ISSN 2078-9181

РОССИЙСКАЯ АКАДЕМИЯ НАУК
Отделение нанотехнологий и информационных технологий

САНКТ-ПЕТЕРБУРГСКИЙ
ИНСТИТУТ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ РАН

ТРУДЫ СПИИРАН

proceedings.spiiras.nw.ru

ВЫПУСК 1(38)

Санкт Петербург
2015

18+

Труды СПИИРАН

Выпуск № 1(38), 2015

Научный, научно-образовательный, междисциплинарный журнал с базовой специализацией в области информатики, автоматизации и прикладной математики

Журнал основан в 2002 году

Учредитель и издатель

Федеральное государственное бюджетное учреждение науки
Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)

Адрес редакции

199178, Санкт-Петербург, 14-я линия, д. 39,
e-mail: publ@iias.spb.su, сайт: http://www.proceedings.spiiras.nw.ru/

Подписано к печати 16.02.2015. Формат 60×90 1/16. Усл. печ. л. 15,6. Заказ № 63. Тираж 200 экз., цена свободная
Отпечатано в Редакционно-издательском центре ГУАП, 190000, Санкт-Петербург, Б. Морская, д. 67

Журнал зарегистрирован Федеральной службой по надзору в сфере связи и массовых коммуникаций, свидетельство ПИ № ФС77-41695 от 19 августа 2010 г.
Подписной индекс 29393 по каталогу «Почта России»

Журнал входит в «Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертации на соискание ученой степени доктора и кандидата наук»

SPIIRAS Proceedings

Issue № 1(38), 2015

Scientific, educational, and interdisciplinary journal primarily specialized
in computer science, automation, and applied mathematics

Trudy SPIIRAN ♦ Founded in 2002 ♦ Труды СПИИРАН

Founder and Publisher

Federal State Budget Institution of Science
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences
(SPIIRAS)

Editorial Board's address

14-th line VO, 39, SPIIRAS, St. Petersburg, 199178, Russia,
e-mail: publ@iias.spb.su, web: http://www.proceedings.spiiras.nw.ru/

Signed to print 16.02.2015
Printed in Publishing center GUAP, 67, B. Morskaya, St. Petersburg, 190000, Russia

The journal is registered in Russian Federal Agency for Communications and Mass-Media Supervision,
certificate ПИ № ФС77-41695 dated August 19, 2010 г.
Subscription Index 29393, Russian Post Catalog

СОДЕРЖАНИЕ

CONTENTS

Предисловие

Данный тематический выпуск журнала посвящен рассмотрению некоторых проблем информационной безопасности в условиях современных вызовов и угроз, а также способов предупреждения и предотвращения информационно-технической и информационно-психологической агрессии. Ряд статей представляет оригинальные результаты в области защиты организационно-технических систем критически важной инфраструктуры с возможностями активного противодействия, включая защиту персонала от вредоносного информационно-психологического воздействия. Предлагаются новые подходы к обеспечению безопасности, основанные на моделировании сценариев поведения сторон в конфликте и синтезе интеллектуальных систем противоборства в киберпространстве. В их числе: упреждающее противоборство, маскирование и сетевая контрразведка, управление информационным контентом и семантический контроль целостности.

Рассмотрены технологии разработки автоматизированных систем в защищенном исполнении с учетом информационных рисков и развиваемые для усложненной модели нарушителя. Представлены оригинальные технологии обнаружения и предупреждения воздействий в сетях связи различных операторов с учетом возможных сценариев поведения нарушителя. Приведены механизмы выявления и пресечения массовых вредоносных воздействий на информационно-телекоммуникационные системы и способы адаптивного управления целевым активным сетевым оборудованием для нейтрализации массированного возмущения и восстановления параметров штатного функционирования. Предлагается система непрерывного контроля целостности средств защиты информации и последующего восстановления эталонного состояния системы безопасности.

