ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 24.1.120.01,
созданного на базе
Федерального государственного бюджетного учреждения науки
Институт системного программирования им. В.П. Иванникова
Российской академии наук
Министерства науки и высшего образования РФ
по диссертации на соискание ученой степени кандидата наук

аттестационное дело № _____

решение диссертационного совета от 15 декабря 2022 года № 2022/13

О присуждении Вишнякову Алексею Вадимовичу, гражданину РФ, ученой степени кандидата физико-математических наук.

Диссертация «Поиск ошибок в бинарном коде методами динамической символьной интерпретации» по специальности 2.3.5 – «математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей» принята к защите 14 октября 2022, протокол № 2022/06 диссертационным советом 24.1.120.01, созданным на базе Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность: Министерство науки и высшего образования РФ; адрес: 109004, г. Москва, ул. А. Солженицына, дом 25), создан Приказом Минобрнауки России о советах по защите докторских и кандидатских диссертаций от 2 ноября 2012 г. № 714/нк.

Соискатель Вишняков Алексей Вадимович, 1996 года рождения.

В 2020 году соискатель окончил факультет вычислительной математики и кибернетики Московского государственного университета имени М. В. Ломоносова по специальности «Прикладная математика и информатика».

Работает младшим научным сотрудником в отделе компиляторных технологий ФГБУН Института системного программирования

им. В. П. Иванникова Российской академии наук (ведомственная принадлежность: Министерство науки и высшего образования РФ).

Диссертация выполнена в отделе компиляторных технологий ФГБУН Института системного программирования им. В. П. Иванникова РАН (ведомственная принадлежность: Министерство науки и высшего образования РФ).

Научный руководитель – кандидат технических наук Федотов Андрей Николаевич, старший научный сотрудник отдела компиляторных технологий ФГБУН Института системного программирования им. В. П. Иванникова РАН.

Официальные оппоненты:

1. Ильин Вячеслав Анатольевич, доктор физико-математических наук, главный научный сотрудник Курчатовского комплекса НБИКС-природоподобных технологий Федерального государственного бюджетного учреждения «Национальный исследовательский центр «Курчатовский институт»,
2. Дмитрий Олегович Маркин, кандидат технических наук, сотрудник ФГКВОУ ВО «Академия Федеральной службы охраны Российской Федерации»

дали положительные отзывы на диссертацию.

Ведущая организация Федеральное государственное учреждение «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», г. Москва в своем положительном заключении, подписанном руководителем отделения ФИЦ ИУ РАН доктором физико-математических наук Синициным Владимиром Игоревичем, указала, что диссертация является законченной научно-квалификационной работой, в которой решена актуальная задача разработки нового автоматизированного комплексного метода обнаружения ошибок в контексте гибридного фаззинга, и полностью соответствует паспорту научной специальности 2.3.5 —

математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей.

Соискатель имеет 16 опубликованных работ, в том числе по теме диссертации опубликовано 6 работ, из них в рецензируемых научных изданиях опубликовано 4 работы.

Публикации посвящены разработке методов поиска ошибок (деления на ноль, целочисленного переполнения и выхода за границу массива) в бинарном коде методами динамической символьной интерпретации. Вклад соискателя в совместных публикациях заключается в разработке алгоритма слайсинга предиката пути, разработке методов моделирования семантики функций, построения предикатов безопасности и автоматизированного поиска ошибок в контексте гибридного фаззинга, реализации методов, обработке и интерпретации экспериментальных результатов, подготовке статей.

Наиболее значимые работы по теме диссертации:

1. Вишняков, А. В. Поиск ошибок в бинарном коде методами динамической символьной интерпретации / А. В. Вишняков, И. А. Кобрин, А. Н. Федотов // Труды Института системного программирования РАН. — 2022. — Т. 34, № 2. — С. 25—42. — (ВАК).
2. Symbolic Security Predicates: Hunt Program Weaknesses / A. Vishnyakov [et al.] // 2021 Ivannikov ISPRAS Open Conference (ISPRAS). — IEEE, 2021. — P. 76—85. — (Scopus, WoS).
3. Sydr: Cutting Edge Dynamic Symbolic Execution / A. Vishnyakov [et al.] // 2020 Ivannikov ISPRAS Open Conference (ISPRAS). — IEEE, 2020. — P. 46—54. — (Scopus, WoS).

