ОТЗЫВ
официального оппонента
кандидата технических наук **Диасамидзе Светланы Владимировны**
на диссертационную работу **Израилова Константина Евгеньевича**
на тему **«Метод алгоритмизации машинного кода для поиска уязвимостей в телекоммуникационных устройствах»**, представленную на соискание ученой степени кандидата технических наук по специальности
05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Актуальность темы диссертационной работы

Диссертационное исследование Израилова К.Е. посвящено вопросу выявления уязвимостей программного обеспечения в телекоммуникационных системах. Существующие методы и разработанные на их основе инструментальные средства поиска уязвимостей при отсутствии исходных текстов программ позволяют в автоматизированном и полуавтоматизированном режиме обнаруживать уязвимости, связанные с различного рода нарушением свойств программной структуры. Уязвимости же более высокого уровня, базирующиеся на нарушениях логики решения функциональных задач и реализации общей архитектуры телекоммуникационной системы, можно выявлять только вручную, на основе косвенных признаков, что требует больших временных затрат и участия в испытаниях экспертов высокой квалификации. При этом полнота и достоверность выявления уязвимостей достаточно невысока, так как без применения инструментальных средств, позволяющих локализовать и, хотя бы частично, распознать такого рода уязвимости, достичь необходимой эффективности практически невозможно.

Таким образом, задачи совершенствования процедур, методов и инструментальных средств поиска уязвимостей программного обеспечения для повышения уровня защищенности, в том числе, и телекоммуникационных систем, **являются актуальными** в области обеспечения информационной безопасности.

В диссертационной работе автор проводит типизацию уязвимостей программного кода и анализирует существующие способы поиска уязвимостей в машинном коде. На основании проведенного анализа разработан авторский метод алгоритмизации машинного кода, заключающийся в построении структурной модели машинного кода с уязвимостями в виде иерархии структурных метаданных и разноуровневых уязвимостей. В качестве практической реализации предложенного метода создано программное средство алгоритмизации машинного кода, позволяющее в автоматическом режиме формировать алгоритмизированное представление исследуемого машинного кода и, по результатам анализа обнаруженных потенциальных уязвимостей, вносить корректирующие изменения в программу для повышения защищенности рассматриваемого программного обеспечения. Автором проведено практическое исследование разработанных метода и программного средства на предмет оценки их эффективности для реализации процесса поиска уязвимостей, в виде комплекса методик и критериев оценки.

Научная новизна результатов работы

1. Предложен новый подход к нелинейному представлению машинного кода программы, включающему высокоуровневые иерархически-связанные структурные элементы кода.

2. Разработаны метод и программное средство алгоритмизации машинного кода, заключающийся в построении структурной модели машинного кода с уязвимостями в виде иерархии структурных метаданных и разноуровневых уязвимостей с возможностью последующей итерационной оптимизации построенной модели и генерации оптимизированного под человека представления программы.

3. Произведены оценка эффективности разработанного метода и сравнение с альтернативными способами поиска уязвимостей, для чего разработан оригинальный комплекс методик и критериев оценки алгоритмизации машинного кода и поиска уязвимостей.

Достоверность и степень обоснованности научных положений, выводов и рекомендаций

Результаты диссертационной работы соответствуют известным положениям, полученные научные выводы имеют строгое теоретическое обоснование. Достоверность основных полученных результатов обеспечивается корректностью постановки научно-технической задачи исследования, опорой на современную научную базу, корректным применением классических и современных методов исследования. Также подтверждением достоверности результатов исследования может служить обсуждение и одобрение их на различных научных форумах и конференциях и полученное автором свидетельство о государственной регистрации программы для ЭВМ.

Теоретическая и практическая значимость

Предложенный подход к представлению машинного кода программы в виде иерархии структурных метаданных и разноуровневых уязвимостей и разработанный на его основе метод алгоритмизации машинного кода позволяют расширить класс методов восстановления исходного кода программы за счет установления логического соответствия машинных команд и структурных метаданных программы.