В выпуске представлены также оригинальные методы и технологии многоуровневой фильтрации потенциально вредоносного контента в мультимедийных потоках данных. Детализированы технологии защиты от скрытой передачи вредоносной видео- и аудиоинформации, призванных снижать риск возможного негативного влияния на индивидуальное и групповое психофизиологическое состояние персонала критической инфраструктуры. Обсуждается подход к созданию теории построения интеллектуальных киберсистем, способных порождать упреждающие стратегии поведения в

киберпространстве по аналогии с антиципирующим поведением биоорганизмов. Предлагаются решения по организации «доверительных сред» функционирования информационно-вычислительных комплексов, использующих потенциально опасные аппаратно-программные комплектующие. В данном тематическом выпуске журнала представлены большей частью статьи сотрудников Военно-космической академии имени А.Ф. Можайского, являющейся в настоящее время системообразующим политехническим ВУЗом Министерства Обороны Российской Федерации в области военно-космической деятельности, инфотелекоммуникационных технологий, а также технологий сбора и обработки специальной информации.

Директор СПИИРАН,
член-корреспондент РАН
Р.М. ЮСУПОВ

Профессор кафедры систем
сбора и обработки информации
Военно-космическая академия
имени А.Ф. Можайского,
доктор технических наук, профессор
А.Г. ЛОМАКО

Preface

This topical issue of the journal is dedicated to some specific aspects of information security emerging under actual threats and challenges, as well as to approaches aimed at preventing and averting of information-technical and information-psychological aggression. Many presented articles deliver original solutions intended for the protection of organization-technical systems of critical infrastructure capable of active counteraction, including protection of the personnel against malicious information-psychological impacts. New approaches are proposed to the security assurance based on modeling the scenarios of the conflict parties' behavior and on the synthesis of intelligent counteraction systems in cyberspace. Namely: anticipatory counteraction, masking and network counterintelligence, information content management and integrity's semantic control.

The technologies for development of secure automated systems that account for the information risks and the sophisticated malefactor model are considered. Original technologies are presented that are meant for detecting and averting the effects in communication networks of different operators with regard to possible scenarios of malefactor's behavior. Mechanisms developed in order to detect and suppress mass malicious effects upon the information and telecommunication systems as well as methods for adaptive control of active target network equipment for neutralization of mass disturbance and recovery of regular functioning parameters are represented. The system of continuous monitoring of the information securities' integrity and subsequent recovering of the reference security state is proposed.

Also this issue presents the original methods and technologies of multilevel filtration of potentially malicious content in multimedia data streams. Technologies of protection against hidden malicious video and audio information transfer meant for decreasing risks of the possible negative influence on the individual and group psycho-physiological condition of the critical infrastructure personnel are given in detail. An approach to developing a theory of designing the intelligent cyber systems capable of generating the proactive behavioral strategies in cyberspace similar to the anticipatory behavior of biological organisms is discussed. Solutions that consider a construct of "confidence environment" for functioning of information and computing systems that use potentially dangerous firmware components are suggested. Most of the articles published in this topical issue of the journal were submitted by the scientists

of the Military Space Academy named after A.F. Mozhaysky that currently is a backbone higher education polytechnic institution at the Russian Federation Ministry of Defense in the area of military-space activities, information telecommunication technologies, as well as technologies of special information gathering and processing.

St. Petersburg Institute for Informatics and Automation of the
Russian Academy of Sciences (SPIIRAS)
Director
Corresponding Member of the Russian Academy of Sciences
Doctor of Technical Sciences, Professor
R.M. YUSUPOV

Military Space Academy named after A. F. Mozhaysky
Department of the Systems for
Data Collection and Processing
Professor
Doctor of Technical Sciences, Professor
A.G. LOMAKO

УДК 613.86;159.913

К.О. Гнидко, А.Г. Ломако

КОНТРОЛЬ ПОТЕНЦИАЛЬНО ОПАСНОГО ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ НА ИНДИВИДУАЛЬНОЕ И ГРУППОВОЕ СОЗНАНИЕ ПОТРЕБИТЕЛЕЙ МУЛЬТИМЕДИЙНОГО КОНТЕНТА

Гнидко К.О., Ломако А.Г. **Контроль потенциально опасного информационно-психологического воздействия на индивидуальное и групповое сознание потребителей мультимедийного контента.**

Аннотация. В настоящей статье рассмотрены основные принципы построения многоуровневой системы контроля потенциально опасного информационно-психологического воздействия на потребителей мультимедийного контента. Представлены результаты экспериментальных исследований по обнаружению скрытых подпороговых воздействий.