Выбор официальных оппонентов и ведущей организации обосновывается их компетентностью и достижениями в данной отрасли науки, наличием публикаций в сфере исследований, соответствующей теме диссертации, и способностью определить научную и практическую ценность диссертации.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

- Разработан алгоритм слайсинга предиката пути, который позволяет устранять избыточные ограничения во время динамической символьной интерпретации. Для предложенного алгоритма были доказаны теоремы о его конечности и корректности. Была произведена формальная оценка асимптотической сложности алгоритма. Проведена экспериментальная оценка эффективности алгоритма, которая показала повышение скорости и точности инвертирования условных переходов.
- Разработан метод построения предикатов безопасности для обнаружения ошибок деления на ноль, выхода за границу массива и целочисленного переполнения при помощи динамической символьной интерпретации бинарного кода. Экспериментальная оценка метода на наборе тестов Juliet показала общую точность 95.59 % для 11 классов ошибок CWE (15772 теста).
- Разработан метод автоматизированного поиска ошибок при помощи символьных предикатов безопасности после гибридного фаззинга. Предложенный метод позволил обнаружить 17 новых ошибок в 10 различных проектах с открытым исходным кодом.
- Предложенные методы были реализованы в программных системах, которые используются в Центре доверенного искусственного интеллекта ИСП РАН.

Теоретическая значимость исследования обоснована тем, что:

- разработаны методы построения предикатов безопасности для обнаружения ошибок деления на ноль, выхода за границу массива и целочисленного переполнения в бинарном коде, которые применимы для анализа больших программных систем в контексте гибридного фаззинга;
- разработан алгоритм слайсинга предиката пути, устраняющий избыточные ограничения во время динамической символьной интерпретации;
- формально исследованы свойства алгоритма слайсинга предиката пути и доказаны необходимые теоремы.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

- разработанные методы позволяют обнаруживать новые программные дефекты в бинарном коде и порождать входные данные для их подтверждения;
- методы позволяют автоматически выделить истинно положительные срабатывания символьных предикатов безопасности;
- предложенные методы встраиваются в системы непрерывной интеграции в рамках следования безопасному циклу разработки ПО;
- разработанные методы позволили обнаружить новые ошибки в различных проектах с открытым исходным кодом;
- разработанные методы используются в Центре доверенного искусственного интеллекта ИСП РАН;
- методы могут применяться в будущем для сертификации и безопасного цикла разработки ПО.

Оценка достоверности результатов исследования выявила:

- формально исследованы свойства алгоритма слайсинга предиката пути: доказаны теоремы о его конечности, корректности, и проведена оценка его вычислительной сложности;
- проведена экспериментальная оценка алгоритма слайсинга предиката пути, которая показала повышение точности и скорости порождения входных данных;
- измерена точность метода построения предикатов безопасности для поиска ошибок в бинарном коде на наборе тестов Juliet, показана общая точность 95.59 %;
- апробирован метод автоматизированного поиска ошибок при помощи символьных предикатов безопасности на различных проектах с открытым исходным кодом, было обнаружено 17 новых ошибок.

Личный вклад соискателя состоит в разработке алгоритма слайсинга предиката пути, методов построения предикатов безопасности и

автоматизированного обнаружения ошибок в контексте гибридного фаззинга, реализации методов, обработке и интерпретации экспериментальных результатов, подготовке статей.

В ходе защиты диссертации были высказаны следующие критические замечания:

- не указано время построения предикатов безопасности и обнаружения ошибок;
- не рассмотрен вопрос об ограничениях по типам ошибок, к которым можно применять разработанные методы;
- не приводится анализ и оценка достаточности и избыточности ограничений предиката пути;
- не описаны процессорные архитектуры и объем программ, к которым применим алгоритм слайсинга предиката пути.

Соискатель Вишняков Алексей Вадимович согласился с замечаниями, ответил на задаваемые ему в ходе заседания вопросы.

На заседании 15 декабря 2022 г. диссертационный совет принял решение присудить Вишнякову А. В. ученую степень кандидата физико-математических наук.

При проведении тайного голосования диссертационный совет в количестве 16 человек, из них 6 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 22 человек, входящих в состав совета, проголосовали: за – 16, против – 0.

Председатель диссертационного совета,
академик РАН Аветисян А. И.

Ученый секретарь диссертационного совета,
кандидат физико-математических наук Зеленов С. В.

15 декабря 2022 года