На правах рукописи

Лавров Андрей Александрович

Метод и алгоритмы мониторинга вычислительных сетей на основе совместного анализа временных и функциональных характеристик стека протоколов TCP/IP

05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2013

Работа выполнена в *Санкт-Петербургском государственном Электротехническом университете «ЛЭТИ» им В.И. Ульянова (Ленина) (СПбГЭТУ) на кафедре «Математического обеспечения и применения ЭВМ»*.

Научный руководитель:	*доктор технических наук, профессор, Лисс Александр Рудольфович*
Официальные оппоненты:	*доктор технических наук, профессор кафедры моделирования электромеханических и компьютерных систем Санкт-Петербургского государственного университета, Карпов Андрей Геннадьевич*
	кандидат технических наук, руководитель отдела Верификации и Идентификации Диктора ООО «Центр речевых технологий», Симончик Константин Константинович
Ведущая организация:	*Санкт-Петербургский институт информатики и автоматизации Российской академии наук*

Защита состоится «27» ноября 2013 г. в 15 часов 30 минут на заседании совета по защите докторских и кандидатских диссертаций Д212.238.01 при СПбГЭТУ «ЛЭТИ», расположенном по адресу 197376, Россия, Санкт-Петербург, улица профессора Попова, дом 5.

С диссертацией можно ознакомиться в библиотеке СПбГЭТУ «ЛЭТИ».

Автореферат разослан «___» _____ 2013 г.

Ученый секретарь
совета по защите докторских и
кандидатских диссертаций Д212.238.01,
к.т.н. Щеголева Н.Л.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. В последние годы с ростом уровня автоматизации, проникновения информационных технологий во все сферы деятельности человека и значительным повышением требований отказоустойчивости и надежности к информационным системам важное значение приобретают вопросы разработки эффективных средств мониторинга и диагностики информационных систем. В связи с повсеместным использованием вычислительных сетей (ВС) и сетей передачи данных для организации взаимодействия как между отдельными рабочими станциями для передачи информации прикладного характера (например, при работе в глобальной сети Интернет), так и взаимодействия внутри замкнутых вычислительных кластеров, информационно-вычислительных комплексов обработки данных, корпоративных сетей и иных распределенных систем, основанных на использовании вычислительных сетей, остро встают вопросы мониторинга состояния подобных систем.

Классические системы мониторинга обеспечивают непрерывный мониторинг текущего состояния узлов, входящих в состав ВС, но в условиях современных всё более усложняющихся распределенных систем и жестких требований к их отказоустойчивости и надежности, а также защищенности и информационной безопасности, к современным системам сетевого мониторинга предъявляются также требования по обеспечению возможностей прогнозирования и диагностики состояния обслуживаемых информационных систем в краткосрочном и долгосрочном периодах, а также реализации комплексного мониторинга, включающего анализ не только текущего состояния узлов ВС на основе формальных показателей их работоспособности, но и комплексный анализ более широкого спектра характеристик функционирования системы и входящих в её состав узлов, а также прогнозирование и диагностику потенциальных проблем в защищенности системы или отдельных её узлов от различных типов внешних вмешательств. Актуальность данных вопросов рассмотрена, в частности, в работах Р. Г. Шыхалиева, а также В.В. Коренькова, А.В. Ужинского и др.

Кроме того, актуальными проблемами разработки систем сетевого мониторинга являются увеличение точности анализа состояния входящих в состав ВС узлов, т. е. обеспечение максимального соответствия показаний системы мониторинга реальному состоянию информационной системы, а также уменьшение интенсивности обмена служебным трафиком и минимизация влияния подсистемы мониторинга на функционирование других подсистем вычислительной сети или распределенной системы.

В связи с изложенным задачи исследования и разработки методов мониторинга и диагностики вычислительных сетей и распределенных систем, а также систем мониторинга на их основе в настоящее время являются актуальными.

Целью работы является разработка метода и алгоритмов мониторинга ВС, основанных на анализе временны́х закономерностей в работе стека протоколов TCP/IP, и построение системы сетевого мониторинга на их основе.

Для достижения поставленной цели были решены следующие **задачи**:

1. Исследование и анализ современных подходов к организации систем сетевого мониторинга (ССМ). Классификация и исследование методов и алгоритмов анализа характеристик функционирования стека протоколов TCP/IP удаленного сетевого узла, оценка существующих ССМ, использующих в своем составе методы и алгоритмы данного класса.
2. Разработка временно́й модели функционирования стека протоколов TCP/IP при отработке механизма повторных передач.
3. Разработка метода и алгоритмов анализа стека протоколов TCP/IP удаленного сетевого узла, основанных на совместном анализе временны́х и функциональных характеристик TCP/IP с использованием методов многоклассовой классификации в качестве аналитического средства.
4. Выбор классификатора для разработанных метода и алгоритмов; определение конфигурации выбранного классификатора, обеспечивающей наибольшую эффективность работы разработанных метода и алгоритмов.
5. Исследование и оценка разработанных алгоритмов и их применимости в ССМ; разработка алгоритма конвейерного опроса сетевых узлов.
6. Разработка комплекса программ, реализующих функции сетевого мониторинга на основе разработанных метода и алгоритмов, внедрение разработанных программных средств в реальную ССМ и исследование их работоспособности.

Объектом исследования в диссертационной работе являются процессы мониторинга и диагностики вычислительных сетей и построенных на их основе распределенных систем.

Предметом исследования являются методы анализа характеристик функционирования стека протоколов TCP/IP удаленных сетевых узлов и возможности их применения в системах сетевого мониторинга.

Методы исследования. Теоретическая часть работы выполнена на основе методов системного анализа, интеллектуального анализа данных и математической статистики. В экспериментальной и практической частях работы приме-

няются методы распределенных вычислений, численные методы, методы интеллектуального анализа данных.

Научная новизна полученных результатов заключается в следующем:

1. Разработана временна́я модель функционирования стека протоколов TCP/IP при отработке механизма повторных передач.
2. Разработан метод идентификации версии стека протоколов TCP/IP, основанный на совместном анализе временны́х и функциональных характеристик TCP/IP с использованием многоклассового классификатора, и набор реализующих его алгоритмов.
3. Определена конфигурация классификатора на базе метода опорных векторов (МОВ), обеспечивающая наибольшую эффективность работы разработанных алгоритмов.
4. На основе разработанной временно́й модели механизма повторных передач и результатов обобщения её реализаций для различных версий стека протоколов TCP/IP разработан алгоритм конвейерного опроса узлов сети.