Ключевые слова: психофизиологические воздействия, суггестия, подпороговые сообщения.

Gnidko K.O., Lomako A.G. **Monitoring of Potentially Dangerous Information-Psychological Affect on Individual and Group Consciousness of Multimedia Content Consumers.**

Abstract. This article reviews the basic principles of multi-level system of diagnostics and monitoring of potentially dangerous informational and psychological affect on consumers of multimedia content. The results of experimental studies on the detection of hidden subliminal messages are represented.

Keywords: psychophiziological affections, suggestion, subliminal messages.

1. Введение. Возможности науки и техники в настоящее время позволяют создавать средства и методы для информационного воздействия на индивидуальное, групповое и массовое сознание граждан РФ. Действующая Военная доктрина Российской Федерации подчеркивает тенденцию смещения военных опасностей и военных угроз в информационное пространство и внутреннюю сферу Российской Федерации, а также указывает на одну из главных внутренних военных опасностей: деятельность по информационному воздействию на население, в первую очередь на молодых граждан страны, имеющую целью подрыв исторических, духовных и патриотических традиций в области защиты Отечества [1].

Обычно под информационной безопасностью подразумевается состояние защищенности жизненно важных интересов граждан, общества и государства в информационной сфере [2]. Однако при этом все же недостаточное внимание уделяется личности человека. А именно личность должна стать предметом пристального внимания и защиты от возможных угроз, в том числе информационных, в период бурного развития телекоммуникационных систем. Информационное оружие имеет целью, в том числе, «массовое распространение и внедрение в сознание людей определенных представлений, привычек и поведенче-

ских стереотипов, вызывающих недовольство или панику среди населения, а также провоцирование деструктивных действия различных социальных групп» [3].

Перечень приоритетных проблем научных исследований в области обеспечения информационной безопасности Российской Федерации, утвержденный Советом Безопасности РФ, определяет в качестве одного из наиболее актуальных направлений исследование проблем защиты индивидуального, группового и массового сознания российского общества от деструктивных воздействий различных информационных источников. Наиболее удобной средой для осуществления атак на защищаемые психофизиологические ресурсы в силу ряда особенностей (масштабность, гетерогенность, децентрализованность, отсутствие цензуры, возможность передачи мультимедийных данных любых видов) в настоящее время является глобальная вычислительная сеть Интернет. Таким образом, чрезвычайно актуальной является не только проблема защиты информации, но и проблема защиты от информации, которая в последнее время приобретает международный масштаб и стратегический характер.

Организациями, ведущими активные исследования в области психотехнологий на территории России, являются кафедра психоэкологии Российского университета дружбы народов, Институт психологии Российской академии наук, научная группа кафедры психиатрии Московской медицинской академии им. Сеченова, Всероссийский научно-исследовательский институт телевидения и радиовещания и некоторые другие организации.

В настоящей статье кратко обобщены результаты проведенных авторами исследований в области защиты пользователей автоматизированных систем от потенциально опасного мультимедийного контента. Проект системы защиты несовершеннолетних пользователей от скрытого вредоносного воздействия мультимедийного контента сети Интернет, разработанный в соответствии с изложенными в данной работе принципами, удостоен приза за лучшую инновационную идею на конкурсе инновационных проектов в сфере науки и высшего профессионального образования Санкт-Петербурга в 2012 году [4].

