На правах рукописи

Израилов Константин Евгеньевич

МЕТОД АЛГОРИТМИЗАЦИИ МАШИННОГО КОДА ДЛЯ ПОИСКА УЯЗВИМОСТЕЙ В ТЕЛЕКОММУНИКАЦИОННЫХ УСТРОЙСТВАХ

05.13.19 – Методы и системы защиты информации,
информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2017

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ).

Научный руководитель: доктор технических наук, профессор,
Буйневич Михаил Викторович

Официальные оппоненты: **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

Диасамидзе Светлана Владимировна,
кандидат технических наук,
федеральное государственное бюджетное
образовательное учреждение высшего образования
«Петербургский государственный университет путей
сообщения Императора Александра I»,
доцент кафедры «Информатика и информационная
безопасность»

Ведущая организация: Акционерное общество «Научно-исследовательский институт программных средств», Санкт-Петербург

Защита состоится 27 сентября 2017 года в 14.00 на заседании объединенного диссертационного совета Д 999.121.03 при федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения», федеральном государственном бюджетном образовательном учреждении высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова» по адресу: Санкт-Петербург, пр. Большевиков, д. 22, корп. 1, ауд. 554/1.

С диссертацией можно ознакомиться в библиотеке СПбГУТ по адресу Санкт-Петербург, пр. Большевиков, д. 22, корп. 1 и на сайте www.sut.ru.

Автореферат разослан 11 августа 2017 года.

Ученый секретарь
диссертационного совета Д 999.121.03,
канд. техн. наук А.Г. Владыко

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Безопасность современных телекоммуникационных систем определяется, в том числе, уязвимостями в программном обеспечении (далее – ПО) входящих в их состав телекоммуникационных устройств (далее – ТКУ). Согласно открытым базам (таким, как NVD, CVE, OSVDB и др.) ежегодно наблюдается рост обнаруживаемых уязвимостей. При этом сфера применяемых в России ТКУ является на 90% «импортозависимой», вынуждая использовать заведомо небезопасное ПО зарубежного производства.

Существующее же множество способов поиска уязвимостей в исходном коде ПО в данном случае не подходит, поскольку преобладающее количество ТКУ поставляется с машинным кодом (далее – МК), способы поиска по которому существенно ограничены и в разы более трудоемки. При этом их целью, в основном, являются достаточно формализуемые низкоуровневые уязвимости – ошибки в реализации вычислений и доступе к данным. Средне- и высокоуровневые уязвимости – ошибки в логике работы алгоритмов и общей архитектуре, обнаруживаемые по субъективным признакам и с привлечением экспертов информационной безопасности, на сегодня не имеют развитых способов поиска.

Таким образом, основное противоречие рассматриваемой предметной области заключается в росте количества и разнообразия средне- и высокоуровневых уязвимостей при ограниченном количестве и возможностях экспертов информационной безопасности. Одной из существенных причин, порождающих указанное противоречие, является низкая производительность работы экспертов, обусловленная использованием для поиска средне- и высокоуровневых уязвимостей представлений кода, продуцируемых традиционными средствами реверс-инжиниринга.

В этих условиях требуется принципиально новый вид представления МК, специализированный для поиска средне- и высокоуровневых уязвимостей – так называемое алгоритмизированное представление. Это предполагает разработку соответствующего метода алгоритмизации и реализующего его средства, что и обуславливает актуальность темы настоящего исследования.

Степень разработанности темы. Методологические вопросы информационной безопасности телекоммуникационных систем, задавшие предпосылки к исследованию, рассматривались крупными Российскими учеными, такими как М.В. Буйневич, Б.С. Гольдштейн, О.В. Казарин, В.И. Коржик, И.В. Котенко, А.Е. Кучерявый, Е.А. Крук, Н.А. Соколов, Р.М. Юсупов, Ю.К. Язов, В.А. Яковлев и др. Безопасность ПО, используемого и в ТКУ, а также непосредственный поиск в нем уязвимостей были рассмотрены в работах А.П. Баранова, М.А. Еремеева, Д.П. Зегжды, П.Д. Зегжды, В.П. Иванникова, А.А. Корниенко, А.Г. Ломако, В.Ю. Осипова, В.Г. Шведа и др. Возможностями реверс-инжиниринга, примененными в интересах алгоритмизации, занимались такие ученые, как А.И. Аветисян, В.А. Падарян, Е.Н. Трошина, А.В. Чернов, C. Cifuentes и др. Существующие представления программного кода, а также подходы к созданию альтернативных, использованные в интересах метода

алгоритмизации, были получены на основании работ С.В. Диасамидзе, А.С. Маркова, Ф.А. Новикова, С.В. Полякова, Д.А. Эделя, B. Shneiderman и др.

Несмотря на достаточное освещение указанных областей, тем не менее, проблемные вопросы алгоритмизации МК в интересах поиска средне- и высокоуровневых уязвимостей оставлены практически без внимания.

Цель и задачи. Целью работы является повышение эффективности поиска уязвимостей в МК ТКУ путем его алгоритмизации.

Для достижения цели исследования в работе были поставлены и решены следующие задачи:

1) Проанализировать способы нейтрализации уязвимостей в программном коде;

2) Идентифицировать метаданные в МК, соответствующие парадигмам разработки программного кода для ТКУ;

3) Исследовать модели МК с позиции структурных метаданных;

4) Построить гипотетическую схему алгоритмизации МК на базе его модели;

5) Синтезировать метод, реализующий схему алгоритмизации;

6) Разработать архитектуру программного средства (далее – ПС) автоматизации метода алгоритмизации;

7) Реализовать прототип ПС алгоритмизации и произвести его базовое тестирование;

8) Сформировать критерии и создать методики для оценки свойств алгоритмизации МК;

9) Произвести комплексную оценку эффективности алгоритмизации в интересах поиска уязвимостей;

10) Предложить перспективы применения и развития метода алгоритмизации.

Объект исследования – машинный код с уязвимостями.

Предмет исследования – восстановление алгоритмов работы программного кода.

Научная (научно-техническая) задача – разработка метода и средства алгоритмизации машинного кода в интересах поиска средне- и высокоуровневых уязвимостей в программном обеспечении телекоммуникационных устройств.

Научная новизна. Научная новизна работы определяется новой предметной областью и новизной полученных результатов и состоит в том, что:

– предложено представление МК, отличное от классического (линейного) наличием иерархически-связанных структурных элементов – структурных метаданных и разноуровневых уязвимостей;

– в отличие от традиционных методов реверс-инжиниринга МК, используется концептуально новый подход к алгоритмизации путем моделирования МК с последующей итерационной оптимизацией модели и генерацией оригинального представления;

– впервые разработана архитектура ПС реверс-инжиниринга МК, ориентированная на создание и обработку его модели, а также использующая оригинальные модули выделения сигнатур подпрограмм, оптимизации и лаконизации внутреннего представления, поиска среднеуровневых уязвимостей;

– создан оригинальный комплекс методик и критериев оценки алгоритмизации МК и ручного поиска средне- и высокоуровневых уязвимостей.

Теоретическая и практическая значимость работы. Теоретическая значимость научных положений, изложенных в работе, состоит в следующем:

– установлено соответствие между инструкциями МК и его структурными метаданными;

– расширен класс методов для восстановления исходного кода программ в части их алгоритмов;

– разработаны классы объектов и процедур для моделирования низкоуровневого представления программы;

– сформированы критерии понятности представления и алгоритмизированности МК.

Практическая значимость результатов проведенных исследований состоит в следующем:

– структурная модель позволяет формулировать научно-обоснованные требования к решению задач, связанных с восстановлением архитектуры и алгоритмов МК, а также с поиском его уязвимостей;

– метод алгоритмизации может быть использован для восстановления архитектуры и алгоритмов МК в человеко-ориентированный вид, подходящий для поиска средне- и высокоуровневых уязвимостей;

– архитектура предоставляет возможность реализации ПС для инвариантного преобразования низкоуровневого представления программ в высокоуровневое;

– методики оценки применимы для обоснованного выбора среди методов и средств, используемых для поиска уязвимостей в МК ТКУ.

