

Отзыв
на автореферат диссертации Израилова К. Е.
«Метод алгоритмизации машинного кода для поиска уязвимостей в
телекоммуникационных устройствах»,
представленной на соискание ученой степени кандидата технических наук по
специальности 05.13.19 – «Методы и системы защиты информации, информационная
безопасность»

Актуальность темы диссертационной работы Израилова К. Е. определяется растущим противоречием между увеличивающимся количеством уязвимостей и ограниченным количеством экспертов в области анализа закрытых исходных кодов. Кроме того, основную угрозу безопасности составляют программные закладки, созданные сознательно, встроенные как часть алгоритмов или архитектуры работающей системы, и поэтому плохо формализуемые. В большинстве случаев они не обнаруживаются автоматическими средствами анализа машинного кода, ручной же анализ имеет высокую трудоемкость и требует привлечения высококлассных специалистов (хотя его упрощает применение утилит *декомпиляции*). Таким образом, удовлетворительных способов обнаружения уязвимостей такого типа (средне и высокоуровневых) на сегодняшний день не существует. Предлагаемое разрешение этого противоречия лежит в плоскости создания метода алгоритмизации машинного кода для последующего поиска уязвимостей, а именно: анализ машинного кода на предмет наличия информации об алгоритмах и архитектуре, синтез способа их восстановления в подходящую для специалиста форму, и оценка эффективности такой алгоритмизации.

Научная новизна работы состоит в том, что автором, в отличие от традиционных методов реверс-инжиниринга исходного кода, используется концептуально новый подход к его алгоритмизации с генерацией оригинального представления. В результате выполненного исследования автором решена научная задача, направленная на восстановление алгоритмов (объединенных в модули архитектуры) машинного кода телекоммуникационных устройств.

Практическая значимость исследования заключается в возможности использования разработанного метода алгоритмизации для восстановления архитектуры исходного кода в человеко-ориентированный вид при проведении сертификационных испытаний на отсутствие недекларированных возможностей.

Теоретическая ценность работы состоит в исследовании новых возможностей «обратного инжиниринга» программного кода.

Исходя из автореферата, диссертация содержит новые научные результаты, такие как:

- 1) структурная модель машинного кода с уязвимостями;
- 2) метод алгоритмизации машинного кода;
- 3) архитектура программного средства алгоритмизации машинного кода;
- 4) комплекс научно-методических средств оценки алгоритмизации машинного кода в интересах поиска уязвимостей.

Основные научные результаты опубликованы в 33 научных трудах (из них 9 – в рецензируемых изданиях из Перечня ВАК), что свидетельствует о личном вкладе автора диссертации в науку.

Тем не менее, анализ автореферата позволяет обратить внимание на ряд недостатков.

- 1) В цели работы заявлено повышение эффективности поиска уязвимостей, в задачах для достижения указанной цели – комплексная оценка эффективности алгоритмизации в интересах поиска. А в тексте автореферата приведена лишь ссылка на разработанные методики.
- 2) В автореферате не приведена в явном виде методика оценки эффективности поиска уязвимостей, а также отсутствуют результаты применения методики оценки эффективности поиска уязвимостей.
- 3) Результат проверки возможности применения разработанных методик приводится в автореферате в таблице 4 в виде баллов от -2 до +1, а смысл и способ начисления баллов для тестов не указан.

Указанные замечания носят дискуссионный характер и не снижают значимости работы.

Диссертация на тему «Метод алгоритмизации машинного кода для поиска уязвимостей в телекоммуникационных устройствах» соответствует паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» и требованиям Положения о присуждении ученых степеней, предъявляемым к кандидатским диссертациям. Ее автор, Израилов К. Е., заслуживает присвоения ученой степени кандидата технических наук.

Генеральный директор ЗАО «АСИС»
кандидат технических наук, доцент

Иванов Александр Владимирович



Закрытое акционерное общество
«Ассоциация специалистов информационных систем» (ЗАО «АСИСС»), www.spbissa
194100, Санкт-Петербург, ул. Кантемировская, д. 7
т/ф (812) 29-55-777, e-mail: info@spbissa