ЗАКЛЮЧЕНИЕ ОБЪЕДИНЕННОГО ДИССЕРТАЦИОННОГО СОВЕТА Д 999.121.03 НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА» ФЕДЕРАЛЬНОГО АГЕНТСТВА СВЯЗИ, ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО АВТОНОМНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ» МИНИСТЕРСТВА ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ, ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «БАЛТИЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ «ВОЕНМЕХ» ИМ. Д.Ф. УСТИНОВА» МИНИСТЕРСТВА ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА ТЕХНИЧЕСКИХ НАУК

аттестационное дело № _____

решение диссертационного совета от 27 сентября 2017 г. № 5

О присуждении Израилову Константину Евгеньевичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Метод алгоритмизации машинного кода для поиска уязвимостей в телекоммуникационных устройствах» по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность. принята к защите 21 июня 2017 года, протокол № 4 объединенным диссертационным советом Д 999.121.03 на базе федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» Федерального агентства связи, федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» Министерства образования и науки Российской Федерации, федерального государственного бюджетного образовательного учреждения высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова» Министерства образования и науки Российской

Федерации, 191186, Санкт-Петербург, наб. реки Мойки, д. 61, приказ № 44/нк от 30 января 2017 года.

Соискатель Израилов Константин Евгеньевич, 1979 года рождения, работает ведущим специалистом в федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» Федерального агентства связи. В 2002 году соискатель окончил Санкт-Петербургский государственный технический университет. В 2015 году окончил освоение программы подготовки научно-педагогических кадров в аспирантуре федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича».

Диссертация выполнена на кафедре защищенных систем связи федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича».

Научный руководитель – доктор технических наук, профессор Буйневич Михаил Викторович, федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», кафедра безопасности информационных систем, профессор.

Официальные оппоненты: 1. Язов Юрий Константинович, доктор технических наук, профессор, Федеральное автономное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю», главный научный сотрудник управления; 2. Диасамидзе Светлана Владимировна, кандидат технических наук, Федеральное государственное бюджетное образовательное учреждение высшего образования «Петербургский государственный университет путей сообщения Императора Александра I», кафедра «Информатика и информационная безопасность», доцент, дали положительные отзывы на диссертацию.

Ведущая организация Акционерное общество «Научно-исследовательский институт программных средств», Санкт-Петербург, в своем положительном заключении, подписанном Езерским Владимиром Васильевичем, доктором технических наук, профессором, заместителем генерального директора по науке и развитию, Хахаевым Иваном Анатольевичем, кандидатом физико-математических наук, доцентом, руководителем центра компетенции СПО, утвержденном Гаценко О.Ю., доктором технических наук, профессором, генеральным директором, указали, что диссертация выполнена на высоком научном уровне и содержит новые, достоверные и значимые результаты, которые несомненно имеют значение для современного развития телекоммуникационных сетей и обеспечения их информационной безопасности, а также могут быть непосредственно использованы для защиты информации при ее обработке машинным кодом; личный вклад автора в получении результатов несомненен; все положения, выносимые на защиту, прошли широкую апробацию и опубликованы в достаточной степени в рецензируемых изданиях; диссертация является законченной научно-квалификационной работой, в которой содержится решение научной задачи по разработке метода и средства алгоритмизации машинного кода в интересах поиска среднеуровневых и высокоуровневых уязвимостей в программном обеспечении телекоммуникационных устройств, имеющей значение для развития отрасли информационной безопасности и защиты информации; диссертация соответствует п. 9 «Положения о присуждении ученых степеней», а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность..

Соискатель имеет 31 опубликованную работу, в том числе по теме диссертации 31 работу, опубликованных в рецензируемых научных изданиях 9. Диссертация не содержит недостоверных сведений об опубликованных соискателем ученой степени работах. Помимо 9 работ в рецензируемых научных изданиях, соискатель имеет 5 – в изданиях, входящих в международную систему цитирования Scopus; 1 – свидетельство о государственной регистрации программы для ЭВМ; 7 – статей в научных журналах; 9 – в сборниках научных статей, трудов, тезисов докладов и материалах конференций; 2 – отчета о НИР. Из

них 13 работ опубликовано соискателем без соавторства. Общий объем авторского вклада в работы (без свидетельства о государственной регистрации программы для ЭВМ) составляет 216 печ.л. из общего количества 596 печ. л.

Наиболее значительные научные работы по теме диссертации:

1) Израилов, К.Е. Метод алгоритмизации машинного кода телекоммуникационных устройств / М.В. Буйневич, К.Е. Израилов // Телекоммуникации. – 2012. – № 12. – С. 2-6.