Часть основных научных результатов используется в учебном процессе на кафедре защищенных систем связи СПбГУТ при подготовке и проведении лекционно-практических занятий для направления 10.00.00 – «Информационная безопасность» по учебным дисциплинам «Ассемблер в задачах защиты информации», «Вредоносное программное обеспечение» и «Реверс-инжиниринг системного программного обеспечения». Другая часть реализована в ООО «Астрософт» при разработке архитектуры системного ПО и в методическом обеспечении лаборатории тестирования.

Методология и методы исследования. Для решения поставленных задач использовались как классические, так и современные методы исследования, а именно:

– системный, причинно-следственный и сравнительный анализ был применен в равной степени для получения практически всех основных научных результатов;

– сбор, систематизация и анализ научно-технической информации предметной области позволили создать структурную модель МК с уязвимостями;

– функциональный и структурный синтез использовался для создания метода алгоритмизации;

– с помощью методов бальной оценки и анализа иерархий был создан комплекс научно-методических средств, позволяющий оценивать эффективность алгоритмизации МК.

Помимо общей методологии программирования, основой архитектуры ПС алгоритмизации послужили теории компиляции и графов; также использовалось компьютерное моделирование для поддержки в нем структурной модели.

Положения, выносимые на защиту. Соискателем лично получены следующие основные научные результаты, выносимые на защиту:

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.

Степень достоверности. Достоверность основных полученных результатов обеспечивается корректностью постановки научно-технической задачи исследования, строго обоснованной совокупностью ограничений и допущений, представительным библиографическим материалом, опорой на современную научную базу, корректным применением апробированных классических и современных методов исследования; и подтверждается непротиворечивостью полученных результатов практики восстановления программного кода и поиска в нем уязвимостей, широкой апробацией результатов на представительных научных форумах, а также получением свидетельства о государственной регистрации программы для ЭВМ.

Апробация результатов. Основные научные положения и результаты диссертации докладывались, обсуждались и получили одобрение на Пятом научном конгрессе студентов и аспирантов «ИНЖЭКОН-2012» (Санкт-Петербург, 2012), Всероссийской научно-методической конференции «Фундаментальные исследования и инновации в национальных исследовательских университетах» (Санкт-Петербург, 2012), научно-практической конференции «Информационные технологии и непрерывность бизнеса» (Санкт-Петербург, 2012), X Международной научно-технической конференции «Новые информационные технологии и системы (Пенза, 2012), Международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (Санкт-Петербург, 2013, 2016), Шестом научном конгрессе студентов и аспирантов «ИНЖЭКОН-2013» Санкт-Петербург, 2013), Международной научно-технической конференции «Фундаментальные и прикладные исследования в современном мире» (Санкт-Петербург, 2013), Международной конференции «Передовые коммуникационные технологии, ICACT» (Ю. Корея, 2014–2017), XIV Санкт-Петербургской Международной конференции «Региональная информатика» (Санкт-Петербург, 2014), IX Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России» (Санкт-Петербург, 2015).

Публикации. Основные результаты диссертационного исследования опубликованы в 31-ом научном труде, из них: 9 – в рецензируемых научных изданиях из Перечня ВАК; 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 – отчеты о НИР.

Структура и объем работы. Диссертационная работа состоит из введения, основной части (содержащей 4 раздела), заключения, списка литературы и приложений. Общий объем работы − 261 страница, из них основного текста – 185 страниц. Работа содержит 69 рисунков и 26 таблиц. Список литературы включает 175 источников.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

В первом разделе в качестве объекта исследовалось представление МК с уязвимостями на предмет содержащихся в нем структурных метаданных, под которыми понимаются архитектура, модули, подпрограммы и алгоритмы (с управляющими структурами – последовательностями, ветвлениями и циклами) программного кода.

Рассмотрены проблемные вопросы обеспечения безопасности программного кода ТКУ и выбран наиболее перспективный из них для решения – поиск уязвимостей в исполняемом коде.

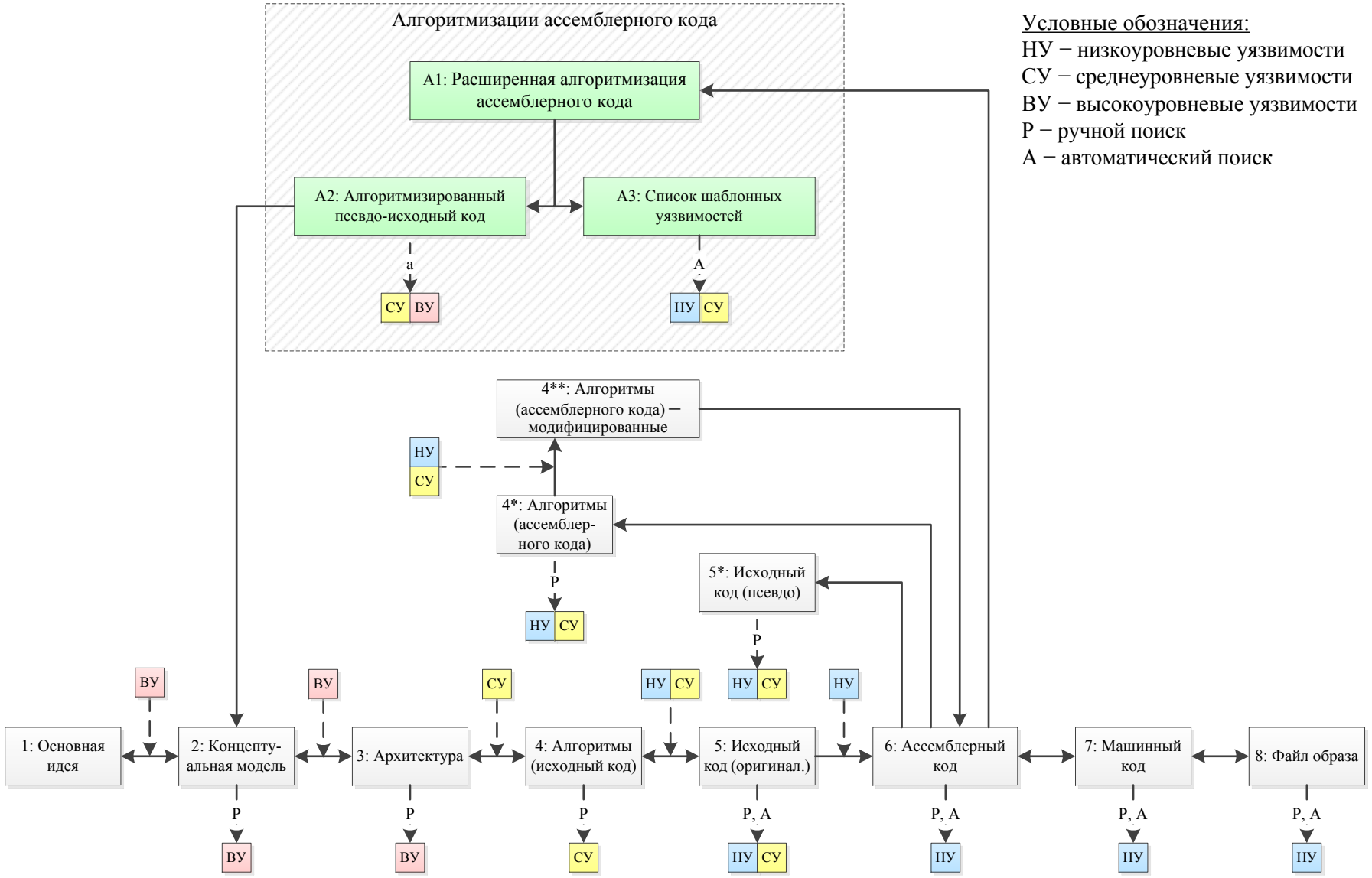
Произведена типизация уязвимостей программного кода по их структурному уровню. Рассмотрены известные способы поиска уязвимостей в МК и произведено критериальное сравнение их эффективности (таблица 1).

