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 11 декабря 2025 года № 2025/28

О присуждении Логуновой Владе Игоревне, гражданке РФ, ученой степени кандидата технических наук.

Диссертация «Разработка методов гибридного фаззинга для приложений процессорных архитектур Байкал-М и RISC-V 64» по специальности 2.3.5 – «математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей» принята к защите 7 октября 2025 года (протокол № 2025/20) 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 Логунова Влада Игоревна, 22.01.1998 года рождения.

В 2022 году соискатель окончила Физтех-школу прикладной математики и информатики федерального государственного автономного образовательного учреждения высшего образования «Московский физико-технический институт (национальный исследовательский университет)» по направлению подготовки «03.04.01 Прикладные математика и физика». В 2025 году соискатель окончила аспирантуру федерального государственного автономного образовательного

учреждения высшего образования «Московский физико-технический институт (национальный исследовательский университет)».

Работает стажером-исследователем в отделе компиляторных технологий Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность: Министерство науки и высшего образования РФ).

Диссертация выполнена в Федеральном государственном бюджетном учреждении науки Институт системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность: Министерство науки и высшего образования РФ).

Научный руководитель – кандидат физико-математических наук Гетьман Александр Игоревич, старший научный сотрудник отдела компиляторных технологий ФГБУН Института системного программирования им. В.П. Иванникова РАН.

Официальные оппоненты:

1. Шабанов Борис Михайлович, доктор технических наук, член-корр. РАН, руководитель отделения Федерального государственного бюджетного учреждения «Национальный исследовательский центр «Курчатовский институт».
2. Маркин Дмитрий Олегович, 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» (ФИЦ ИУ РАН), г. Москва, в своем положительном заключении, подписанном Разумчиком Ростиславом Валерьевичем, д.ф.-м.н, заместителем директора ФИЦ ИУ РАН по научной работе, и Синициным Владимиром Игоревичем, д.ф.-м.н., руководителем отделения ФИЦ ИУ РАН, гл. науч. сотр., указала, что диссертация является

законченной научно-квалификационной работой, в которой решена актуальная задача разработки методов гибридного фаззинга для приложений процессорных архитектур Байкал-М и RISC-V 64, и полностью соответствует требованиям ВАК РФ к диссертационным работам на соискание звания кандидата технических наук по специальности 2.3.5. – математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей.

Соискатель имеет 6 опубликованных работ, в том числе по теме диссертации опубликовано 5 работ, из них в рецензируемых научных изданиях опубликовано 5 работ, в изданиях из перечня ВАК – 2 работы. По теме работы получено 1 свидетельство о регистрации программы для ЭВМ.

Публикации посвящены динамическому анализу бинарных программ и разработке методов динамической символьной интерпретации и гибридного фаззинга. Вклад соискателя в совместных работах заключается в разработке метода моделирования семантики функций стандартной библиотеки, исследовании существующих решений для проведения динамической символьной интерпретации и для реализации концепции непрерывного фаззинг-тестирования, а также изложении последовательности применения инструментов, повышающей эффективность динамического анализа при проведении гибридного фаззинг-тестирования. Основные результаты диссертации опубликованы в работе с единоличным авторством.

Список опубликованных работ по теме диссертации:

1. Логунова В.И. Применение динамической символьной интерпретации в гибридном фаззинге бинарного кода для архитектур Байкал-М и RISC-V 64 [Текст]. Труды Института системного программирования РАН, том 37, вып. 4, часть 2, 2025, стр. 235-250. DOI: 10.15514/ISPRAS-2025-37(4)-29.

2. Вишняков А.В. Sydr-Fuzz: непрерывный гибридный фаззинг и динамический анализ для жизненного цикла безопасной разработки [Текст] / Вишняков А.В., Куц Д.О., Логунова В.И. [и др.] // Труды Института системного программирования РАН, том 37, вып. 4, часть 2, 2025, стр. 251-270. DOI: 10.15514/ISPRAS-2025-37(4)-30.

3. *Vishnyakov, A.* Sydr-Fuzz: Continuous Hybrid Fuzzing and Dynamic Analysis for Security Development Lifecycle [Текст]/ A. Vishnyakov, D. Kuts, V. Logunova, D. Parygina, E. Kobrin, G. Savidov, A. Fedotov // 2022 Ivannikov ISPRAS Open Conference (ISPRAS). IEEE, 2022. — С. 111–123.

4. *Vishnyakov, A. Symbolic Security Predicates: Hunt Program Weaknesses [Текст] / A. Vishnyakov, V. Logunova, E. Kobrin, D. Kuts [и др.] // 2021 Ivannikov Ispras Open Conference (ISPRAS). —IEEE. 2021. — С. 76—85.*

5. *Vishnyakov, A.* Sydr: Cutting edge dynamic symbolic execution [Текст] / A. Vishnyakov, A. Fedotov, D. Kuts, A. Novikov, D. Parygina, E. Kobrin, V. Logunova, P. Belecky, Sh. Kurmangaleev // 2020 Ivannikov ISPRAS Open Conference (ISPRAS). — IEEE. 2020. — С. 46—54.