Практическая значимость. Практическую ценность имеют следующие полученные автором результаты:

1. Методика идентификации версии стека протоколов TCP/IP на основе совместного анализа временны́х и функциональных характеристик TCP/IP с использованием многоклассового классификатора.
2. Алгоритм конвейерного опроса узлов сети, предназначенный для извлечения значений анализируемых характеристик TCP/IP.
3. Программный комплекс мониторинга вычислительной сети, основанный на разработанных моделях и алгоритмах.

На защиту выносятся следующие основные результаты и положения:

1. Метод идентификации версии стека протоколов TCP/IP, основанный на совместном анализе временны́х и функциональных характеристик TCP/IP с использованием многоклассового классификатора, и набор реализующих его алгоритмов.
2. Конфигурация классификатора на базе МОВ, обеспечивающая наибольшую эффективность работы разработанных алгоритмов.
3. Алгоритм конвейерного опроса узлов сети, предназначенный для практического применения разработанных метода и алгоритмов.
4. Комплекс программ сетевого мониторинга, основанных на разработанных моделях и алгоритмах.

Апробация работы. Основные результаты работы докладывались и обсуждались на XVII Международной открытой научной конференции «Современ-

ные проблемы информатизации в анализе и синтезе технологических и программно-телекоммуникационных систем» (Воронеж, ноябрь 2011 г. – январь 2012 г.), VII международной научно-практической конференции «Перспективные разработки науки и техники» (Przemysl, Польша, 7-15 ноября 2011 г.), 64-й и 65-й научно-технических конференциях профессорско-преподавательского состава СПбГЭТУ «ЛЭТИ» (Санкт-Петербург, январь-февраль 2011 г. и январь-февраль 2012 г. соответственно).

Достоверность научных положений и результатов работы подтверждается результатами вычислительных экспериментов, результатами испытаний разработанных программных средств в условиях реальных вычислительных сетей, а также апробацией основных положений работы на международных и российских конференциях.

Реализация и внедрение результатов. Теоретические и практические результаты работы внедрены в рамках НИР «Разработка системы гидроакустического мониторинга акватории на базе покровных антенн», выполняемой по заказу ОАО «Концерн «Океанприбор», в составе подсистемы сетевого мониторинга цифрового вычислительного комплекса обработки гидроакустических сигналов. Разработанный комплекс программ используется также в качестве ССМ корпоративной сети кафедры Математического обеспечения и применения ЭВМ Санкт-Петербургского государственного Электротехнического университета «ЛЭТИ». Результаты работы используются в рамках учебного процесса по дисциплинам «Сети и телекоммуникации» и «Сетевые технологии» для подготовки бакалавров и магистров по направлениям 231000 «Программная инженерия» и 010400 «Прикладная математика и информатика».

Публикации. По теме работы опубликованы 11 научных работ, среди которых 3 публикации в ведущих рецензируемых изданиях, рекомендованных ВАК, 1 монография, 2 учебно-методических издания и 1 учебное пособие.

Структура и объем диссертации. Диссертация состоит из введения, 4 глав, заключения, списка сокращений и обозначений, библиографического списка, 3 приложений. Общий объем диссертации составляет 138 страниц, включая 31 рисунок и 16 таблиц. Библиографический список включает 102 наименования.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность диссертационной работы, сформулирована цель и аргументирована научная новизна исследований, показана практическая значимость полученных результатов, представлены выносимые на защиту научные положения.

Первая глава работы посвящена анализу современного состояния в области мониторинга ВС и распределенных систем, анализу современных методов сетевого мониторинга, а также методов анализа стека протоколов TCP/IP и их применимости в задачах сетевого мониторинга.

Под мониторингом ВС понимают функции постоянного наблюдения в пределах сети с целью поиска медленных или неисправных систем и оповещения сетевых администраторов о сбоях и иных неисправностях. Функции мониторинга выполняет система сетевого мониторинга (ССМ). Задачами сетевого мониторинга являются своевременное выявление отказов, разного рода неисправностей и аномалий в работе сетевых узлов и выработка рекомендаций по их устранению, а также их диагностика и профилактика.

Типичная ССМ в общем случае обеспечивает наблюдение только за заранее определенным перечнем узлов и отслеживает исключительно формальные показатели работоспособности узлов (загрузка CPU, состояние памяти, устройств хранения данных и т. п.). В настоящее время актуальна задача разработки методов и алгоритмов извлечения более широкого спектра характеристик функционирования сетевых узлов и их конфигурации с целью реализации дополнительных возможностей мониторинга.

Одной из разновидностей подобных методов являются методы сбора информации об удаленных сетевых узлах, важнейшей задачей которых является идентификация версии системного ПО (операционной системы) удаленного узла на основе анализа особенностей сетевого взаимодействия с данным узлом.

Методы идентификации версии операционной системы (ИОС) удаленных сетевых узлов применяются в ССМ и системах обеспечения сетевой информационной безопасности для решения следующих задач:

1. Инвентаризация сетевых узлов и установленного на них ПО.

2. Контроль за изменениями в конфигурации ПО узлов.

3. Отслеживание несанкционированных подключений посторонних аппаратных средств.

4. Аудит информационной безопасности.

Методы ИОС подразделяются на активные и пассивные (рис. 1).

Пассивные методы основаны на прослушивании и анализе сетевого трафика от целевого узла и не получили широкого распространения. Активные методы ИОС предполагают инициирование целенаправленного сетевого взаимодействия с целевой системой. Наибольшее распространение получили активные методы ИОС на основе обмена нестандартными пакетами и анализа заголовков TCP-пакетов, используемые совместно.

Вместе с тем, метод ИОС, основанный на обмене нестандартными TCP-пакетами, обладает рядом существенных недостатков:

1. Высокая зависимость от количества открытых и закрытых портов TCP и UDP на целевой системе.
2. Генерация значительного объема сетевого трафика.
3. Использование заведомо некорректных сетевых пакетов.