Таблица 1 – Критериальная оценка известных способов поиска уязвимостей в МК

Критерий	**Способы**				
	1. СР	**2. СРД**	**3. АШ**	**4. ДВ**	**5. ФТ**
1. Поиск среднеуровневых уязвимостей	+/–	+/–	–	+/–	–
2. Поиск высокоуровневых уязвимостей	–	–	–	–	–
3. Автоматизация	–	+	+	+/–	+
4. Достоверность результатов	+	+	+/–	+/–	–
5. Инвариантность представления МК	–	+	+/–	+/–	+
6. Обработка больших объемов кода	–	+/–	+	–	–
7. Возможность адаптации процесса	+/–	–	–	+/–	–
8. Минимизация излишней информации	–	+/–	+	+/–	+
9. Дополнительная информация об уязвимостях	–	–	+/–	–	+/–
10. Не высокая сложность применения	–	+/–	+/–	–	+
Сумма баллов	2	5	5	3	4.5

Примечание. Использованы следующие обозначения способов поиска уязвимостей в МК: СР – статический ручной, СРД – статический ручной с декомпиляцией, АШ – автоматический по шаблонам, ДВ – динамическое выполнение, ФТ – фаззинг тестирование.

Синтезирована схема областей жизни уязвимостей в представлениях ПО, на основании которой выделено направление для решения выбранного проблемного вопроса (рисунок 1).



Условные обозначения:
НУ – низкоуровневые уязвимости
СУ – среднеуровневые уязвимости
ВУ – высокоуровневые уязвимости
P – ручной поиск
A – автоматический поиск

Рисунок 1 – Схема областей жизни уязвимостей в представлениях ПО

Идентифицированы структурные метаданные в МК согласно используемым парадигмам программирования. Установлено, что применение модульной парадигмы приводит к наличию в МК информации о модулях программного кода и их взаимосвязи (т. е. архитектуре), процедурной – подпрограммах и их взаимодействия, структурной – алгоритмах и управляющих структурах, императивной – взаимосвязи метаданных через переменные.

Выявлена низкоуровневая информация в МК, которая может быть использована для идентификации структурных метаданных, а именно: в коде выполнения – переходы на адреса для подпрограмм, вычисления для параметров управляющих структур, безусловные/условные переходы и циклы для управляющих структур, вызовы подпрограмм для сигнатуры подпрограмм, модулей и архитектуры программного кода; в коде данных – глобальные переменные для связи алгоритмов подпрограмм через «разделяемые» данные.

Сформулированы требования к модели МК, применимой для его алгоритмизации и последующего поиска уязвимостей. Так, во-первых, заданы отражение и взаимосвязь основных элементов модели: блоков МК, структурных метаданных, дополнительной информации об уязвимостях. Во-вторых, определены общенаучные требования к модели: адекватность, анализируемость, универсальность и целесообразность. И, в-третьих, обоснована необходимость наличия у модели внешних интерфейсов для управления и обмена информацией.

Описана классическая линейная модель МК, подразумеваемая «de-facto» (L-модель) и обоснована ее неприменимость в интересах алгоритмизации.

Задан вектор из 3-х структурных моделей: общая, адаптированная (рисунок 2) и частная, уточняющих каждую из предыдущих и позволяющих осуществлять на их базе алгоритмизацию МК.

Предложен концептуальный подход к алгоритмизации МК, основанный на его S-моделировании с последующим проведением эксперимента для получения алгоритмизированного представления. Сформулированы требования к реализации предложенного подхода.

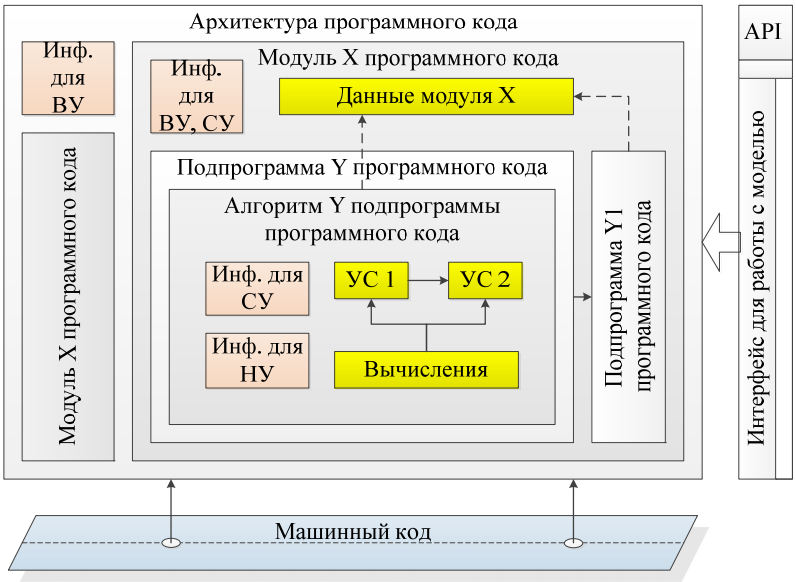


Рисунок 2 – Схема адаптированной S-модели МК

Основным научным результатом, изложенным в первом разделе, является структурная модель МК с уязвимостями (S-модель), суть которой заключается в его представлении в виде иерархии структурных метаданных и разноуровневых уязвимостей. Также, модель содержит специальную информацию, используемую для поиска уязвимостей различных типов: низкоуровневых, среднеуровневых и высокоуровневых.

Частными научными результатами, изложенными в первом разделе, являются: критерии эффективности известных способов поиска уязвимостей, структурная типизация уязвимостей программного кода, схема областей жизни уязвимостей в представлениях ПО, линейная L-модель и промежуточные S-модели МК. Первый результат непосредственно был использован для установления условия достижения цели исследования, а последние – для получения основного научного результата.

Основное содержание раздела и полученных научных результатов изложено в работах автора [2, 5, 7-8, 12, 16, 21, 23-27, 29-31].

Во втором разделе в качестве объекта исследовалась структурная модель МК на предмет создания его алгоритмизированного представления в форме, подходящей для анализа специалистом.

С использованием предложенного концептуального подхода построена гипотетическая схема алгоритмизации МК, которая состоит из 13-ти шагов и имеет итеративное выполнение. Особенностью схемы является ее инвариантность к последующей реализации метода.

Описаны общие принципы поддержки S-модели на основании особенностей и условий ее применения в гипотетической схеме алгоритмизации.

Показана работоспособность S-модели на гипотетическом примере ее построения и преобразования.

Произведена этапизация метода алгоритмизации путем группирования шагов ее схемы в следующие 5 этапов (таблица 2).

Таблица 2 – Соответствие шагов гипотетической схемы реализациям этапов метода алгоритмизации МК

Шаги	Этап
1. Распаковка МК	1. Получение ассемблерного представления
2. Подготовка МК	
3. Разбор МК и корректировок к нему	2. Алгоритмизация ассемблерного представления
4. Сбор структурных метаданных	
5. Сбор информации об уязвимостях	
6. Построение частной S-модели	
7. Анализ S-модели	
8. Синтез алгоритмизированного представления	
9. Генерация алгоритмизированного представления	
10. Анализ алгоритмизированного представления	3. Анализ алгоритмизированного представления АК
11. Проверка S-модели. Удовлетворительна?	
12. Создание корректировок для моделирования	4. Корректировка алгоритмизации АК
13. Гармонизация алгоритмизированного представления	5. Гармонизация алгоритмизированного представления АК

Определены средства, необходимые для реализации этапов метода, а именно: автоматическая обработка МК интерактивным дизассемблером IDA Pro и ассемблерного кода (далее – АК) специальным ПС алгоритмизации, а также ручной анализ алгоритмизированного представления экспертом.