2. Многоуровневая фильтрация потенциально опасных информационно-психологических воздействий в мультимедийных потоках. Эффективная система диагностики и контроля потенциально опасных информационно-психологических воздействий на индивидуальное и групповое сознание должна обеспечивать выполнение следующих функций:

– на внешнем уровне: обнаружение и ликвидация условий, по-

рождающих проявление угроз, а также создание условий, препятствующих их проявлению;

– на граничном уровне: обнаружение проявлений угроз, препятствие доступу реализуемых угроз к защищаемым ресурсам;

– на внутреннем уровне: обнаружение и локализация несанкционированных воздействий на защищаемый ресурс, своевременная ликвидация последствий и причин возникших нарушений информационно-психологической безопасности.

Перечислим подмножества классов негативного контента, подлежащих вскрытию и фильтрации при обработке мультимедийных потоков данных в контурах автоматизированных систем инфраструктуры критически важных объектов.

1. Текстовые массивы. К наиболее значимым параметрам, определяющим воздействие текста на психофизиологическое состояние человека, относятся:

– негативная фоносемантическая окраска;

– фрактальные свойства, определяющие меру суггестивности текста [5, 6].

2. Видеопотоки. Наибольшее значение для деятельности человека-оператора имеет зрительный анализатор, через который поступает около 90% всей обрабатываемой информации. Зрение позволяет воспринимать форму, цвет, яркость и движение предметов. Возможность зрительного восприятия определяется энергетическими, пространственными, временными и информационными свойствами сигналов, поступающих к оператору. Совокупность этих свойств и динамика их изменения во времени (структура видеопотока) определяют информацию, которую визуальный сигнал несет в сферу сознательного и бессознательного психики оператора. В ряде работ [7–10] рассматриваются различные аспекты угрозы скрытого воздействия видеосигнала на сознание, подсознание и психофизиологическое состояние человека. Общеизвестен инцидент, приведший к госпитализации в Японии 16 декабря 2007 года более 700 детей после просмотра мультфильма «Покемоны». Вызвано это было тем, что мелькание цветовых пятен в кадре на протяжении около 10 секунд вызвало эффект «резонанса» с основными частотами функционирования головного мозга.

Экспериментальное подтверждение имеют эффекты воздействия на сознание и подсознание человека скрытых неосознаваемых визуальных вставок, а также световая частотная стимуляция [11, 12]. В связи с этим, фильтрации в видеопотоке подлежат:

– скрытые визуальные вставки;

– диспарантные видеовставки;

– колебания яркости (мерцания) в диапазоне биоэффективных частот.

3. Аудиопотоки. Вредоносный контент, подлежащий фильтрации в аудиопотоках, включает:

– аудиосуггестию (под аудиосуггестией здесь и далее понимается процесс воспроизведения и восприятия особой аудиоинформации, результатом которого является существенное снижение уровня критического восприятия объекта воздействия (суггеренда), изменяется его эмоциональное и психофизиологическое состояние) [13, 14];

– вредоносные бинауральные ритмы в области биоэффективных частот (так называемые «цифровые наркотики»).

Разработанная авторами концепция реализует системный подход к фильтрации потенциально вредоносного контента в мультимедийных потоках данных и учитывает особенности возникновения и реализации угроз на всех этапах их существования.

Достижение поставленной цели предполагает решение следующих задач:

1. Установление подозрения на наличие вредоносных структур в мультимедийных потоках данных. Объемы информации, циркулирующие в современных сетях передачи данных, определяют высокие требования к скорости анализа и выявления потенциально вредоносных конструкций в мультимедийном контенте. При этом сохраняется значительная неопределенность признаков вредоносности. В данных условиях эффективным решением является построение распознавателя верхнего уровня на основе аппаратной реализации нейронной сети прямого распространения, предварительно обученной на репрезентативной выборке эталонных объектов. Входными данными для нейросетевого классификатора являются параметры структуры бинарного потока, полученные в результате его предварительной обработки. Выходной информацией нейросетевого классификатора является решение о принадлежности анализируемого участка бинарного потока к классу нейтральных или потенциально вредоносных (подозрительных) объектов.