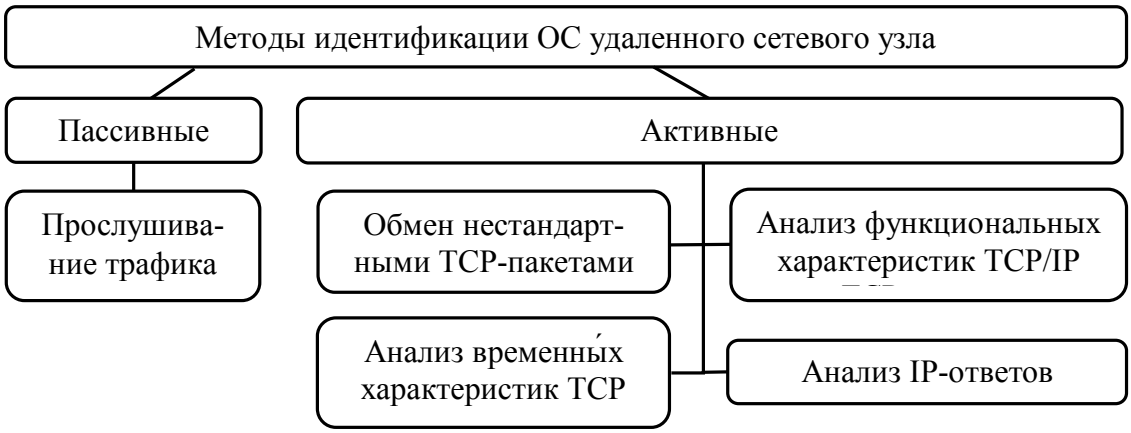

Рис. 1. Классификация методов ИОС

Методы анализа временны́х характеристик TCP лишены перечисленных недостатков, что позволяет рассматривать их как альтернативу методу, основанному на обмене нестандартными TCP-пакетами. Тем не менее, данная группа методов в настоящее время исследована в недостаточной степени, а число их программных реализаций невелико.

Исходя из вышесказанного поставлена следующая задача диссертационного исследования: исследование и разработка методов и алгоритмов ИОС, основанных на совместном анализе функциональных и временны́х характеристик взаимодействия по протоколу TCP, а также создание программных средств (ПС) сетевого мониторинга, основанных на разработанных методах.

Вторая глава посвящена исследованию и анализу известных методов ИОС, основанных на использовании временны́х характеристик TCP, а также разработке и исследованию метода и алгоритмов ИОС, основанных на совместном анализе функциональных и временны́х характеристик TCP/IP.

Один из возможных методов ИОС, основанный на анализе значений временны́х характеристик TCP, используемых для отработки механизма повторных передач (*Retransmission Timeouts*, RTO), получил название RING и заключается в анализе значений таймаутов повторных передач пакета SYN-ACK в процессе установления TCP-соединения (рис. 2).

В результате измерений формируется сигнатура ОС удаленного узла, представляющая собой набор значений $\lambda_1, \lambda_2, \lambda_3 \ldots \lambda_n$, где λ_i – интервал между регистрацией поступивших от целевого узла i-го и i+1-го пакетов.

Степень близости ОС анализируемого узла к некоторой *k*-й ОС из существующей базы сигнатур может быть оценена по следующей формуле:

$$C_k = \sum | \lambda_i - \tau_i |,$$

где τ_i – интервал времени между получением *i*-го и *i*+1-го пакетов для *k*-й ОС из существующей базы сигнатур.

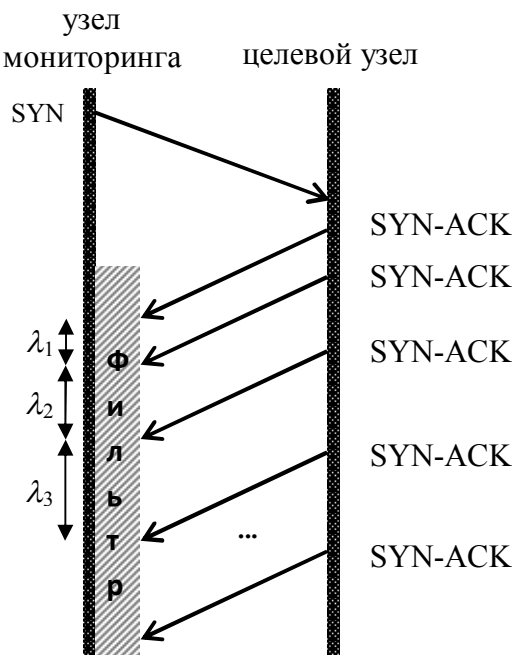

Рис. 2. Метод ИОС на основе анализа значений RTO для ситуации установления соединения

Преимущества RING заключаются в необходимости наличия на целевом узле только одного открытого порта TCP и использовании стандартных TCP-запросов.

Результаты исследований Ф. Вейсета, Т. Беадсли и др., а также собственного авторского исследования подтверждают существование различий в значениях таймаутов повторных передач стеков TCP/IP различных ОС и возможность решения задачи ИОС на основе анализа их значений.

Основным недостатком метода RING является его относительно невысокое быстродействие. Кроме того, использование RING невозможно в случае, если анализируемый узел расположен за системами типа Stateful firewall (в частности, SYN Relay и SYN Gateway).

Другой метод ИОС, свободный от ограничений, связанных с возможным использованием в сети систем SYN Relay или SYN Gateway, впервые упомянут в работах Грега Талека. Суть данного метода заключается в измерении и анализе значений RTO, характерных для ситуации потери пакетов при передаче данных по TCP-соединению.

Анализ значений временны́х интервалов λ_1, λ_2,..., λ_n между повторными передачами и их сравнение с существующей базой сигнатур, выполняемые аналогично случаю для процесса установления TCP-соединения, также позволяют сделать предположение о версии ОС целевого узла.

Преимущества по сравнению с RING заключаются в следующем:

1. Возможность работы через шлюзы SYN Relay или SYN Gateway.
2. Бóльшая прозрачность для систем IDS и фильтрации трафика.

Автором выполнено экспериментальное исследование метода Г. Талека (ГТ), в ходе которого проведены измерения значений характеристик RTO для

различных ОС. Пример полученных сигнатур (ГТ) для четырех различных ОС представлен в табл. 1.