Заданы требования к новому ПС алгоритмизации и 3-х фазный процесс его работы: построение внутреннего представления, обработка внутреннего представления и создание текстового описания архитектуры и алгоритмов.

Основным научным результатом, изложенным во втором разделе, является метод алгоритмизации МК, суть которого заключается в моделировании экземпляра МК и построении его алгоритмизированного представления.

Частными научными результатами, изложенными во втором разделе, являются критерии и результаты сравнительной оценки существующих способов и подходов к поиску уязвимостей с точки зрения их применимости для метода алгоритмизации. Эти результаты непосредственно были использованы для составления требований к реализации ПС алгоритмизации.

Основное содержание раздела и полученных научных результатов изложено в работах автора [1, 10, 11, 13, 17, 28].

В третьем разделе в качестве объекта исследовался метод алгоритмизации МК на предмет автоматизации процесса его выполнения с помощью специального ПС алгоритмизации (далее – Утилиты).

Разработана функциональная архитектура Утилиты, состоящая из следующих элементов: последовательно-выполняемые фазы с их делением на стадии, модули и их взаимодействия, а также входные, выходные и определяющие S-модель внутренние данные (рисунок 3).

Для каждой стадии описаны модули архитектуры со следующим назначением: лексический, синтаксический и семантический анализатор на стадии 1; выделение подпрограмм, построение графа потока управления и выделение глобальных переменных на стадии 2; построение графа потока данных, уточнение сигнатур подпрограмм и выделение структурных метаданных на стадии 3; оптимизация структурных метаданных, дерева потока управления и вычислений на стадии 4; генерация псевдокода глобальных переменных и подпрограмм, лаконизация псевдокода, генерация псевдокода архитектуры на стадии 5; генерация текстового описания корректировок, архитектуры, глобальных переменных, подпрограмм и информации об уязвимостях на стадии 6.

Задан базовый сценарий функционирования Утилиты и ее глобальные настройки в виде флагов, влияющих на отладочный вывод, комментирование алгоритмов, параметры лаконизации алгоритмизированного представления и компактности его вывода, генерацию вспомогательной низкоуровневой информации.

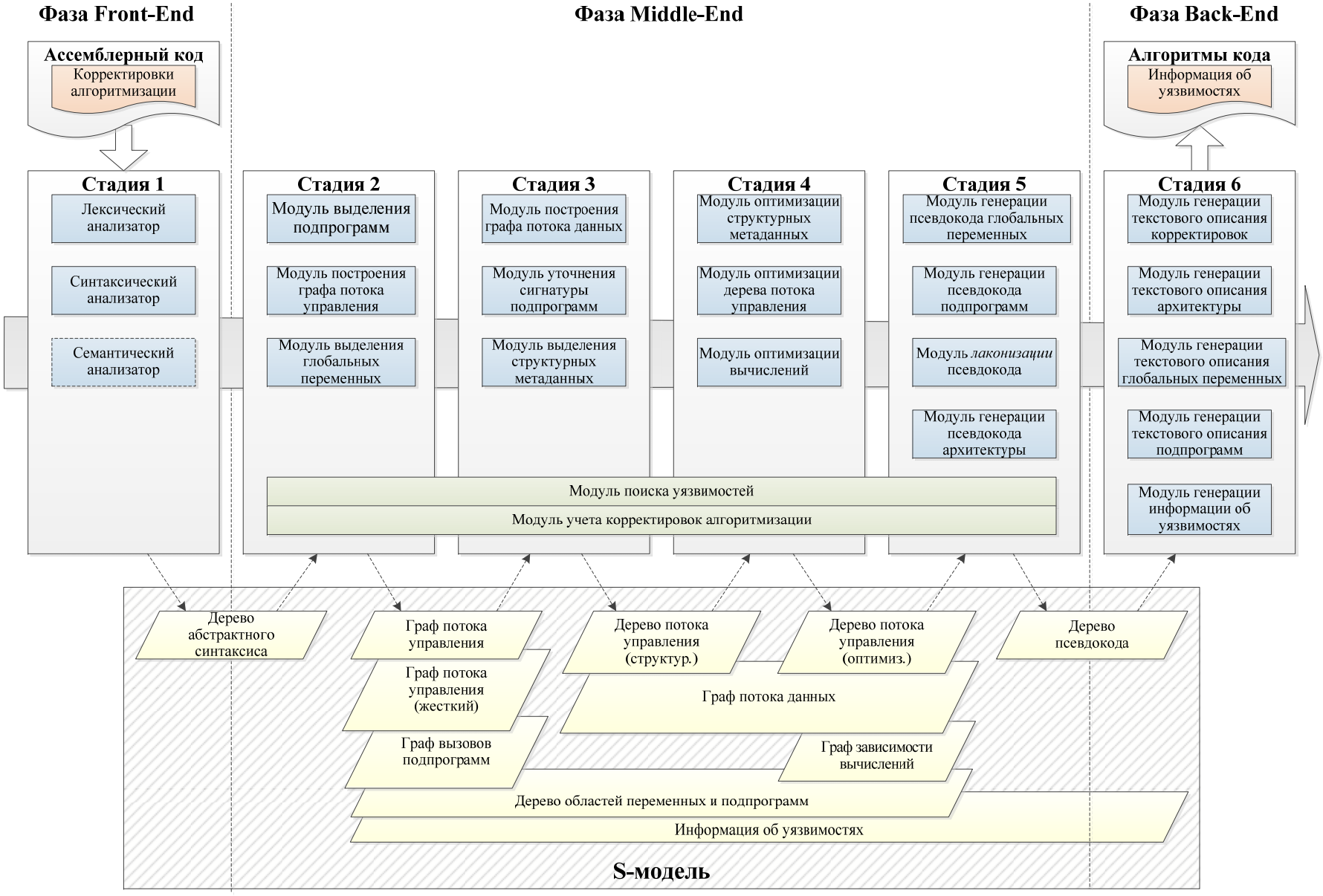


Рисунок 3 – Функциональная архитектура Утилиты

Разработана информационная архитектура Утилиты, задающая организацию и формализацию ее внутренних данных (рисунок 4). Описаны синтаксисы входного АК и выходного текстового описания алгоритмов, а также формализованные внутренние данные, используемые Утилитой.

