Экз. № 1

**ЗАКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «ИНСТИТУТ ТЕЛЕКОММУНИКАЦИЙ»**

ул. Кантемировская, д.5,
Санкт-Петербург, 194100
тел. (812) 740-77-07, факс 740-77-[redacted]
office@itain.spb.ru
ОКПО 59452298,
ОГРН 1027801538600

ИНН/КПП 7802199182/780201001

УТВЕРЖДАЮ
Генеральный директор
ЗАО «Институт телекоммуникаций»
заслуженный деятель науки РФ,
доктор технических наук, профессор

[redacted] С. П. Присяжнюк

«[redacted]» сентября 2017 г.

# ОТЗЫВ

на автореферат диссертации Израилова Константина Евгеньевича «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»

В настоящее время наличие недекларированных возможностей программного обеспечения сетевых устройств является серьезной угрозой информационной безопасности. Основное множество существующих способы поиска таких уязвимостей эффективно применяется для исходного кода, который, как правило, с телекоммуникационным оборудованием не поставляется. Анализ машинного кода автоматическими средствами позволяет обнаружить и нейтрализовать лишь случайные ошибки разработчиков и типовой код злоумышленника, что не подходит для более сложных ситуаций – внесение изменений в алгоритмы кода, логику взаимодействия его модулей, общую архитектуру, другие программные закладки. Применение труда эксперта для ручного поиска имеет крайне высокую трудоемкость, не удовлетворительную в современных условиях многообразия оборудования, частоты выпускаемых версий программного обеспечения, уникальности создаваемых уязвимостей. Вопросу создания условий для эффективного ручного поиска последних (отнесенных в автореферате к средне и высокоуровневым уязвимостям) и посвящена диссертационная работа Израилова К. Е. Автор исследует возможность восстановления из заведомо низкоуровневого представления машинного кода телекоммуникационных

устройств высокоуровневой информации об его исходном коде. При этом поиск уязвимостей по такому представлению призван быть более эффективным, чем альтернативные способы. Поэтому тема диссертации актуальна и соответствует современному уровню осмысления проблем безопасности и защиты информации в телекоммуникациях.

Из автореферата следует, что в ходе достижения цели исследования автором получены следующие научные результаты, выносимые на защиту:

1) Структурная модель машинного кода, отражающая в виде иерархии разноуровневые программные элементы исходного кода, а также связанные с ними уязвимости;

2) Метод алгоритмизации машинного кода, поэтапно (и с возможностью подстройки) преобразующий экземпляр машинного кода к его структурной модели, по которой воссоздается архитектура и алгоритмы кода;

3) Архитектура программного средства, описывающая с различных сторон средство алгоритмизации, применяемое для реализации метода;

4) Комплекс научно-методических средств оценки алгоритмизации машинного кода, входящие в состав которого критерии и методики позволяют оценить метод алгоритмизации с точки зрения поиска уязвимостей.

Полученные научные результаты имеют несомненную практическую ценность и теоретическую значимость. Их достоверность не вызывает сомнений и подкрепляется представительной апробацией и публикациями автора в рецензируемых изданиях. Также, положительные результаты тестирования программного средства (прототипа программы для алгоритмизации, являющегося основой метода и обеспечивающего работу с моделью) могут считаться обоснованием сделанных теоретических выводов и будущего практического применения научных результатов диссертации.

Необходимо особо отметить как общее количество публикаций (31 научный труд), так и их разнородность (рецензируемые научные издания из перечня ВАК и международной системы цитирования Scopus, статьи в научных журналах и сборниках, отчеты о НИР, свидетельство о государственной регистрации программы для ЭВМ), а также то, что почти половина всех работ написана Израиловым К.Е. лично. Все это характеризует автора как научного исследователя, обладающего достаточной степенью самостоятельности.

Новизна диссертационной работы определяется следующим:

1. Моделированием машинного кода, отличным от классического, путем выделения в нем информации о структуре кода (метаданных) и разноуровневых уязвимостях.

2. Построением процесса реверс-инжиниринга машинного кода вокруг модели, которая для этого создается, обрабатывается и приближается к требуемой эксперту, а затем используется для генерации результатов.

3. Созданием ориентированных на работу со структурной моделью функционального, информационного и программного архитектурных слоев, использующих авторские модули, структуры данных и алгоритмы; к последним, в частности, относятся: выделение аргументов и возвращаемых значений функций, восстановление структурных метаданных, оптимизация и лаконизация; также не маловажным является предложенный в качестве примера алгоритм обнаружения программной закладки с разрушением структуры кода.

4. Оригинальным набором методик и критериев оценки различных аспектов метода: входящей в его состав программного средства, получаемого описания архитектуры и алгоритмов, итогового поиска уязвимостей с применением метода, альтернативных способов поиска уязвимостей.

В качестве недостатков автореферата необходимо отметить:

- в автореферате на стр. 9 указано, что разработанный метод алгоритмизации МК исследовался с помощью специального ПС алгоритмизации. Однако как становится ясно из автореферата, специальное ПС алгоритмизации реализует разработанный метод. Таким образом получается, что метод исследовался программой, реализующей метод, что ставит под сомнение результаты исследования;

- в автореферате указано, что оценка эффективности проводилась с помощью методики, основанной на МАИ, однако, во-первых, отсутствует обоснование выбора именно этого метода, а во-вторых, непонятно, каким образом были выбраны конкретные значения приоритетов введенных критериев, и не окажется ли, что при других значениях разработанное ПС будет уступать известному программному продукту;

- в автореферате очень мало внимания уделено основному научному результату – методу алгоритмизации МК (1 страница), в то время как описание

разработанного программного средства составляет почти четверть автореферата (5 страниц).

Однако перечисленные замечания не снижают научной, теоретической и практической ценности работы и не изменяют общей положительной оценки полученных научных результатов.

ВЫВОДЫ:

В целом, судя по автореферату и публикациям автора, диссертационная работа выполнена на достаточном научно-техническим уровне и содержит решение новой научно-технической задачи. Содержание диссертации соответствует специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность». Несмотря на отмеченные недостатки, диссертационная работа как квалификационный труд по новизне, научному уровню и практической значимости отвечает требованиям «Положения о порядке присуждения ученых степеней», предъявляемым к кандидатским диссертациям, а ее автор, Израилов Константин Евгеньевич, заслуживает присуждения ученой степени кандидата технических наук.

Отзыв утвержден генеральным директором ЗАО «Институт телекоммуникаций», заслуженным деятелем науки РФ, доктором технических наук, профессором Присяжнюком Сергеем Прокофьевичем.

Отзыв составили:

Заместитель начальника НИО-1
канд. техн. наук, доцент Овчинников Георгий Ревмирович

Научный секретарь
канд. техн. наук Аванесов Михаил Юрьевич