ОТЗЫВ

на автореферат диссертации Израилова Константина Евгеньевича «Генетический реверс-инжиниринг для нейтрализации уязвимостей программного обеспечения», представленной к защите на соискание ученой степени доктора технических наук по специальностям 2.3.5. Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей и 2.3.6. Методы и системы защиты информации, информационная безопасность

Актуальность. Рост сложности программных систем затрудняет управление их безопасностью и повышает риски возникновения ошибок, что подтверждается ежегодно растущим количеством обнаруживаемых уязвимостей программного обеспечения. При этом не всегда существует возможность их выявления и устранения на этапе разработки. Например, программные компоненты, распространяемые в виде исполняемых модулей без доступа к исходному коду, могут содержать уязвимости, внедренные преднамеренно. Нейтрализация таких уязвимостей осложняется тем, что они могут внедряться в любом из промежуточных представлений, в которых оказывается программа в процессе создания, в то время как для их поиска зачастую имеется лишь исполняемый код. В работе для разрешения данного противоречия предложен новый подход генетической деэволюции представлений программы, который позволяет последовательно восстанавливать представления программы, повышая эффективность поиска и устранения уязвимостей в каждом из них, что делает саму работу актуальной, а полученные теоретические и практические результаты значимыми и востребованными в области обеспечения безопасности программных систем.

Теоретическая значимость положений, выносимых на защиту, состоит в обобщении и систематизации основных методов и средств реверс-инжиниринга программных систем в виде графоаналитической схемы, установлении двунаправленной эволюционной взаимосвязи представлений программы в рамках модели ее жизненного цикла, обосновании применения генетических алгоритмов для восстановления различных представлений программы в процессе ее реверс-инжиниринга, установлении статистических зависимостей между размерами исходного и соответствующего машинного кодов, определении вероятности появления констант в исходном коде, определении метрики близости двух ассемблерных кодов, а также в развитии сигнатурных способов поиска программных уязвимостей.

Практическая значимость работы определяется возможностью применения полученных в ней результатов для реверс-инжиниринга сложных разнородных программных систем, восстановления соседних промежуточных представлений программ без непосредственного участия эксперта, а также получения исходного кода по имеющемуся ассемблерному коду для поиска в нем уязвимостей как предложенным, так и существующими способами с

последующей нейтрализацией выявленных уязвимостей и получением безопасной версии программы. Востребованность полученных результатов подтверждается их использованием профильными подразделениями научно-исследовательских институтов, университетов и организаций.

Обоснованность и достоверность научных положений, выводов и рекомендаций, сформулированных в диссертации, подтверждается проведенным анализом современного состояния исследований в предметной области, корректным применением апробированных методов анализа и синтеза, непротиворечивостью полученных результатов, а также их широкой апробацией на представительных всероссийских и международных научных форумах и конференциях. Результаты исследования опубликованы автором в 48 статьях в рецензируемых научных изданиях, рекомендованных ВАК для публикации основных результатов диссертаций на соискание ученой степени доктора наук, 21 статье в журналах и сборниках трудов конференций, входящих в международную систему цитирования, 2 главах в коллективных монографиях и 29 работах в прочих изданиях. Получено 14 свидетельств о государственной регистрации программ для ЭВМ. Общее количество публикаций по теме диссертации – 114. Указанные публикации в достаточной степени отражают основные результаты, отмеченные в тексте автореферата.

По автореферату имеются следующие **замечания**:

1) Автор рассматривает процесс генетической деэволюции представлений программы как оптимизационную задачу максимизации целевой фитнес-функции. Не вполне понятно, учитываются ли локальные максимумы этой функции, соответствующие семантически эквивалентным представлениям программы, отличающимся лишь синтаксически и одинаково преобразуемым в последующие представления вследствие оптимизаций (минимизация логических функций, свертка циклов и т.п.).

2) В формулах (1)-(3) используется параметр V_0, обозначающий изначальное количество уязвимостей в программе, однако не раскрыто, как предполагается его оценивать.

3) На странице 26 указано, что после обнаружения и нейтрализации уязвимости «…требуется пересборка конечного представления программы, которое тем самым становится безопасным», однако неясно, учитывается ли при этом возможность непреднамеренного внесения новых уязвимостей или проявления существовавших ранее, но скрытых вследствие эффекта взаимного ослабления, о котором упомянуто на странице 22.

4) На рисунке 5 в компоненте поиска уязвимостей присутствует «Модуль статического фаззинга». Данное название не вполне понятно, поскольку фаззинг является методом динамического анализа, подразумевающим исполнение программы или ее фрагментов.

Указанные замечания не снижают научной ценности и не влияют на общую положительную оценку диссертационной работы.

Заключение

Насколько можно судить по автореферату, диссертационная работа Израилова К.Е. **является** завершенным научно-квалификационным трудом, содержащим решение актуальной научной проблемы, заключающейся в несоответствии уровня развития теории и технологий реверс-инжиниринга для нейтрализации уязвимостей программного обеспечения потребностям практики. Диссертационная работа **соответствует** требованиям пп. 9-14 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства РФ от 24 сентября 2013 г. N 842 «О прядке присуждения ученых степеней» (в действующей редакции), а ее автор, Израилов Константин Евгеньевич, **заслуживает** присуждения ученой степени доктора технических наук по специальностям 2.3.5. Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей и 2.3.6. Методы и системы защиты информации, информационная безопасность.

Я, Новиков Владимир Александрович, даю согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета, и их дальнейшую обработку.

Генеральный директор акционерного общества «Технологии радиоконтроля», доктор технических наук (20.02.27)

Новиков Владимир Александрович

«12» февраля 2026 г.

Акционерное общество «Технологии радиоконтроля»
Адрес: 195220, г. Санкт-Петербург, Пискаревский пр., 63Б
Телефон: +7(812)244-33-21
E-mail: info@ao-trk.ru

Подпись Генерального директора доктора технических наук Новикова Владимира Александровича заверяю.

Начальник отдела кадров

Шиканова Анна Валерьевна

«12» февраля 2026 г.