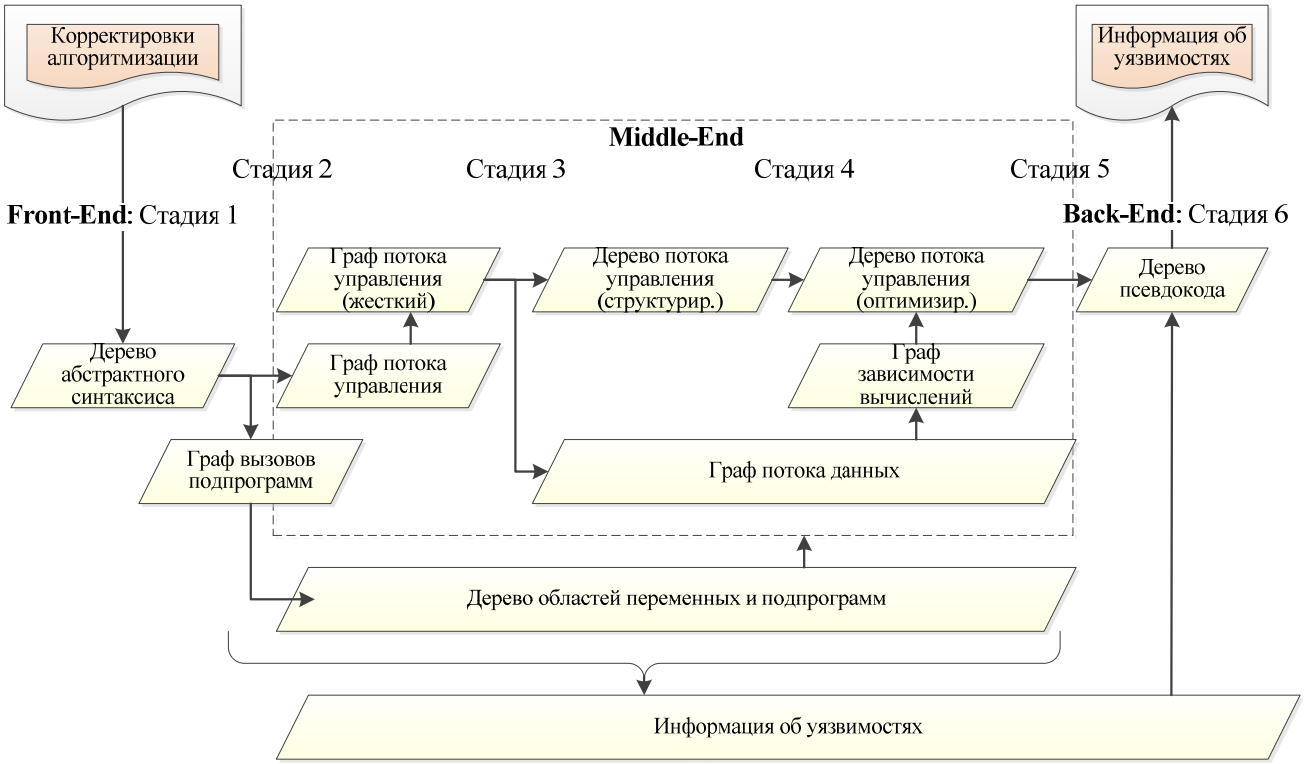
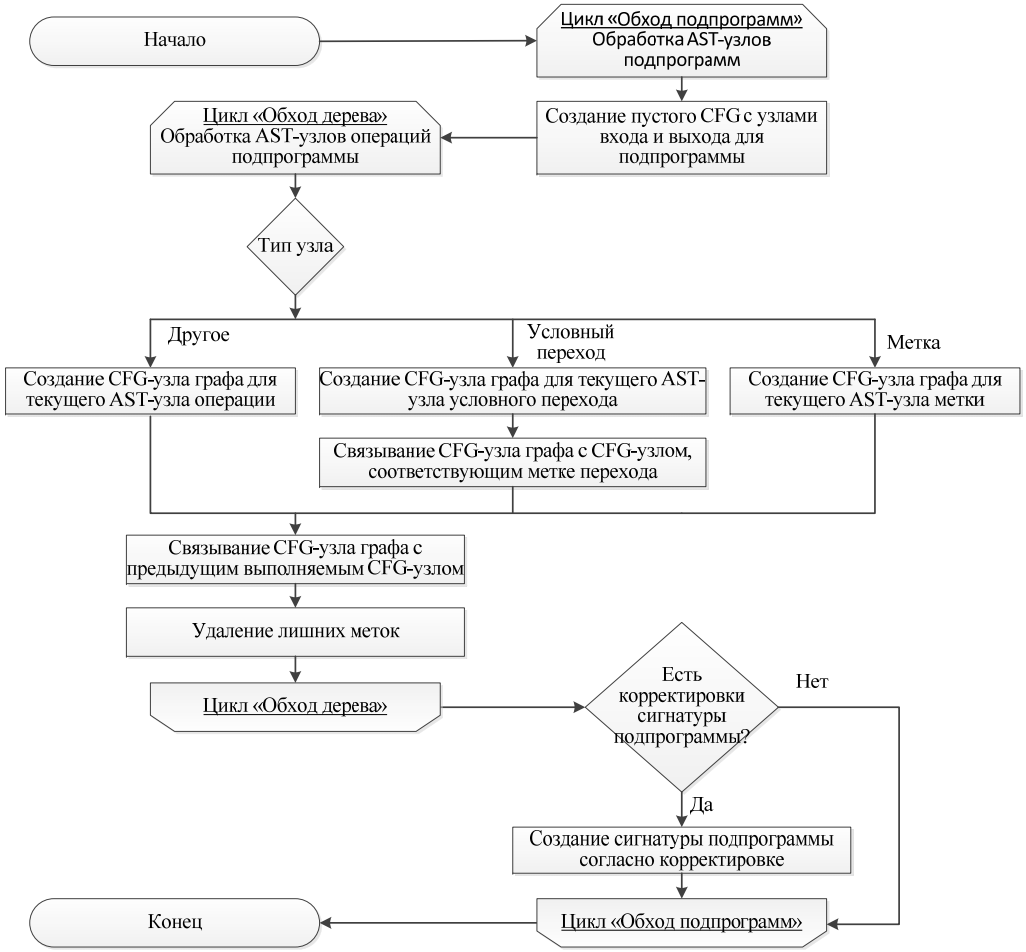


Рисунок 4 – Информационная архитектура Утилиты

Разработана программная архитектура Утилиты, описывающая алгоритмы ее основных модулей. Описана технология программной реализации его прототипа в виде строения исходного кода, а также использованных средств разработки и отладки. Примеры блок-схем алгоритмов модулей различных стадий представлены на рисунках 5 и 6.

Произведено практическое применение прототипа Утилиты на базовых примерах АК функций: нахождения максимального их трех чисел, алгоритма определения старшего бита числа и проверки пароля с внедренной закладкой. В таблице 3 показана работа прототипа для первого примера. Обозначено состояние разработки Утилиты и перспективы ее развития.

