ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.087.01
на базе Федерального государственного бюджетного учреждения науки
Институт системного программирования им. В.П. Иванникова
Российской академии наук
Федерального агентства научных организаций РФ
по диссертации на соискание ученой степени кандидата наук

аттестационное дело № _____

решение диссертационного совета от 21 декабря 2017 года № 2017/27

О присуждении Федотову Андрею Николаевичу, гражданину РФ, ученой степени кандидата технических наук.

Диссертация «Разработка метода оценки эксплуатируемости программных дефектов» по специальности 05.13.11 – «математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей» принята к защите 19 октября 2017 г., протокол № 2017/21 диссертационным советом Д 002.087.01 на базе Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность – Федеральное агентство научных организаций), 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 Федотов Андрей Николаевич, 1991 года рождения, работает младшим научным сотрудником в отделе компиляторных технологий Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук, ФАНО.

В 2013 году соискатель окончил Федеральное государственное автономное образовательное учреждение высшего профессионального

образования "Национальный исследовательский ядерный университет МИФИ".

В 2016 году соискатель окончил аспирантуру Федеральное государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук.

Диссертация выполнена в отделе компиляторных технологий Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук, ФАНО.

Научный руководитель – кандидат физико-математических наук Падарян Вартан Андроникович, Федеральное государственное бюджетное учреждение науки Институт системного программирования им. В.П. Иванникова Российской академии наук, отдел «Компиляторных технологий», ведущий научный сотрудник.

Официальные оппоненты:

1. Ильин Вячеслав Анатольевич, доктор физико-математических наук, Национальный исследовательский центр «Курчатовский институт», отдел Курчатовского комплекса НБИКС-технологий Национального исследовательского центра «Курчатовский институт», начальник отдела,
2. Козачок Александр Васильевич, кандидат технических наук, ФГКВОУ ВО «Академия Федеральной службы охраны Российской Федерации», сотрудник,

дали положительные отзывы на диссертацию.

Ведущая организация Межведомственный суперкомпьютерный центр Российской академии наук – филиал Федерального государственного учреждения «Федеральный научный центр Научноисследовательский институт системных исследований Российской академии наук», г. Москва в своем положительном заключении, подписанным Шабановым Борисом

Михайловичем (кандидат технических наук, доцент, заместитель директора по научной работе ФГУ ФНЦ НИИСИ РАН, директор МСЦ РАН — филиала ФГУ ФНЦ НИИСИ РАН), указала, что диссертационная работа содержит новые научные результаты, имеющие существенное значение для науки и практики.

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.

Соискатель имеет 8 опубликованных работ, в том числе по теме диссертации 5 работ, из них 4 опубликованы в рецензируемых научных изданиях, в том числе 1 работа в журнале, индексируемом в WoS и Scopus.

В работах [1;3;5] представлен разработанный автором метод автоматической генерации эксплойтов. В статье [4] автором описаны улучшения метода автоматической генерации эксплойтов, позволяющие учитывать механизмы защиты от эксплуатации уязвимостей. В работе [2] представлен разработанный автором метод оценки эксплуатируемости программных дефектов.

1. Падарян В.А., Каушан В.В., Федотов А.Н. Автоматизированный метод построения эксплойтов для уязвимости переполнения буфера на стеке // Труды Института системного программирования РАН. — 2014. — Т. 26, № 3.
2. Федотов А.Н. Метод оценки эксплуатируемости программных дефектов // Труды Института системного программирования РАН. — 2016. — Т. 28, № 4.
3. Padaryan V.A., Kaushan V.V., Fedotov A.N. Automated exploit generation for stack buffer overflow vulnerabilities // Programming and Computer Software. — 2015. — Vol. 41, no. 6. — Pp. 373–380.
4. Оценка критичности программных дефектов в условиях работы современных защитных механизмов / А.Н. Федотов, В.А. Падарян,

В.В. Каушан и др. // Труды Института системного программирования РАН. — 2016. — Т. 28, № 5. — С. 73–92.

5. Каушан В.В., Федотов А.Н. Развитие технологии генерации эксплойтов на основе анализа бинарного кода // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». — 2015.

Диссертационный совет отмечает, что соискателем получены следующие новые научные результаты:

- На основе новейших технологий анализа исполняемого кода разработан метод оценки эксплуатируемости программных дефектов. Метод способен ранжировать обнаруженные сбои согласно тому, как они могут повлиять на надежность и безопасность программы. Из потока аварийных завершений исключаются ситуации, которые не могут быть использованы для исполнения произвольного кода известными методами вредоносного программного обеспечения, для остальных случаев автоматически строится эксплойт и проверяется его работоспособность. Характеристики представленного метода позволяют включать его в цикл разработки безопасного программного обеспечения.
- Впервые разработан метод автоматической генерации эксплойтов, позволяющий формировать эксплойты с учётом механизма защиты от трактовки данных как кода (DEP) и рандомизации адресного пространства процесса (ASLR). Данный аспект позволяет точней оценивать влияние анализируемого программного дефекта на надежность и безопасность ПО.

Отмечается, что разработанные методы были реализованы в виде соответствующих программных инструментов.

Полученные и представленные результаты отвечают специальности 05.13.11, поскольку относятся к областям исследований «Модели, методы и алгоритмы проектирования и анализа программ и программных систем, их эквивалентных преобразований, верификации и тестирования» и «Оценка качества, стандартизация и сопровождение программных систем».

Теоретическая значимость исследования состоит в том, что:

- разработаны алгоритмы построения предикатов безопасности, учитывающие работу защитных механизмов: рандомизации адресного пространства процесса (ASLR) и защиты от трактовки данных как кода (DEP).
- разработана классификация аварийных завершений, учитывающая влияние встроенных компилятором механизмов защиты от переполнений буферов.

Значение полученных соискателем результатов исследования для практики состоит в том, что на базе предложенных автором методов и алгоритмов разработан инструмент для оценки эксплуатируемости программных дефектов. Инструмент оценки эксплуатируемости программных дефектов предназначен для использования в цикле разработки безопасного программного обеспечения с целью обнаружения и ранжирования наиболее критичных дефектов.

Достоверность результатов исследования состоит в том, что:

- экспериментальные результаты для оценки эксплуатируемости программных дефектов получены на наборе аварийных завершений, который, в свою очередь, получен с помощью фаззинга;
- для аварийных завершений, полученных из открытых источников, разработанная система позволила получить эксплойты, работоспособные в условиях работы защитных механизмов DEP и ASLR.

Личный вклад соискателя состоит в разработке метода оценки эксплуатируемости программных дефектов, разработке метода автоматической генерации эксплойтов и метода предварительной фильтрации аварийных завершений, разработке алгоритмов построения предикатов безопасности, реализации инструмента для оценки эксплуатируемости программ.

На заседании 21 декабря 2017г. диссертационный совет принял решение присудить Федотову А.Н. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 16 человек, из них 6 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 20 человек, входящих в состав совета, проголосовали: за – 15, против – 0, недействительных бюллетеней – 1.

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

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

21 декабря 2017 года