Табл. 1. Пример сигнатур ОС для метода Грега Талека

Номер повторной передачи	Задержка перед повторной передачей, с			
	Fedora release 13 2.6.33.3	Windows Server 2003 R2	Windows XP SP3	Ubuntu 9.04
1	2,89	2,82	2,71	2,89
2	6,00	6,02	6,04	6,00
3	12,00	12,05	11,97	12,00
4	24,00	11,90	12,07	23,99
5	47,99	12,03	11,97	48,00
6	-	24,07	24,04	95,99
7	-	48,03	29,97	-

Автором предложен метод TCP-FTA, заключающийся в анализе временны́х характеристик RING и ГТ совместно с функциональными характеристиками TCP/IP с использованием методов классификации. Схема работы метода представлена на рис. 3.

Векторы значений временны́х характеристик $\mathbf{T}^N$ размерностью N и функциональных характеристик $\mathbf{F}^M$ размерностью M объединяются в единый вектор признаков $\mathbf{V}^D$ размерностью D, где $D = N + M$, $\mathbf{V}^D = \mathbf{T}^N \cup \mathbf{F}^M$, после чего вектор $\mathbf{V}^D$ передается для анализа многоклассовому классификатору, предварительно обученному на данных из эталонной базы сигнатур ($\mathbf{S}_K^D$). Результатом классификации является номер R сигнатуры из базы сигнатур, наиболее близкой к сигнатуре $\mathbf{V}^D$. Версия ОС, соответствующая результирующей сигнатуре R, является наиболее вероятной версией ОС целевого узла.

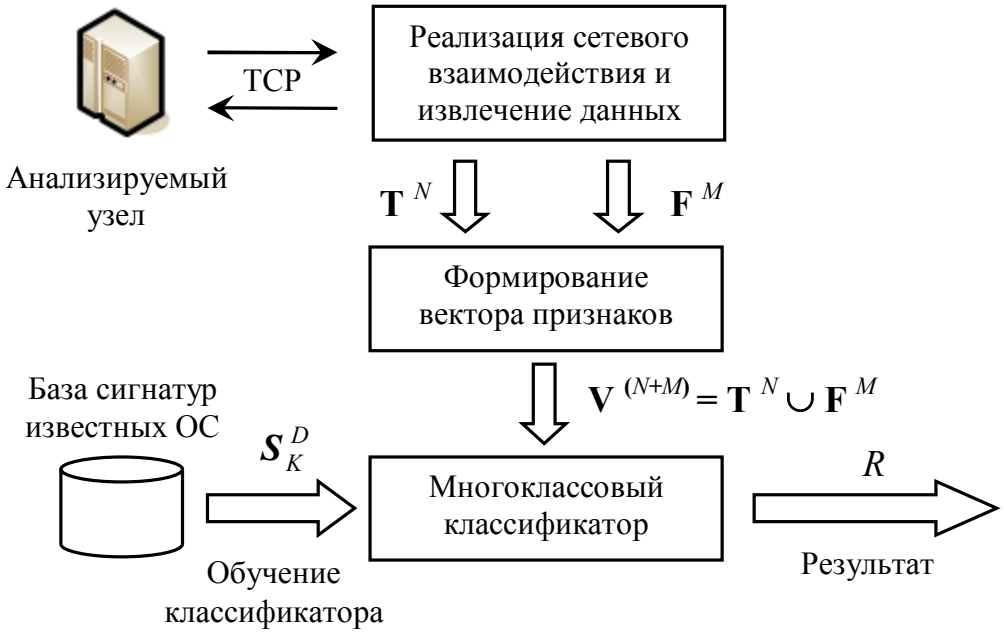

Рис. 3. Схема работы метода TCP-FTA

В качестве анализируемых характеристик рассматриваются значения следующих параметров функционирования стека TCP/IP целевого узла:

- функциональные: набор опций и порядок их объявления, размер окна, значение времени жизни пакета (TTL), значение Windows Scale;
- сигнатура RING;
- сигнатура ГТ совместно с признаком отправки завершающего пакета с установленным флагом RST.

В составе метода TCP-FTA в качестве классификатора предлагается использовать метод опорных векторов (МОВ), что обусловлено особенностями анализируемых векторов признаков, а именно неоднородностью признаков, наличием составных характеристик и относительно низкой размерностью векторов и обучающей выборки.

Возможны три алгоритма реализации метода TCP-FTA, отличающиеся набором анализируемых временны́х характеристик:

- TCP-FTA1 – анализируется сигнатура RING;
- TCP-FTA2 – анализируется сигнатура ГТ;
- TCP-FTA3 – совместно анализируются сигнатуры RING и ГТ.

Для определения наиболее эффективного алгоритма проведено экспериментальное исследование, по результатам которого установлено, что наиболее эффективным алгоритмом является TCP-FTA2.

Разработанные алгоритмы реализации метода TCP-FTA предполагают использование МОВ. Особенностью МОВ является отсутствие универсальных алгоритмов выбора конфигурации ядра. Автором было проведено экспериментальное исследование с целью выбора ядра МОВ и значений параметров ядра, обеспечивающих наибольшую эффективность работы алгоритма TCP-FTA2.

В целях исследования использована свободная библиотека libsvm, реализующая функциональность МОВ в задачах классификации. Исследование выполнено для четырех типов ядер: линейное (L), полиномиальное (P), радиально-базисное (R), сигмоидальное (S).

В рамках исследования использовалась выборка, состоящая из более чем 130 векторов признаков, соответствующих различным версиям ОС семейств Windows и Linux. Выбор векторов для формирования обучающей выборки осуществлялся случайным образом. Для достижения распределения векторов в обучающих выборках, близкого к равномерному, обучение и тестирование классификатора для каждой из анализируемых конфигураций ядра проводилось 100 тыс. раз со случайной генерацией обучающей выборки в каждом из тестов. Для проведения исследования была разработана GRID-система.