Модуль построения графа потока управления



Модуль выделения структурных метаданных

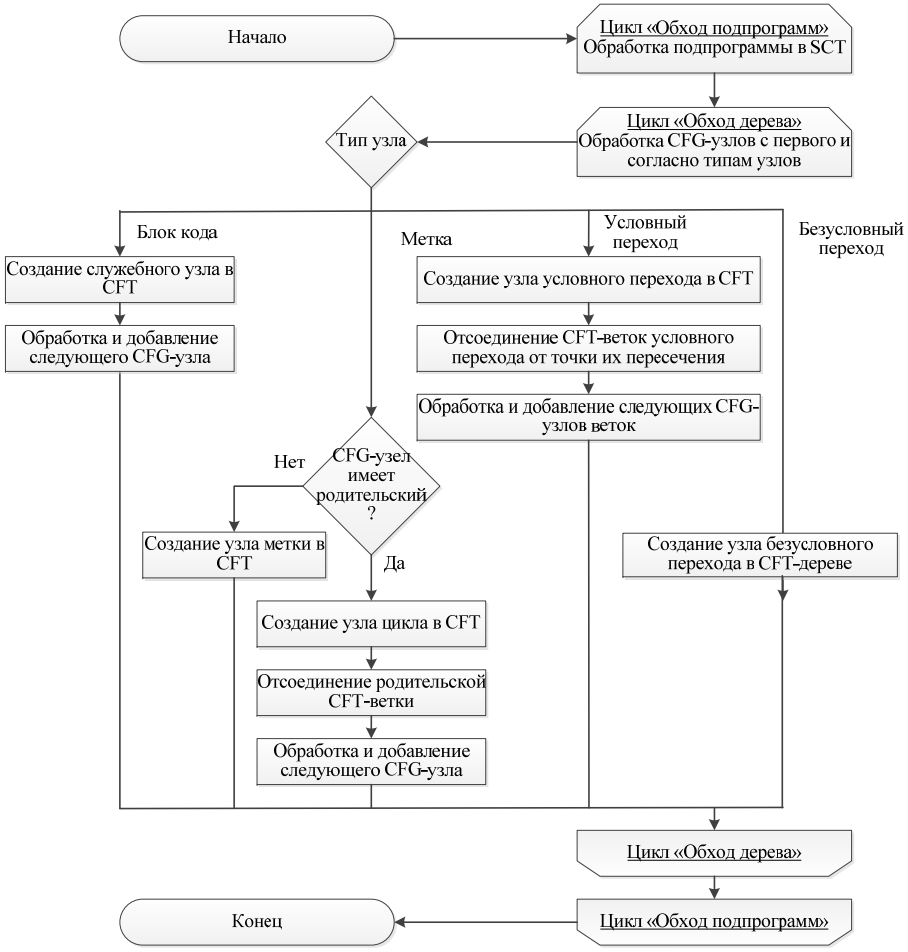
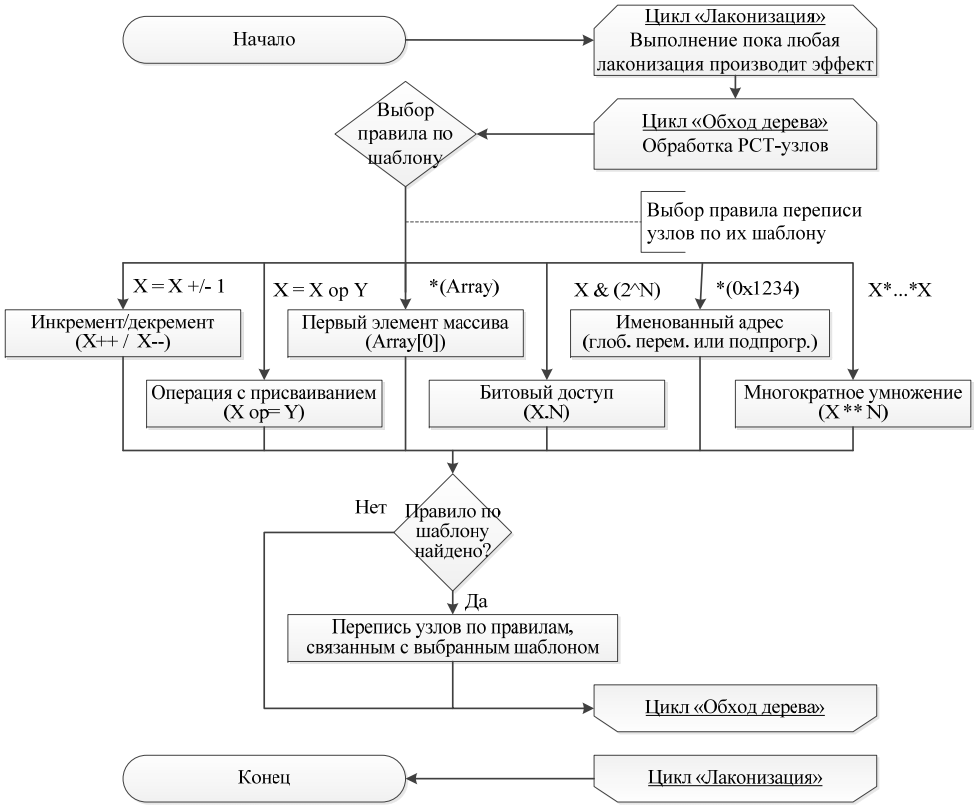


Рисунок 5 – Примеры блок-схем алгоритмов модулей стадий 2 и 3

Модуль лаконизации псевдокода



Модуль генерации текстового описания подпрограмм

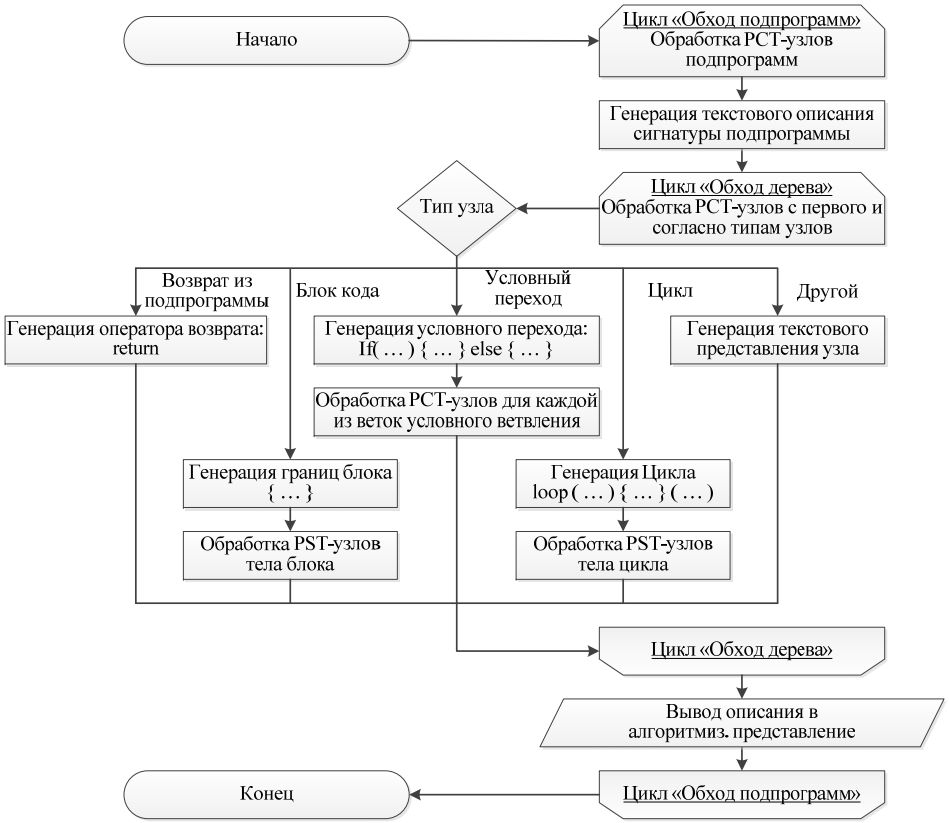


Рисунок 6 – Примеры блок-схем алгоритмов модулей стадий 5 и 6

Таблица 3 – Пример работы прототипа Утилиты для функции максимального из 3-х чисел

Исходный код (C)	**Ассемблерный код (PowerPC)**	**Алгоритмизированный код**

`int max3(int x, int y, int z) {`
`  int m, n;`
`  if (x > y) {`
`  m = x;`
`  } else {`
`  m = y;`
`  }`
`  if (m > z) {`
`  n = m;`
`  } else {`
`  n = z;`
`  }`
`  return n;`
`}`
	`max3(){ // {x(r3), y(r4), z(r5), m(r6), n(r7)`
	`  0x00000001:  max3:`
	`  0x00000002:  cmpw r3, r4  //  if (x > y)`
	`  0x00000003:  ble label_1  //  {`
	`  0x00000004:  mr r6, r3  //  m = x;`
	`  0x00000005:  b label_2  //  }`
	`  0x00000006:  label_1:  //  else {`
	`  0x00000007:  mr r6, r4  //  m = y;`
	`  0x00000008:  label_2:  //  }`
	`  0x00000009:  cmpw r6, r5  //  if(m > z)`
	`  0x0000000A:  ble label_3  //  {`
	`  0x0000000B:  mr r7, r6  //  n = m;`
	`  0x0000000C:  b label_4  //  }`
	`  0x0000000D:  label_3:  //  else {`
	`  0x0000000E:  mr r7, r5  //  n = z;`
	`  0x0000000F:  label_4:  //  }`
	`  0x00000010:  mr r3, r7  //  return n;`
	`  0x00000011:  blr  // }`
	`}`
		`(r3) max3(x, y, z) {`
		`  if (x <= y) {`
		`  x = y;`
		`  }`
		`  if (x <= z) {`
		`  x = z;`
		`  }`
		`  return (x);`
		`}`

Основным научным результатом, изложенным в третьем разделе, является архитектура ПС алгоритмизации МК, суть которой заключается в пофазном и помодульном описании средства с позиции взаимоувязанных функциональной, информационной и программной составляющих.