2) Израилов, К.Е. Автоматизированное средство алгоритмизации машинного кода телекоммуникационных устройств / М.В. Буйневич, К.Е. Израилов // Телекоммуникации. – 2013. – № 6. – С. 2-9.

3) Израилов, К.Е. Укрупненная методика оценки эффективности автоматизированных средств, восстанавливающих исходный код в целях поиска уяз-вимостей / А.Ю. Васильева, К.Е. Израилов, А.И. Рамазанов // Вестник ИНЖЭКОНа. Серия: Технические науки. – 2013. – № 8(67). – С. 107-109.

4) Израилов, К.Е. Структурная модель машинного кода, специализированная для поиска уязвимостей в программном обеспечении автоматизирован-ных систем управления / М.В. Буйневич, К.Е. Израилов, О.В. Щербаков // Проблемы управления рисками в техносфере. – 2014. – № 3(31). – С. 68-74.

5) Израилов, К.Е. Методика оценки эффективности средств алгоритмизации, используемых для поиска уязвимостей / К.Е. Израилов // Информатизация и связь. – 2014. – № 3. – С. 39-42.

6) Израилов, К.Е. Архитектурные уязвимости моделей телекоммуникационных сетей [Электронный ресурс] / М.В. Буйневич, А.Г. Владыко, К.Е. Из-раилов, О.В. Щербаков // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2015. – № 4. – С. 86-93. – Режим доступа: http://vestnik.igps.ru/wp-content/uploads/V74/14.pdf.

7) Израилов, К.Е. Проблемные вопросы нейтрализации уязвимостей программного кода телекоммуникационных устройств / М.В. Буйневич, К.Е. Израилов, Д.И. Мостович, А.Ю. Ярошенко // Проблемы управления рисками в техносфере. – 2016. – № 3(39). – С. 81-89.

8) Израилов, К.Е. Система критериев оценки способов поиска уязвимостей и метрика понятности представления программного кода / К.Е. Израилов // Информатизация и связь. – 2017. – № 3. – С. 111-118.

9) Izrailov, K. Method and utility for recovering code algorithms of telecommunication devices for vulnerability search / M. Buinevich, K. Izrailov // 16th International Conference on Advanced Communication Technology (ICACT-2014). – 2014. – PP. 172-176.

10) Izrailov, K. The life cycle of vulnerabilities in the representations of software for telecommunication devices / M. Buinevich, K. Izrailov, A. Vladyko // 18th International Conference On Advanced Communications Technology (ICACT-2016). – 2016. – PP. 430-435.

11) Izrailov, K. Testing of Utilities for Finding Vulnerabilities in the Machine Code of Telecommunication Devices / M. Buinevich, K. Izrailov, A. Vladyko // 19th International Conference on Advanced Communication Technology (ICACT-2017). – 2017. – PP. 408-414.

12) Израилов, К.Е. Утилита восстановления алгоритмов работы машинного кода: свидетельство о государственной регистрации программы для ЭВМ / К.Е. Израилов. – рег. № 2013618433. – 09.09.2013.

На диссертацию и автореферат поступили отзывы: ведущей организации АО «Научно-исследовательский институт программных средств»; официального оппонента Язова Ю.К.; официального оппонента Диасамидзе С.В.; Белова В.М., д-ра техн. наук, проф., проф. кафедры безопасности и управления в телекоммуникациях Сибирского государственного университета телекоммуникаций и информатики; Синякова А.Р., канд. техн. наук, заместителя начальника отдела Ленинградского отделения Центрального научно-исследовательского института связи – филиала ФГУП ЦНИИС; Арустамова С.А., д-ра техн. наук, проф., проф. кафедры проектирования и безопасности компьютерных систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптик; Шаблюка С.М., канд. техн. наук, помощника главного конструктора, Филиппова С.В., канд. техн. наук, начальника научно-технического центра, утв. Доценко С.М., д-ром техн. наук, проф., первым заместителем генерального директора – главным

конструктором АО «Научно-производственное объединение «Импульс»; Овчинникова Г.Р., канд. техн. наук, доц., заместителя начальника НИО-1, Аванесова М.Ю., канд. техн. наук, научного секретаря, утв. Присяжнюком С.П., д-ром техн. наук, проф., генеральным директором ЗАО «Институт телекоммуникаций»; Солодянникова А.В., канд. техн. наук, доц., генерального диретора ЗАО«Ассоциация специалистов информационных систем»; Воробьева Е.Г., канд. техн. наук, доц., заведующего кафедрой "Информационная безопасность", утв. Гайворонским Д.В., канд. техн. наук, доц., и.о. проректора по научной работе Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина); Осипова В.Ю., д-ра техн. наук, проф., заведующего лабораторией информационно-вычислительных систем и технологий программирования Санкт-Петербургского института информатики и автоматизации Российской академии наук; Синещука Ю.И., д-ра техн. наук, проф., проф. кафедры специальных информационных технологий Санкт-Петербургского университета Министерства внутренних дел Российской Федерации. Все отзывы положительные, но имеют критические замечания:

1) Не достаточно полно сформулирована и раскрыта задача исследования в виде «разработки метода и средства алгоритмизации», отсутствуют существующие начальные и требуемые конечные условия выполнения, не приводятся в явном виде результаты оценки эффективности алгоритмизации и какая-либо методика последующего поиска уязвимостей, а также, не рассматривается методология формальной верификации программного обеспечения.

2) Изложение материала в автореферате является недостаточным, например, частные научные результаты изложены декларативно, не указаны особенности и специфика телекоммуникационных устройств, используются сравнительные таблицы с баллами без раскрытия способа их начисления, не обоснован выбор метода анализа иерархии и его критериев, отсутствует разъяснение терминов «метаданные», «инвариантность и блок машинного кода», не раскрывается связь уязвимостей с элементами структурной модели.

3) Оформление текста в ряде случаев является некорректным, например, недостаточно ясно сформулированы фразы («исследования метода на предмет

автоматизации специальным программным средством»), некоторые рисунки и схемы имеют лишние (стрелки на блок-схемах), ошибочные (машинный код вместо ассемблерного) или же не раскрытые (метаданные, УС) элементы, не соблюдается форматирование текста, а также иногда отсутствует нумерация списков.

4) Ряд основных научных результатов необходимо доработать, например, формализовать синтаксис входного ассемлерного и выходного алгоритмизированного представлений, расширить функционал средства алгоритмизации поддержкой смыслового декодирования, целесообразно произвести более полноценное тестирование метода и средства алгоритмизации, соотнести предложеные уязвимости с классами, установленными ГОСТ-ом, а также нет полноценного сравнения предлагаемого решения с существующими, как зарубежными, так и отечественными дизассемблерами и трансляторами.

Выбор официальных оппонентов и ведущей организации обосновывается тем, что в круг научных интересов вышеуказанных ученых (д-ра техн. наук, проф. Язова Ю.К., канд. техн. наук Диасамидзе С.В.) и ведущей организации (АО "НИИ ПС") входят темы, связанные с проблематикой представленной к защите диссертации, а также наличием значительного количества публикаций по тематике диссертации, что гарантирует их способность определить научную и практическую значимость работы.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований: разработаны новый подход к алгоритмизации машинного кода путем иттерационного моделирования его экземпляра, соответствующая ему схема и реализующий ее метод алгоритмизации, архитектура программного средства автоматизации метода, включающая форматы используемых данных, а также комплекс методических средств оценки алгоритмизации в интересах поиска уязвимостей; предложена модель машинного кода, построенная на базе структурных метаданных кода и связанных с ними разноуровневых уязвимостей; доказано повышение эффективности поиска уязвимостей в алгоритмах и архитектуре машинного кода при использовании предложенного метода алгоритмизации, а также его программного средства и генерируемого им представления; введены: типизация уязвимостей по их

структурному уровню в коде; понятие процесса алгоритмизации машинного кода, направленного на восстановление его алгоритмов и архитектуры; а также метаданные, описывающие структурные особенности кода.

Теоретическая значимость исследования обоснована тем, что: доказано наличие структурных метаданных в машинном коде в соответствии с используемыми парадигмами программирования, а также возможность восстановления структурных метаданных на основании их взаимосвязи с инструкциями в машинном коде; применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов) использованы сбор, систематизация и анализ научно-технической информации; системный, причинно-следственный и сравнительный анализ; функциональный и структурный синтез; методы бальной оценки и анализа иерархий; методология программирования, теория компиляции и графов, компьютерное моделирование; изложены способы представления программного обеспечения, их свойства и взаимосвязь, содержащиеся уязвимости и способы их поиска; шаги схемы алгоритмизации машинного кода, этапы соответствующего ей метода алгоритмизации, а также подходы, способы и средства для реализации последнего; раскрыто основное противоречие предметной области в виде роста количества и разнообразия уязвимостей при ограниченном количестве и возможностях экспертов информационной безопасности; а также описаны проблемные вопросы, решение которых позволит получить безопасный машинный код для телекоммуникационных устройств.; изучены аспекты алгоритмизации машинного кода, систематизация которых позволила произвести этапизацию метода алгоритмизации и выбрать подходы, способы и средства для их реализации; проведена модернизация классической линейной модели машинного кода путем добавления структурной составляющей в виде иерархии метаданных, а также внесением информации о потенциальных уязвимостях.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что: разработаны и внедрены структурная модель машиного кода с уязвимостями и метод алгоритмизации машинного кода для подготовки и проведения лекционно-практических занятий при обучении студентов на кафедре защищенных систем связи СПбГУТ; архитектура программного средства