2. Выявление скрытых информационно-психологических воздействий в мультимедийных объектах на основе частных алгоритмов распознавания. Входными данными для частных алгоритмов распознавания вредоносных свойств в мультимедийных объектах, являются файлы, содержащие данные объекты. На данном этапе из анализа исключаются файлы, зашифрованные криптографическими средствами, а также мультимедийные файлы, для которых в автоматизированной системе отсутствуют соответствующие декодеры. Выходные данные для каждого из алгоритмов, зависят от типа анализируемого объекта и

класса выявляемой угрозы вредоносного воздействия. В общем случае результатом работы частных алгоритмов является решение о принадлежности анализируемого мультимедийного объекта по признаку наличия вредоносных свойств к одному из двух классов: подозрительные на вредоносность и нейтральные.

3. Подтверждение факта вредоносного воздействия на основе контроля ответных физиологических реакций. Принятие решения о наличии негативного влияния на потребителей мультимедийного контента осуществляется на основе применения нечеткого классификатора, входными данными для которого являются психофизиологические параметры персонала, снимаемые комплексом датчиковой аппаратуры. Базисом для построения классификации на основе теории размытых множеств являются регулярные наблюдения и опыт экспертов в области психофизиологии. Выход нечеткой модели зависит от ее структуры и параметров – функций принадлежностей и весов правил. В общем случае настройка представляет собой нахождение параметров, минимизирующих расстояние между желаемым и действительным поведением нечеткой модели на обучающей выборке.

Вероятность возникновения психофизиологических угроз новых типов предъявляет к разработанной технологии требование по возможности дообучения распознавателей различных уровней. В силу того, что обучаемым элементом системы является вероятностная нейронная сеть, соблюдение данного требования возможно при наличии обратной связи – от подсистемы контроля психофизиологических параметров к нейросетевому распознавателю. При этом выявленные нечетким классификатором вредоносные объекты должны пройти соответствующую первичную обработку.

Обобщенная схема модели системы диагностики и контроля потенциально опасных информационно-психологических воздействий на индивидуальное и групповое сознание потребителей мультимедийного контента представлена на рисунке 1.

Вредоносные конструкции, скрытые в мультимедийных объектах, на бинарном уровне представления обладают, подобно компьютерным вирусам, набором сигнатурных признаков, по которым может быть установлено подозрение на наличие вредоносных свойств в анализируемом участке бинарного потока. Подобные признаки могут быть определены в результате структурного и спектрального анализа бинарных образов эталонных вредоносных объектов.

В соответствии со схемой, представленной на рисунке 1, на вход системы поступает бинарный поток, содержащий мультимедийные данные. Анализируемый бинарный поток является двоичной по-

следовательностью конечной длины и представляет собой конкатенацию некоторого числа L двоичных символов.