Частным научным результатом, изложенными в третьем разделе, является базовое тестирование разработанного прототипа Утилиты. Этот результат непосредственно был использован для подтверждения успешности выбранного способа автоматизации метода.

Основное содержание раздела и полученных научных результатов изложено в работах автора [3, 10, 13, 15, 18-20, 22].

В четвертом разделе в качестве объекта исследовались метод и ПС алгоритмизации МК на предмет целевой оценки их эффективности для осуществления поиска уязвимостей.

Описан целевой способ поиска уязвимостей в МК, состоящий из применения автоматизированного метода алгоритмизации с последующим ручным анализом полученного представления. Сравнение этого способа поиска с альтернативными по критериям из таблицы 1 представлено на рисунке 7 (МА – способ с применением алгоритмизации).

Разносторонняя оценка метода была произведена по объектам целевого способа, а именно: средству алгоритмизации (Утилите и ее прототипу), получаемому представлению и последующему поиску уязвимостей.

Для оценки потребительских свойств Утилиты разработана методика, основанная на методе анализа иерархий; в качестве альтернативы обоснованно выбран продукт IDA Pro с плагином декомпиляции Hex-Rays (далее – IDA+Hex-Rays).

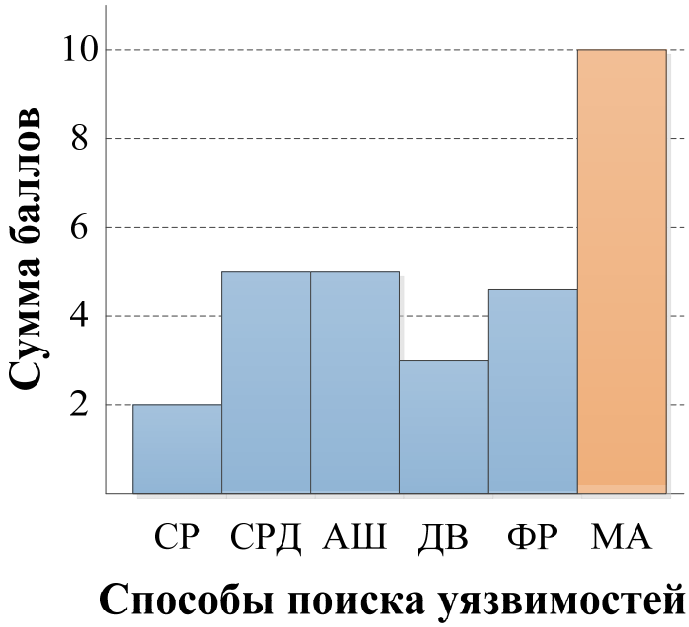


Рисунок 7 – Гистограмма сравнения целевого способа поиска уязвимостей и альтернативных

Значения приоритетов введенных критериев (в количестве N = 10) были определены следующим образом: скорость работы – 0.032, трудоемкость – 0.111, представление алгоритма – 0.164, информация об уязвимостях – 0.155, поддерживаемые процессоры – 0.04151, применимость для различных типов уязвимостей – 0.15, актуальность средства – 0.076, достоверность результатов – 0.164, экономическая целесообразность – 0.075, распространенность – 0.031. Главное собственное значение матрицы сравнений критериев равно:

$$\lambda_{max} = \sum_{n=1}^{N}\left(\sum_{m=1}^{N} a_{nm}\right) \times b_n = 11.46,$$

а индекс согласованности равен:

$$\mu = \frac{\lambda_{max} - N}{N - 1} = 0.16219.$$

В этом случае отношение согласованностей (при случайном индексе 1.49) равно:

$$\gamma = \frac{\mu}{1.49} = 0.10885,$$

что является допустимым и подтверждает корректность заполнения матрицы. Значение глобального приоритета для Утилиты равно 0.584, что превосходит 0.416 для IDA Pro.

Таким образом, применение разработанной методики показало преимущество предложенного ПС по сравнению с ближайшим аналогом.

Для оценки функциональности средств алгоритмизации МК в интересах поиска уязвимостей разработана методика, использующая экспертно-бальный метод (рисунок 8).

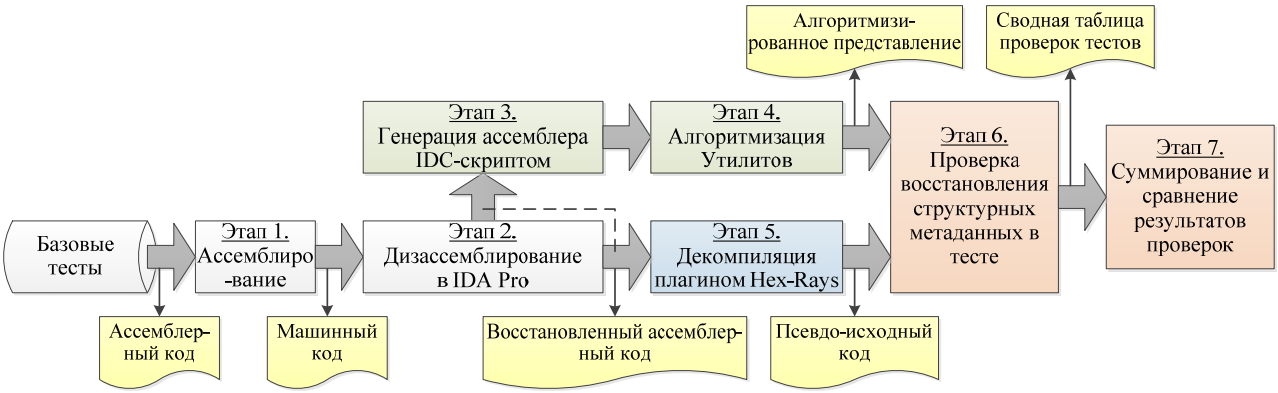


Рисунок 8 – Методика оценки функциональности ПС алгоритмизации

Применение разработанной методики для базы тестов показало преимущество прототипа Утилиты по сравнению с ближайшим аналогом – IDA+Hex-Rays (таблица 4).

Таблица 4 – Результаты проверок тестов для прототипа Утилиты и IDA+Hex-Rays

ПС\Тесты	**№ 1**	**№ 2**	**№ 3**	**№ 4**	**№ 5**	**№ 6**	**№ 7**	**№ 8**	**№ 9**	**Итог**
Утилита	-1	-1	+1	0	0	0	-1	+1	0	-1
IDA+Hex-Rays	0	0	0	-1	-1	-1	-2	0	-2	-7

Выбрана и обоснована система критериев алгоритмизированности МК, состоящая из объективных (количество ошибок, корректно выделенные структурные метаданные и вызовов подпрограмм, операторы безусловного перехода, используемые переменные, лишние или сложные конструкции, обнаруженные уязвимости, дублируемая информация, а также циклическая сложность) и субъективных (уровень абстракции и плотность описания алгоритмов) параметров.

Создана метрика понятности представления программного кода, связанная с этапами его осмысления и их критериями понятности. Расчет метрик для алгоритмизированного представления МК и получаемого с помощью IDA+Hex-Rays показал объективное преимущество первого.

Разработана методика оценки эффективности поиска уязвимостей с использованием алгоритмизации МК.

Основным научным результатом, изложенным в четвертом разделе, является комплекс научно-методических средств оценки алгоритмизации МК в интересах поиска уязвимостей, суть которого заключается в раздельной оценке объектов целевого способа поиска уязвимостей: средства алгоритмизации, получаемого представления МК и его последующего ручного анализа.

Частным научным результатом, изложенным в четвертом разделе, является база тестов для комплексной проверки эффектов алгоритмизации. Этот результат непосредственно был использован в методике оценки функциональности средства алгоритмизации.

Основное содержание раздела и полученных научных результатов изложено в работах автора [4, 6, 9, 14].