Разработанные метод и программное средство алгоритмизации машинного кода целесообразно использовать в целях подтверждения соответствия программного обеспечения, в том числе, и являющегося составной частью телекоммуникационных систем. Данное программное средство может рассматриваться как одно из перспективных инструментальных средств поиска уязвимостей.

Разработанный комплекс научно-методических средств оценки алгоритмизации машинного кода для поиска уязвимостей позволяет осуществлять обоснованный выбор метода и средства, используемого для поиска уязвимостей в программном обеспечении телекоммуникационных систем в каждом конкретном случае.

Теоретическая и практическая значимость исследования подтверждается свидетельством о государственной регистрации программы для ЭВМ, двумя отчетами по выполненным научно-исследовательским работам и двух актов о внедрении результатов диссертации.

Полнота опубликованных результатов и соответствие паспорту специальности

По теме диссертации опубликована 31 печатная работа, в том числе 9 публикаций в изданиях, входящих в перечень рецензируемых научных изданий, рекомендованных ВАК Минобрнауки России, 5 публикаций в изданиях, входящих в международную систему цитирования Scopus, 7 публикаций в научных журналах, 9 публикаций в сборниках научных статей и сборниках трудов научных конференций. Получено свидетельство о государственной регистрации программы для ЭВМ. Основные результаты диссертационной работы обсуждались на различных научно-технических конференциях.

Работа выполнена в соответствии со следующими пунктами паспорта научной специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность:

– п. 3 «Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса»;

– п. 6 «Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования»;

– п. 10 «Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты».

Замечания по диссертации и автореферату

1. Представляется целесообразным привести в диссертации формальный синтаксис не только входного ассемблерного кода, но и полученного после обработки алгоритмизированного кода.

2. Имеется несоответствие между отображением входных данных для начального шага этапа 2 метода алгоритмизации машинного кода. Согласно таблице 2 автореферата и таблице 2.5 диссертации на вход подается машинный код, а в рисунке 3 автореферата, пункте 2.3.2 и рисунке 3.1 диссертации таковым является ассемблерное представление кода.

3. Исходя из схемы функциональной архитектуры программного средства алгоритмизации машинного кода (рисунок 3 автореферата) процессы уточнения сигнатуры подпрограмм и выделения структурных метаданных происходят последовательно, а не параллельно, как должно следовать из предлагаемой логики построения структурной модели машинного кода с уязвимостями.

4. В автореферате недостаточно четко описана система применяемых критериев для оценивания эффективности применения разработанного метода, хотя в диссертации этому вопросу уделено достаточно внимания.

Указанные замечания не меняют положительной оценки диссертации в целом и являются скорее рекомендацией для дальнейшей научной работы.

Заключение

Диссертация Израилова К.Е. является законченной научно-квалификационной работой, в которой решена задача актуальная в области обеспечения информационной безопасности, по разработке метода, позволяющего алгоритмизировать машинный код телекоммуникационных устройств в интересах последующего обнаружения в нем уязвимостей.

Диссертация и автореферат содержат все требуемые разделы, а также оформлены в соответствии с п. 24.1 «Положения о совете по защите диссертаций на соискание учёной степени кандидата наук, на соискание учёной степени доктора наук», утверждённого приказом Министерства образования и науки РФ

от 13.01.2014 № 7. Содержание автореферата соответствует основным положениям диссертационной работы.

Отмеченные недостатки носят частный характер и не снижают научной ценности и практической значимости проведенного исследования.

Диссертационная работа соответствует критериям, установленным п.п. 9–14 «Положения о присуждении учёных степеней», утверждённого Постановлением Правительства РФ от 24.09.2013 № 842, а ее автор, Израилов Константин Евгеньевич, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Официальный оппонент,
доцент кафедры «Информатика и информационная безопасность»,
кандидат технических наук

Диасамидзе Светлана Владимировна

Подпи
соналом
Егоров
2017 г.

Организация:
Федеральное государственное бюджетное образовательное учреждение высшего образования «Петербургский государственный университет путей сообщения Императора Александра I», www.pgups.ru
190031, Санкт-Петербург, Московский пр., д. 9
телефон: 8(812)310-34-72
эл. почта: sv.diass99@yandex.ru