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 метод символьной интерпретации набора целочисленных инструкций архитектуры, RISC-V, включающего сокращенные инструкции и псевдоинструкции. Разработанный метод реализует символьную семантику инструкций, посредством конструирования SMT-формулы, описывающей преобразование символьного контекста на уровне выполнения отдельной инструкции RISC-V. Апробация метода продемонстрировала его применимость как для проведения символьной эмуляции, так и в рамках реализации конкретно-символьного анализа.
- Разработаны методы динамической символьной интерпретации бинарного кода архитектур Байкал-М (AArch64) и RISC-V 64. Методы предоставляют возможность точного определения границ для множественных условных переходов, что позволяет выявлять соответствующие целевые адреса исполняемого кода в процессе динамической символьной интерпретации бинарного кода и ускорять исследование новых путей выполнения.

Экспериментальная оценка разработанных методов показала их практическую применимость в контексте проведения гибридного фаззинг-тестирования прикладных программ целевых архитектур.

- Предложенные методы были реализованы в программных системах, которые используются в Центре доверенного искусственного интеллекта ИСП РАН, а также в процессах безопасной разработки ООО «Фобос-НТ» и ООО «Лаборатория безопасности».

Теоретическая значимость исследования обоснована тем, что:

- разработаны методы динамической символьной интерпретации бинарного кода процессорных архитектур Байкал-М (AArch64) и RISC-V 64, а также метод символьной интерпретации набора целочисленных инструкций архитектуры RISC-V на основе конструирования абстрактных синтаксических деревьев их операционной семантики;
- изучены различные способы обеспечения переносимости технологий символьного анализа для бинарного кода и проведена экспериментальная оценка эффективности разработанных методов динамической символьной интерпретации для анализа бинарных приложений целевых архитектур в контексте гибридного фаззинг-тестирования.

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

- разработанные методы позволяют увеличивать покрытие исследуемых приложений в процессе динамического анализа бинарного кода, способствуя обнаружению новых программных дефектов;
- разработанные методы динамической символьной интерпретации используются в Центре доверенного искусственного интеллекта ИСП РАН;
- разработанные методы динамической символьной интерпретации внедрены в процессы безопасной разработки ООО «Фобос-НТ» и ООО «Лаборатория безопасности»;
- разработанный метод символьной интерпретации целочисленных инструкций RISC-V интегрирован в открытую символьную библиотеку Triton, которая может быть использована сообществом исследователей

бинарного кода для создания собственных инструментов динамического анализа.

Оценка достоверности результатов исследования выявила:

- разработанные методы, реализованные в составе инструмента динамической символьной интерпретации Sydr и открытой символьной библиотеки Triton, показывают свою практическую применимость для проведения символьного анализа и в контексте гибридного фаззинг-тестирования прикладных программ целевых архитектур;
- экспериментально показана эффективность предложенных методов с точки зрения увеличения покрытия исследуемого кода при проведении динамического анализа бинарных программ.

Личный вклад соискателя состоит в разработке методов динамической символьной интерпретации бинарного кода архитектур Байкал-М (AArch64) и RISC-V 64, метода символьной интерпретации набора целочисленных инструкций архитектуры RISC-V, включающего сокращенные инструкции и псевдоинструкции, реализации указанных методов, обработке и интерпретации экспериментальных результатов, подготовке публикаций.

В ходе защиты диссертации были высказаны следующие критические замечания:

- недостаточно подробно раскрыты способы определения размеров таблиц косвенных переходов в бинарном коде;
- не приводится анализ и оценка достаточности набора используемых расширений архитектеры RISC-V;
- для архитектуры RISC-V 64 не приводится сравнение гибридного фаззинга с инструментом AFL++;
- не приведена оценка производительности символьной эмуляции для подтверждения заключения об ограничениях возможностей ее практического применения в контексте гибридного фаззинга;
- неочевидна целесообразность указания архитектуры Байкал-М как целевой для разработки метода относительно архитектуры AArch64;
- по содержанию автореферата и диссертации не удалось оценить полноту набора интерпретируемых инструкций относительного их общего

количества, а также качество реализации инструкций;

- для некоторых реализаций ПО метод динамической символьной интерпретации для AArch64 не эффективен по сравнению с аналогами из-за отсутствия оптимизации для обработки большого массива входных данных в цикле;
- метод динамической символьной интерпретации бинарного кода архитектуры RISC-V 64 не учитывает уже исследованные итерации при наличии больших циклов в коде и тратит больше времени на анализ.

Соискатель Логунова Влада Игоревна согласилась с замечаниями, ответила на задаваемые ей в ходе заседания вопросы.

На заседании 11 декабря 2025 г. диссертационный совет принял решение присудить Логуновой В. И. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 11 человек, из них 6 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 15 человек, входящих в состав совета, проголосовали: за – 11, против – 0, недействительных бюллетеней – 0.

Заместитель председателя диссертационного совета,
доктор физико-математических наук Белеванцев А. А.

Ученый секретарь диссертационного совета,
кандидат физико-математических наук Турдаков Д. Ю.

11 декабря 2025 г.