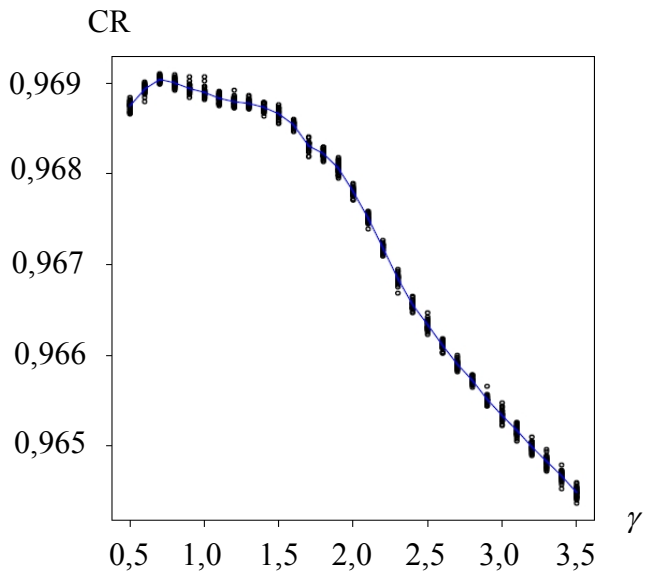

Рис. 4. График зависимости CR(γ) для радиально-базисного ядра

Для ядер с несколькими параметрами выбор оптимальных значений параметров выполнялся с помощью построения средневзвешенных графиков зависимости относительного числа правильно классифицированных векторов признаков (CR) от значения каждого из параметров ядра. Пример графика зависимости CR(γ) для радиально-базисного ядра приведен на рис. 4.

В результате исследования определены искомые конфигурации классификатора на базе МОВ для каждого из перечисленных ядер (табл. 2).

Табл. 2. Наилучшие конфигурации ядер МОВ для алгоритма TCP-FTA2

Ядро	Значения параметров настройки				CR, %
	γ	r	d	C, 10^3	
P	0,001..0,0011	1..1,08	529...530	236...241	96,75
L	–	–	–	20...40	96,60
S	0,019...0,035	0,05...0,25	–	5000...10000	96,68
R	0,6...0,9	–	–	50000...130000	96,91

По результатам исследования можно сделать вывод о том, что для практического применения алгоритма TCP-FTA2 следует рекомендовать радиально-базисное ядро МОВ с конфигурацией, соответствующей табл. 2.

Было также проведено экспериментальное исследование эффективности работы алгоритма TCP-FTA2 по сравнению с существующими методами ИОС, получившими практическое применение. В рамках исследования разработана программная реализация алгоритма TCP-FTA2, сформирована база сигнатур TCP-FTA2, насчитывающая 36 наименований, и проведен сравнительный анализ достоверности результатов работы программной реализация TCP-FTA2 с существующими ПС, реализующими методы ИОС: NMap, XProbe2, SinFP.

Результаты исследования представлены в табл. 3.

Табл. 3. Результаты исследования эффективности работы алгоритма TCP-FTA2 в сравнении с существующими программными реализациями методов ИОС

Программная реализация	CR, %	Количество пакетов, шт.	Трафик, Кб.
TCP-FTA2	87,07	18	9,51
NMap 6.25	82,39	2173	123,11
XProbe2	55,00	12	0,98
SinFP	68,26	14	0,95

Полученные результаты демонстрируют превосходство алгоритма TCP-FTA2 в сравнении с NMap по критерию CR и уровню потребления трафика. С учетом известных существенных недостатков NMap, от которых свободен метод TCP-FTA, можно сделать вывод о том, что во многих случаях практического применения методов ИОС программная реализация алгоритма TCP-FTA2 является эффективной заменой NMap.

В **третьей** главе работы предлагаются формализованная временна́я модель функционирования стека TCP/IP при отработке механизма повторных передач (МПП) потерянных пакетов данных и архитектура ССМ, основанной на алгоритме TCP-FTA2, а также рассматривается возможность применения метода TCP-FTA в системах обеспечения сетевой информационной безопасности.

Модель МПП стека протоколов TCP/IP представляет собой набор временны́х характеристик, описывающих моменты времени, соответствующие повторным передачам потерянного пакета данных, а также момент времени, соответствующий посылке завершающего пакета с флагом RST:

$$P = \{\tau_1, \tau_2, \tau_3, \ldots, \tau_R\}, \text{ где}$$

$$\tau_1 = \lambda_1;\ \tau_i = \tau_{i-1} + \lambda_i,\ 1 < i \le N;\ \tau_R = \tau_N + \lambda_R.$$

Здесь N – количество повторных передач; λ_R – интервал времени между отправкой N-го повторного пакета данных и завершающего RST-пакета.

Реализации модели МПП для различных версий стека протоколов TCP/IP описывают во временно́й области процесс обмена сетевыми пакетами, осуществляемый в рамках алгоритма TCP-FTA2.

В главе 1 сформулирован перечень задач сетевого мониторинга, для решения которых могут быть использованы методы ИОС. Автором предлагается архитектура ССМ целостности программной и аппаратной конфигураций ВС (рис. 5), основанной на использовании алгоритма TCP-FTA2. Принцип работы ССМ заключается в регулярном опросе узлов ВС на предмет определения соответствия сигнатур стека проколов TCP/IP узлов их штатным сигнатурам.

Блок-схема алгоритма принятия решения о возникновении нештатной ситуации в состоянии узла сети представлена на рис. 6. Нештатная ситуация определяется фактом выхода за пределы заданных допустимых значений $\{D_i\}$, $1 \le i \le M$, более чем P_{max} параметров сигнатуры узла $\{G_1, G_2, ..., G_K\}$, полученной в результате измерений, по сравнению с штатной сигнатурой $\{S_1, S_2, ..., S_M\}$.

Метод TCP-FTA также применим в системах обеспечения сетевой информационной безопасности для решения задачи анализа и поиска потенциальных и существующих уязвимостей и угроз безопасности сетевых узлов. Одним из важнейших этапов решения данной задачи является сканирование целевого уз-

ла методами ИОС на предмет определения версии его ОС. В настоящее время с этой целью применяется существующее ПО (NMap и др.), не использующее методы анализа временны́х характеристик TCP в качестве методов ИОС.