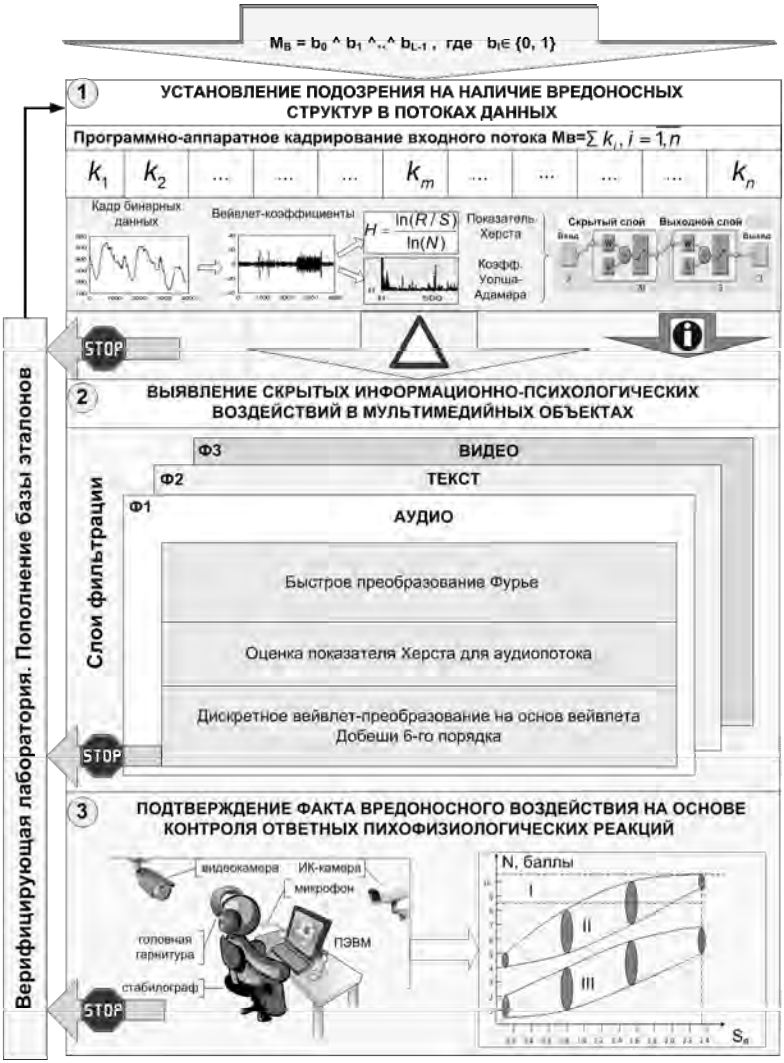


Рис. 1. Модель многоуровневой системы диагностики и контроля потенциально опасных информационно-психологических воздействий на индивидуальное и групповое сознание потребителей мультимедийного контента

Элементарным (неделимым) структурным элементом бинарного

потока является бит (двоичный символ): $M_b=b_0 \wedge b_1 \wedge \ldots \wedge b_{L-1}$, где $b_i \in \{0,1\}$, $i=\overline{1,L-1}$. Как правило, для сокращения объема передаваемой информации и увеличения скорости и надежности передачи информации применяются различные форматы кодирования и сжатия данных. Структура и свойства обработанных таким образом потоков могут не иметь признаков наличия вредоносных объектов. Вместе с тем, для реализации угрозы психофизиологического воздействия негативный контент должен быть предъявлен атакуемому лицу в явном виде, определенном особенностями восприятия и порогами чувствительности органов чувств человека. Данное обстоятельство позволяет осуществлять наиболее результативное выявление и фильтрацию вредоносных информационно-психологических воздействий непосредственно после декодирования бинарного потока на этапе, предшествующем этапу восприятия.

Таким образом, входной бинарный поток данных должен быть декодирован с применением декодеров соответствующего типа и разделен по типам мультимедийных объектов (текст, видео-, аудиообъект). Поэтому необходимым условием для корректного выполнения последующих процедур фильтрации является наличие в системе установленного пакета кодеков (кодеров-декодеров) для всех типов обрабатываемых мультимедийных объектов.

Основным объектом анализа на первом этапе разработанной технологии являются особенности структуры, в которых могут быть выявлены признаки, характерные для вредоносных информационно-психофизиологических объектов. Для выявления параметров структуры бинарный поток разбивается на отдельные кадры k_i, представляющие собой битовые последовательности длиной d. Определение битовой длины d кадров, на которые разбивается входной бинарный поток, осуществляется с учетом доступных вычислительных ресурсов и зависит от мощности и конфигурации привлекаемой для анализа автоматизированной системы. Уменьшение длины кадра снижает нагрузку на вычислительные ресурсы, однако увеличивает время обработки данных.

Для каждого из кадров осуществляется дискретное вейвлет-преобразование. Преимущество вейвлет-анализа перед другими видами спектрального и структурного анализа заключаются в том, что с его помощью могут быть подвергнуты анализу как общие свойства набора данных, так и локальные особенности, например, резкие изменения, скачки, диссонирующие с общим фоном. На основе полученного набора аппроксимирующих вейвлет-коэффициентов для каждого из кадров бинарного потока выполняется быстрое преобразование Уол-

ша-Адамара и рассчитывается фрактальная размерность на основе вычисления показателя Херста, что позволяет при общем сокращении признакового пространства выделить наиболее значимые и информативные признаки исследуемого бинарного потока.