ЗАКЛЮЧЕНИЕ

В работе исследовался МК с уязвимостями на предмет восстановления алгоритмов его работы. В соответствии с целевой установкой и поставленными задачами были получены основные научные результаты, выносимые на защиту, а именно:

1) Структурная модель МК с уязвимостями;
2) Метод алгоритмизации МК;
3) Архитектура программного средства алгоритмизации МК;
4) Комплекс научно-методических средств оценки алгоритмизации МК в интересах поиска уязвимостей.

Совокупность полученных научных результатов свидетельствует о достижении поставленной цели исследования – повышении эффективности поиска средне- и высокоуровневых уязвимостей в МК ТКУ путем его алгоритмизации.

Перспективность метода алгоритмизации МК заключается не только в его текущем применении, но и в теоретико-практической значимости новых потенциальных результатов. Таким образом, исследования могут быть продолжены по следующим направлениям: во-первых, разработка интерактивной среды для визуализации АК и его структурных метаданных; во-вторых, создание механизма сравнения логики работы МК на основании его алгоритмизированного представления для проведения плановой проверки неизменности основного функционала кода; в-третьих, автоматизированный поиск средне- и высокоуровневых уязвимостей в МК; в-четвертых, разработка концепции и формата алгоритмизированного представления для максимально эффективного его понимания экспертом.

Выполнение перспективных исследований по перечисленным направлениям позволит повысить общую безопасность ПО ТКУ по количественным показателям, таким как число найденных разноуровневых уязвимостей, время поиска, степень покрытия кода и др.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых научных изданиях

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. Модель прогнозирования угроз телекоммуникационной системы на базе искусственной нейронной сети / К.Е. Израилов // Вестник ИНЖЭКОНа. Серия: Технические науки. – 2012. – № 8(59). – С. 150-153.

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

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

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

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

7. Израилов, К.Е. Архитектурные уязвимости моделей телекоммуникационных сетей [Электронный ресурс] / М.В. Буйневич, А.Г. Владыко, К.Е. Израилов, 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.

8. 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.

9. 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.

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

В изданиях, входящих в международную систему цитирования Scopus

11. 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.

12. Izrailov, K. Method for partial recovering source code of telecommunication devices for vulnerability search / M. Buinevich, K. Izrailov, A. Vladyko // 17th International Conference on Advanced Communications Technology (ICACT-2015). – 2015. – PP. 76-80.

13. 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.

14. Izrailov, K. Method and prototype of utility for partial recovering source code for low-level and medium-level vulnerability search / M. Buinevich, K. Izrailov, A. Vladyko // 18th International Conference on Advanced Communication Technology (ICACT-2016). – 2016. – PP. 700-707.

15. 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.

В других изданиях

16. Израилов, К.Е. Анализ состояния в области безопасности программного обеспечения / К.Е. Израилов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2013): сборник научных статей II Международной научно-технической и научно-методической конференции. – 2013. – С. 874-877.

17. Израилов, К.Е. Сравнительный анализ подходов к поиску уязвимостей в программном коде / М.В. Буйневич, К.Е. Израилов, Д.И. Мостович // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2016): сборник научных статей V Международной научно-технической и научно-методической конференции. – 2016. – С. 256-260.

18. Израилов, К.Е. Расширение языка «С» для описания алгоритмов кода телекоммуникационных устройств [Электронный ресурс] / К.Е. Израилов // Информационные технологии и телекоммуникации. – 2013. – № 2(2). – С. 21-31. – Режим доступа: http://www.sut.ru/doci/nauka/review/2-13.pdf.

19. Израилов, К.Е. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 1. Функциональная архитектура [Электронный ресурс] / М.В. Буйневич, К.Е. Израилов // Информационные технологии и телекоммуникации. – 2016. – Т. 4. – № 1. – С. 115-130. – Режим доступа: http://sut.ru/doci/nauka/review/20161/115-130.pdf.

20. Израилов, К.Е. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 2. Информационная архитектура [Электронный ресурс] / К.Е. Израилов // Информационные технологии и телекоммуникации. – 2016. – Т. 4. – № 2. – С. 86-104. – Режим доступа: http://sut.ru/doci/nauka/review/20162/86-104.pdf.

21. Израилов, К.Е. Категориальный синтез и технологический анализ вариантов безопасного импортозамещения программного обеспечения телекоммуникационных устройств [Электронный ресурс] / М.В. Буйневич, К.Е. Израилов // Информационные технологии и телекоммуникации. – 2016. – Т. 4. – № 3. – С. 95-106. – Режим доступа: http://sut.ru/doci/nauka/review/20163/95-106.pdf.

22. Израилов, К.Е. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 3. Модульно-алгоритмическая архитектура [Электронный ресурс] / К.Е. Израилов // Информационные технологии и телекоммуникации. – 2016. – Т. 4. – № 4. – С. 104-121. – Режим доступа: http://www.sut.ru/doci/nauka/review/20164/104-121.pdf.

23. Израилов, К.Е. Архитектурные уязвимости программного обеспечения / К.Е. Израилов // Шестой научный конгресс студентов и аспирантов СПбГИЭУ (ИНЖЭКОН-2013): сборник тезисов докладов научно-практической конференции факультета

информационных систем в экономике и управлении «Инфокоммуникационные технологии и математические методы». – 2013. – С. 35.

24. Израилов, К.Е. Алгоритмизация машинного кода телекоммуникационных устройств как стратегическое средство обеспечения информационной безопасности / К.Е. Израилов // Национальная безопасность и стратегическое планирование. – 2013. – № 2(2). – С. 28-36.

25. Израилов, К.Е. Рассмотрение представлений кода программ с позиций метаданных / К.Е. Израилов // Фундаментальные исследования и инновации в национальных исследовательских университетах: материалы Всероссийской научно-методической конференции. – 2012. – Т. 5. – С. 176-180.

26. Израилов, К.Е. Модель машинного кода, специализированная для поиска уязвимостей / М.В. Буйневич, К.Е. Израилов, О.В. Щербаков // Вестник Воронежского института ГПС МЧС России. – 2014. – № 2 (11). – С. 46-51.

27. Израилов, К.Е. Язык описания модели безопасности телекоммуникационной сети / А.Ю. Васильева, К.Е. Израилов // Новые информационные технологии и системы (НИТИС-2012): сборник трудов X Международной научно-технической конференции. – 2012. – С. 272-275.

28. Израилов, К.Е. Метод и программное средство восстановления алгоритмов машинного кода телекоммуникационных устройств для поиска уязвимостей / К.Е. Израилов // Региональная информатика (РИ-2014): материалы XIV Санкт-Петербургской международной конференции. – 2014. – С. 140-141.

29. Израилов, К.Е. Поиск уязвимостей в различных представлениях машинного кода / К.Е. Израилов // Информационная безопасность регионов России (ИБРР-2015): материалы IX Санкт-Петербургской межрегиональной конференции. – 2015. – С. 157.

30. Израилов, К.Е. Исследование и моделирование угроз безопасности цифровой телекоммуникационной сети: отчет о НИР шифр «Цифровая угроза-2012» / М.В. Буйневич, К.Е. Израилов и др. – СПбГУТ, 2012. – рег. № 047-12-054. – 219 с.

31. Израилов, К.Е. Разработка предложений по организационно-техническому обеспечению устойчивости функционирования сетей связи, защиты сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации, методов проверки и определение перечня нарушений целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации: отчет о НИР / М.В. Буйневич, А.Г. Владыко, К.Е. Израилов и др. – СПбГУТ, 2012. – рег. № 034-12-054. – 177 с.

Подписано в печать 21.06.2017. Формат 60x84 1/16.
Печ. л. 1,0. Тираж 60 экз.

Отпечатано в СПбГУТ, 193232, Санкт-Петербург, пр. Большевиков, д. 22, корп. 1