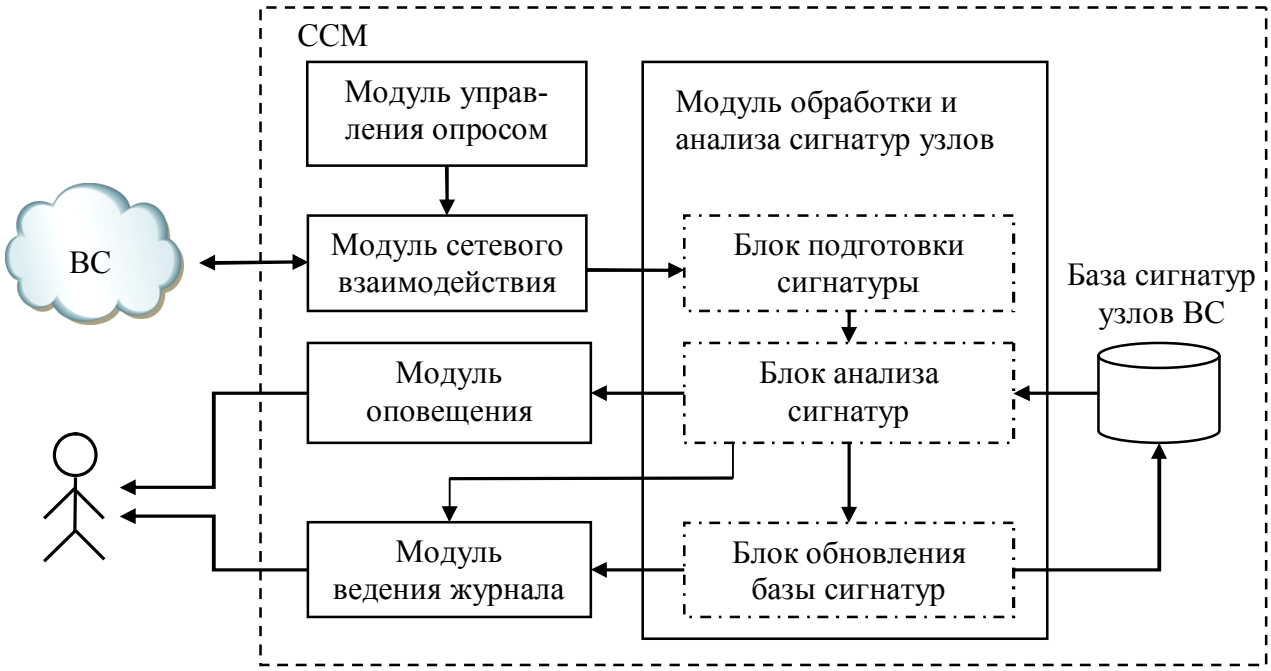

Рис. 5. Архитектура ССМ на основе алгоритма TCP-FTA2

Вместе с тем, как отмечалось ранее, существующие и получившие распространение в сетевых сканерах методы ИОС обладают рядом существенных недостатков. В связи с этим представляется целесообразным применение алгоритма TCP-FTA2 в составе средств анализа уровня защищенности сетевых узлов.

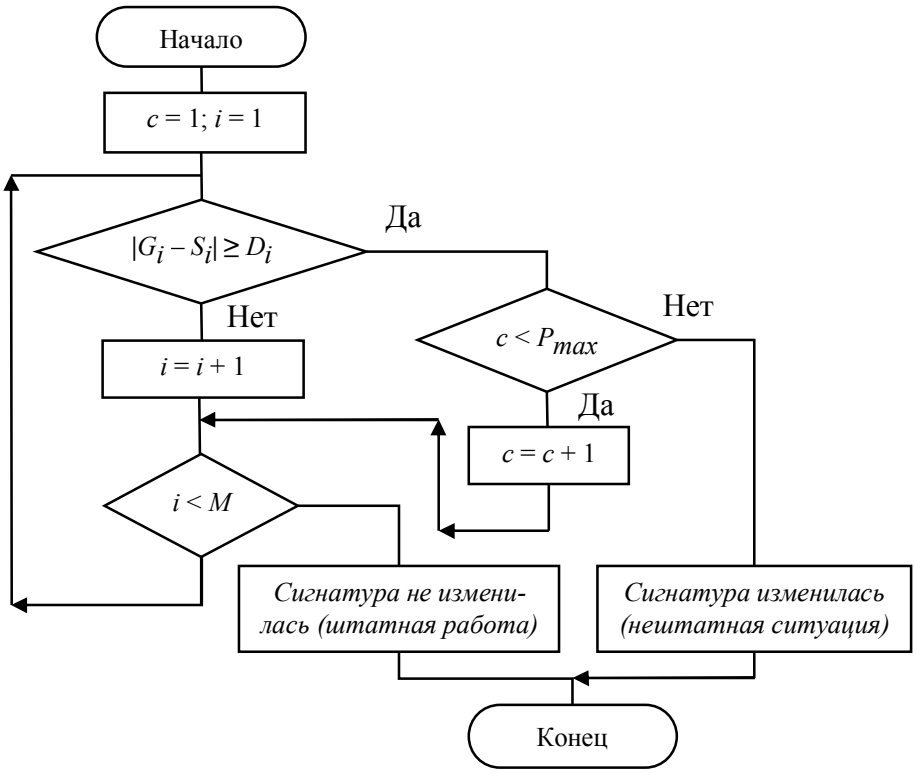

Рис. 6. Алгоритм принятия решения о нештатном состоянии узла

Модель программных средств аудита сетевых узлов, использующих алгоритм TCP-FTA2 для реализации функций ИОС, представлена на рис. 7.