алгоритмизации машинного кода и комплекс научно-методических средств оценки алгоритмизации машинного кода в интересах поиска уязвимостей при разработке архитектуры системного ПО (компиляторов C/C++ для встроенных систем) и в методическом обеспечении лаборатории тестированияв ООО «Астрософт»; определены перспективы практического использования: структурной модели – для формулированию требований к решению задач реверс-инжиниринга; метода алгоритимзации – для восстановления архитектуры и алгоритмов машинного кода в виде, подходящем для поиска уязвимостей; архитектуры средства алгоритмизации – для реализаци программных средств преобразования программ из низкоуровневого представления в высокоуровневое; комплекса научно-методичеких средств оценки – для осуществлении выбора среди средств и методов поиска уязвимостей в машинном коде; создана схема представлений программного обеспечения и областей жизни уязвимостей, определяющая начальные условия и конечные результаты применения метода алгоритмизации и последующего поиска уязвимостей; представлены перспективы развития метода алгоритмизации по направлениям: глубокий ручной поиск низкоуровневых уязвимостей, плановая проверка неизменности основного функционала программного кода, автоматизация поиска средне- и высокоуровневых уязвимостей, создание формата алгоритмизированного представления.

Оценка достоверности результатов исследования выявила: для экспериментальных работ результаты получены с помощью программного обеспечения и могут быть многократно воспроизведены для различных входных и промежуточных условий; теория построена на известных, проверяемых данных, согласуется с опубликованными данными по теме диссертации, а также подтверждается экспериментальным применением метода и практическими результатами работы разработанного программного средства алгоритмизации (имеющего свидетельство о государственной регистрации программы для ЭВМ.); идея базируется на анализе и обобщении подходов к обеспечению безопасности программного обеспечения, учете специфики телекоммуникационных устройств, передовой практике поиска уязвимостей в машинном коде; использованы имеющийся у автора обширный опыт работы с телекоммуникационным

оборудованием, ручного анализа и реверс-инжиниринга низкоуровневого представления кода, разработки программных средств преобразований представлений; сравнение авторских результатов с полученным другими авторами по тематики диссертационной работы; установлено качественное совпадение авторских результатов в виде получаемых алгоритмизированного представления экземпляров машинного кода с результатами независимых источников, полученных с помощью альтерантивных средств реверс-инжиниринга и ручным восстановлением машинного кода; использованы современные математические инструменты проведения оценок и осуществлению выбора в условиях сложных проблем принятия решений.

Личный вклад соискателя состоит в: критическом рассмотрении существующих способов обеспечения безопасности программного кода телекоммуникационных устройств; постановке цели и задачи исследования; проведении анализа машинного кода и парадигм программирования на предмет наличия в них общих метаданных; создании схемы метода восстановления алгоритмов и архитектуры машинного кода с последующей этапизацией; разработке архитектуры способа автоматизации метода и реализации соответствующего программного средства с доведением последнего до работоспособного прототипа; проведении объемного количества тестов метода и программного средства; создании целого комплекса методик, метрик и критериев оценки алгоритмизации, а также проведении соответствующих измерений; публикации основных и частных научных результатов (лично и в соавторстве); апробации полученных результатов на конференциях и при личном общении с близкими по тематике работы экспертами информационной безопасности, внедрение и реализация всех основных научных результатов.

Диссертационный совет пришёл к выводу о том, что диссертация представляет собой научно-квалификационную работу, в которой содержится решение научной задачи, имеющей значение для развития знаний в области защиты информации, и соответствует критериям, установленным Положением о присуждении ученых степеней (утв. Постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842).

На заседании 27 сентября 2017 года диссертационный совет принял решение присудить Израилову К.Е. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 19 человек, из них 7 докторов наук (отдельно по каждой специальности рассматриваемой диссертации), участвовавших в заседании, из 25 человек, входящих в состав совета, проголосовали: за – 18, против – нет, недействительных бюллетеней – 1.

Заместитель председателя диссертационного совета,
доктор технических наук, профессор

Крук Евгений Аврамович

Ученый секретарь диссертационного совета,
кандидат технических наук

Владыко Андрей Геннадьевич

29 сентября 2017 года