Данные, полученные в результате указанных преобразований, поступают на вход нейронной сети, предварительно обученной на основе репрезентативной обучающей выборки. Обучающая выборка должна включать бинарные образы объектов двух классов: безопасных относительно оказываемого психофизиологического воздействия и априорно рассматриваемых как вредоносные. С учетом этого нейросетевой классификатор осуществляет разделение кадров бинарного потока по признаку вредоносности на следующие классы:

1) Имеющие признаки вредоносных конструкций. Кадрам данного класса по результатам распознавания присваивается идентификационный маркер «красный».

2) Не имеющие признаков наличия вредоносных конструкций (нейтральные). Кадрам данного класса присваивается классифицирующий маркер «зеленый».

2.1. Применение нейронной сети прямого распространения для обнаружения подозрительных на вредоносные конструкции в бинарном потоке данных. Цель обучения нейронной сети состоит в такой подстройке ее параметров, чтобы заданному входному вектору X сеть ставила в соответствие целевой выходной вектор Z**.** Вместе эти векторы составляют обучающую пару, а группа обучающих пар составляет обучающее множество. Алгоритм обучения искусственной нейронной сети в общем виде включает в себя следующие шаги (рисунок 2):

1) Выбор обучающей пары векторов из обучающего множества и подача входного вектора на входы сети.

2) Вычисление выходного вектора сети.

3) Вычисление разности между выходным и целевым векторами.

4) Коррекция весов сети с целью минимизации ошибки.

5) Повтор шагов с 1 по 4 для каждой пары обучающего множества до тех пор, пока ошибка на всем множестве не достигнет заданного уровня.

После завершения обучения нейросеть готова к решению задачи классификации конструкций, подозрительных на вредоносные, в бинарном потоке данных. В рабочем режиме сети предъявляется входной вектор, состоящий из тройки параметров (максимальное значение коэффициента Уолша-Адамара, порядковый номер коэффициента, при котором достигается его максимальное значение, и показатель Херста,

рассчитанный для анализируемого бинарного кадра). Входной вектор соответствующим образом активирует нейроны слоя образцов. Каждый нейрон слоя образцов выдает на своем выходе некоторый уровень активности $y_i(x)$.

Шаг 1. Вычисление дискретных значений амплитудной вейвлет-функции:

$$W_A(a_i,b_j)=\frac{1}{n(a_i,b_j)}\sum_{k=0}^{N-1}x_k\psi\left(\frac{t_k-b_j}{a_i}\right)$$

Шаг 2. Вычисление скейлограмы:

$$S(a_i,b_j)=\left|W_A(a_i,b_j)\right|^2$$

Шаг 3. Масштабирование вейвлета:

$$d_a=2\Delta_t a$$

Шаг 4. Расчет параметров для обучения нейронной сети:

$$NL(S(a_i,b_j))=\min d(f;f_{вфф});\qquad W=\max(NL);I=index(W);\qquad H=\frac{\ln(R/S)}{\ln(N)}$$

Шаг 5. Передача параметров H,W,I ***на вход нейросети прямого распространения:***

Шаг 6. Нормализация входного вектора значений

$$x_j^N=\frac{x_j}{\sqrt{x_1^2+x_2^2+\ldots+x_N^2}}=\frac{x_j}{\sqrt{\sum_{j=1}^{N}x_j^2}}$$

Шаг 7. Выбор обучающей пары векторов из обучающего множества и подача входного вектора на входы сети.

Исходные обучающие векторы		Нормлизованные обучающие векторы	
x_1	x_2	x_1''	x_2''
3,0	5,0	0,5145	0,8575

Шаг 8. Вычисление выходного вектора сети.

$$Y^k=\sum_{i=1}^{L_k}\exp\left(\frac{1}{\sigma^2}\sum_{j=1}^{N}x_j^N w_{ij}^N-1\right),k=\overline{1,m}$$

Класс	№ нейрона	w_1	w_2	$y_i(X)$	$Y^k(X)$
A	1	0,5145	0,8575	0,0000	0,5458
	2	0,7071	0,7071	0,3950	
	...	...	...	...	
B	7	0,9615	0,2747	0,0011	0,1389
	8	0,9191	3939	0,0516	
	...	...	...	...	