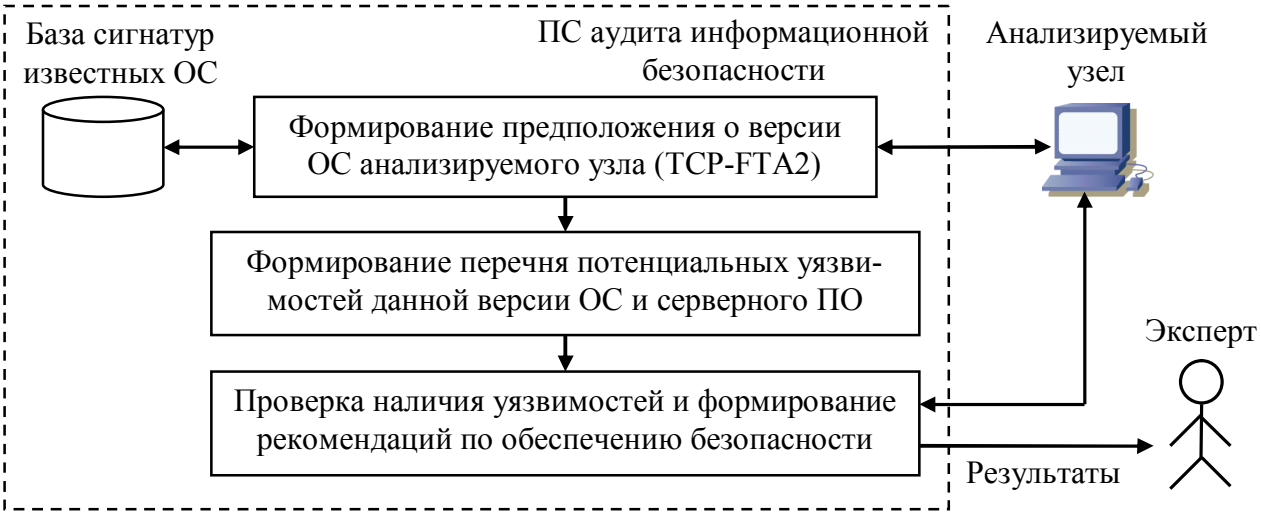

Рис. 7. Модель ПС аудита сети, использующих алгоритм TCP-FTA2

Алгоритм TCP-FTA2 может применяться в качестве инструмента ИОС в любых программных средствах, в составе которых необходима реализация возможности определения версии системного ПО сетевых узлов, включая автоматизированные системы выявления уязвимостей, системы инвентаризации и др.

Четвертая глава работы посвящена вопросам практической реализации алгоритма TCP-FTA2 в составе реальной ССМ.

На основе предложенной архитектуры ССМ и разработанной модели МПП стека протоколов TCP/IP на языке C++ с использованием библиотеки libpcap разработаны программные средства мониторинга целостности ВС, предназначенные для развертывания в среде Linux.

Особенностью метода TCP-FTA является длительное время анализа, что затрудняет его практическое использование. В целях практического применения алгоритма TCP-FTA2 разработан алгоритм конвейерного опроса узлов сети, функционирующих под управлением ОС семейств Windows и/или Linux.

В общем случае все N узлов сети, участвующие в процессе мониторинга, делятся на группы по N_R узлов в каждой, инициализация опроса узлов происходит последовательно по группам (рис. 8). Моменты начала опросов узлов определяются интервалом t и должны быть подобраны таким образом, чтобы в эти моменты времени отсутствовали пакеты с данными от других узлов. Значения t и N_R вычисляются при инициализации алгоритма.

Механизм вычисления интервала t базируется на результатах обобщения реализаций модели МПП для стеков протоколов TCP/IP ОС Windows и Linux (рис. 9), возможным благодаря частичному взаимному пересечению реализаций модели МПП для ОС указанных семейств.

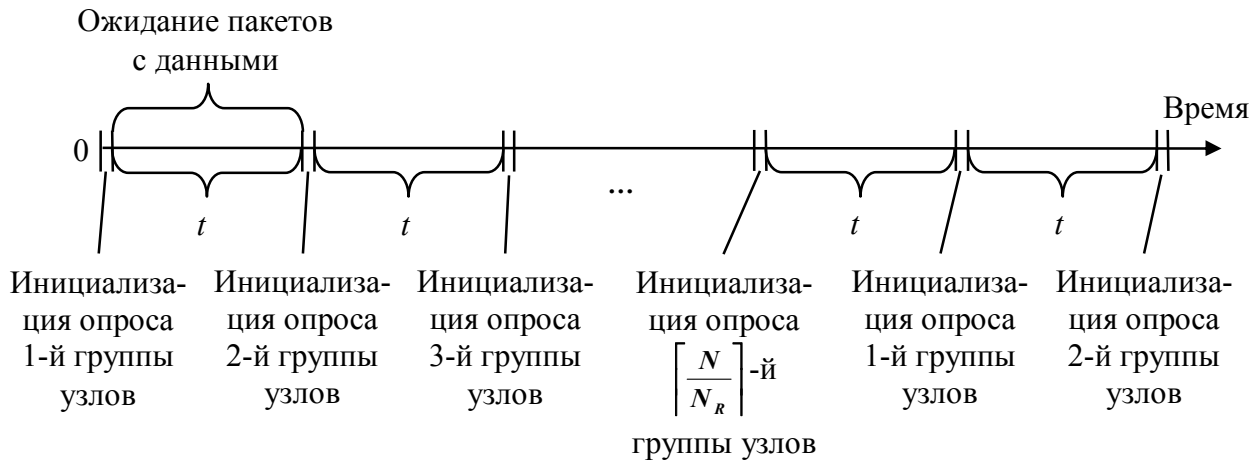

Рис. 8. Временна́я диаграмма конвейерного опроса узлов

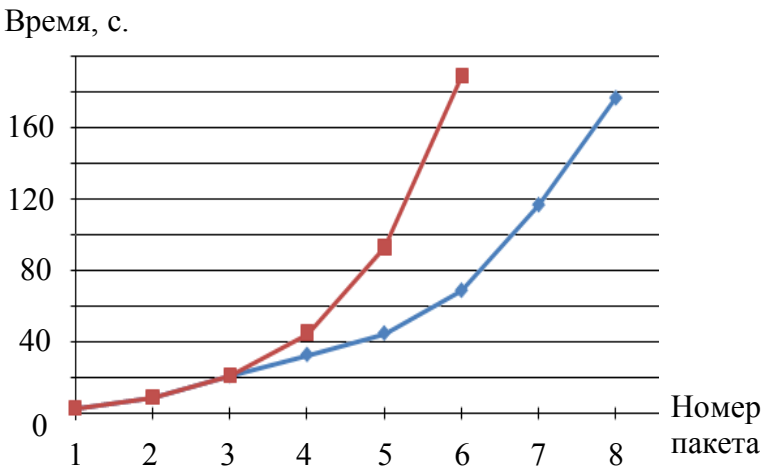

Рис. 9. Обобщение реализаций модели МПП для ОС семейств Windows и Linux

Из графика на рис. 9 установлены моменты времени, в которые гарантированно отсутствуют пакеты с данными от анализируемых узлов и, кроме того, существует достаточный запас времени до моментов возможного поступления пакетов с данными. К числу таких моментов времени относятся моменты времени через 105, 147 и 220 секунд после начала опроса узла. Отсюда получаем формулу для вычисления значений t и N_R:

$$\begin{cases} t = 105,\ N_R = \left\lceil \dfrac{105}{\tau} \right\rceil \text{ при } \tau \in [0;\ 105) \\ t = 105,\ N_R = 1 \text{ при } \tau \in [105;\ 147) \\ t = 147,\ N_R = 1 \text{ при } \tau \in [147;\ 220) \\ t = 220,\ N_R = 1 \text{ при } \tau \geq 220 \end{cases}, \tau = \frac{P}{N}, \text{ где}$$

P – период опроса ВС, заданный администратором ССМ, $P > 0$.

Под периодом опроса ВС понимается интервал времени, в течение которого должны быть опрошены все узлы ВС, участвующие в процессе мониторинга.

Нижний предел количества узлов, поддерживаемых конвейерным алгоритмом опроса в однопоточной реализации, может быть оценен по формуле:

$$N_M = 10\left\lceil \frac{P}{105} \right\rceil$$

Разработанные программные средства внедрены в составе подсистемы сетевого мониторинга цифрового вычислительного комплекса обработки гидроакустических сигналов в рамках ОКР «Гидропоиск», выполняемой ОАО «Концерн «Океанприбор». Испытания в условиях реальной ССМ показали работоспособность и корректность работы разработанных ПС.

В **заключении** подводятся итоги работы, формулируются выводы об эффективности и применимости полученных результатов.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В ходе решения поставленных в диссертационной работе задач получены следующие основные научные и практические результаты:

1. Разработана временна́я модель функционирования стека протоколов TCP/IP при отработке механизма повторных передач, проведено обобщение реализаций модели для стеков TCP/IP ОС различных версий.
2. Разработан метод идентификации версии стека протоколов TCP/IP удаленного сетевого узла, основанный на совместном анализе временны́х и функциональных характеристик TCP/IP с использованием многоклассового классификатора, и набор реализующих его алгоритмов, использующих метод опорных векторов в качестве классификатора.
3. Проведено экспериментальное исследование эффективности разработанных алгоритмов, по результатам которого определена наилучшая конфигурация классификатора на базе МОВ и установлено, что разработанные алгоритмы обладают бо́льшей эффективностью с точки зрения достоверности результатов и уровня потребления трафика по сравнению с аналогами.
4. Разработан алгоритм конвейерного опроса сетевых узлов, предназначенный для практического применения разработанного метода.
5. Разработан комплекс программ сетевого мониторинга, реализующий мониторинг целостности конфигурации аппаратного и программного обеспечения ВС. Комплекс программ внедрен в реальную ССМ, проведены его испытания в условиях реальной ВС.

СПИСОК ПУБЛИКАЦИЙ

В изданиях, рекомендованных ВАК РФ:

1. Лавров А. А., Яновский В. В. Идентификация операционной системы удаленного хоста методами анализа временных характеристик // Известия СПбГЭТУ «ЛЭТИ», 2011. №3, С. 34-39.

2. Лавров А. А., Большев А. К. Метод идентификации версии системного программного обеспечения удаленного сетевого узла, основанный на комплексном анализе характеристик TCP/IP // Известия СПбГЭТУ «ЛЭТИ», 2012. №1, С. 45-51.

3. Лавров А. А., Лисс А. Р. Программные средства мониторинга целостности конфигурации цифрового вычислительного комплекса обработки гидроакустических сигналов // Гидроакустика, 2012. Выпуск 16(2), С. 90-97.

Монография:

4. Лавров А. А., Лисс А. Р., Яновский В. В. Мониторинг и администрирование в корпоративных вычислительных сетях: научное издание. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2013. 160 с.

В других изданиях:

5. Лавров А. А., Большев А. К. Метод идентификации ОС удаленного хоста на основе анализа временных характеристик стека TCP/IP в задачах сетевого мониторинга // Сб. тр. 64-й науч.-техн. конф. проф.-преп. состава СПбГЭТУ «ЛЭТИ». СПб., 2011. С. 104-110.

6. Лавров А. А., Большев А. К., Яновский В. В. Идентификация ОС удаленного сетевого узла на основе комплексного анализа характеристик стека TCP/IP // Материалы VII международной научно-практической конференции «Перспективные разработки науки и техники», 07 - 15 ноября 2011 г. Przemysl, Польша: Sp. z o.o. «Nauka I studia», 2011. Том 53, С. 13-15.

7. Лавров А. А. Метод идентификации ОС удаленного узла на основе анализа функциональных и временных характеристик стека TCP/IP // Сборник трудов XVII Международной открытой научной конференции «Современные проблемы информатизации в анализе и синтезе технологических и программно-телекоммуникационных систем», ноябрь 2011 г. – январь 2012 г. Воронеж: Изд-во «Научная книга», 2012. Вып. 17, С. 271-273.

8. Лавров А. А. Алгоритмы классификации в задаче идентификации версии ОС удаленного сетевого узла // Сб. тр. 65-й науч.-техн. конф. проф.-преп. состава СПбГЭТУ «ЛЭТИ». СПб., 2012. С. 102-106.

Прочие работы:

9. Лавров А. А. Архитектура и программные средства сервисно-ориентированных систем: методические указания к курсовому проектированию / сост.: Кринкин К. В., Лавров А. А., Яновский В. В. – СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2010. – 52 с.

10. Лавров А. А., Большев А. К., Яновский В. В. Проектирование и анализ вычислительных сетей: методические указания к курсовому проектированию: учебное электронное издание [Электронный ресурс]: номер гос. регистрации 0321101787 // – СПб.: СПбГЭТУ «ЛЭТИ», 2011.

11. Лавров А. А., Большев А. К., Яновский В. В. Администрирование систем сервисно-ориентированной архитектуры: учеб. пособие. – СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2011. – 96 с.