотека falafel, браузер Google Chrome

8 Краткая характеристика полученных результатов

Было разработано средство поиска уязвимостей нарушения целостности (в частности уязвимости DOM-based XSS) в программах на языке JavaScript, использующее метод динамического анализа хода выполнения программ и позволяющее сократить время, затрачиваемое на локализацию уязвимости. Корректность работы средства подтверждена найденной с его помощью уязвимостью в реальном проекте.

9 Полученные гранты, при выполнении работы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_-\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Название гранта)

10 Наличие публикаций и выступлений на конференциях по теме выпускной работы \_Да\_\_

(Да, нет)

а) 1 Просочкина Д. А. Поиск уязвимостей нарушения целостности динамическим анализом

(Библиографическое описание публикаций)

программ на языке JavaScript/ Д. А. Просочкина// Список-2016: Материалы всероссийской научной конференции по проблемам информатики. 26-29 апреля 2016 г. Санкт-Петербург. – СПб.: ВВМ, 2016 (тезисы приняты к публикации).

б) 1 Доклад «Поиск уязвимостей нарушения целостности динамическим анализом программ на языке JavaScript». Всероссийская научная конференция по проблемам информатики «СПИСОК-2016» (26.04.2016 – 29.04.2016). Место проведения: Санкт-Петербургский государственный университет.

(Библиографическое описание выступлений на конференциях)

Выпускник Просочкина Д. А \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ФИО) (подпись)

Руководитель Спивак А. И. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ФИО) (подпись)

“\_\_\_\_\_\_\_\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г.