Шаг 9. Вычисление разности между выходным и целевым векторами.

$$d_q=\left|Y_q^k(X_l)-S_q(a_i,b_j)\right|$$

$$W=\begin{vmatrix}w_{11} & w_{12} & \cdots & w_{1L}\\ w_{21} & w_{22} & \cdots & w_{2L}\\ \cdots & \cdots & \cdots & \cdots\\ w_{N1} & w_{N1} & \cdots & w_{NL}\end{vmatrix}=\begin{vmatrix}x_{11} & x_{12} & \cdots & x_{1L}\\ x_{21} & x_{22} & \cdots & x_{2L}\\ \cdots & \cdots & \cdots & \cdots\\ x_{N1} & x_{N1} & \cdots & x_{NL}\end{vmatrix}$$

Шаг 11. Повтор шагов с 6 по 9 для каждой пары обучающего множества до тех пор, пока ошибка на всем множестве не достигнет приемлемого уровня.

Шаг 12. Завершение обучения. Применение нейрораспознавателя

Рис. 2. Алгоритм обучения искусственной нейронной сети

Каждый *k*-нейрон слоя суммирования суммирует уровни активности $y_i(X)$ всех нейронов слоя образцов своего *k*-класса и выдает на своем выходе общий уровень активности данного *k*-класса $Y^k(X)$. Выходной нейрон на основании вычисленных сетью уровней активности по каждому классу $Y^k(X)$ определяет, какой нейрон слоя суммирования имеет максимальный выходной сигнал. Тем самым (по номеру *k* нейрона), определяется номер класса *k*, к которому с большей вероятностью принадлежит предъявленный входной образ X.

Таким образом, в результате работы нейросетевого классификатора делается вывод о принадлежности анализируемого участка бинарного кода к классу подозрительных на вредоносные.

В рамках экспериментальных исследований на стенде применялся нейросетевой классификатор на основе вероятностной нейронной сети прямого распространения [15]. Количество выходных состояний сети – два. Для первого состояния характерно выявление бинарных кадров, «подозрительных» на наличие вредоносных закладок, второе состояние характеризуется выбором бинарных кадров, не имеющих признаков наличия негативного информационного контента. Выборка разбивается на 3 части (обучающую, проверочную и тестовую). Рекомендуемым является следующее соотношение: обучающая часть составляет 75% от общего объема выборки, проверочная и тестовые – по 15% от общего объема. Обучающее, проверочное и тестовое множества бинарных кадров являются непересекающимися, что позволяет оценить способность обученной нейронной сети к обобщению. Результаты оценивания качества разработанного распознавателя (на этапах обучения, коррекции весов нейронов и тестирования) при обнаружении в сетевом трафике признаков аудиосуггестии приведены в виде матриц неточностей на рисунке 3.

Рис. 3. Результаты оценивания качества разработанного нейросетевого распознавателя при обнаружении в бинарном потоке данных аудиосуггестии

2.2. Подтверждение факта вредоносного воздействия на основе нечеткой классификации физиологических показателей пользователя. Подтверждение факта воздействия негативного контента данных может быть осуществлено на основе регистрации в процессе деятельности психофизиологических параметров потребителей мультимедийного контента. Сложность определения функционального состояния человека по совокупности полученных параметров заключается в нечетком характере ответных реакций организма на входные информационные стимулы и размытости границ их диапазонов. Учитывать данные особенности позволяет применение нечеткого классификатора на основе размытых множеств.

Достоверность определения психофизиологического состояния персонала повышается пропорционально увеличению количества регистрируемых параметров и частоте съема данных параметров. Вместе с тем, комплект датчиковой аппаратуры должен причинять минимальные неудобства пользователю системы. Исходя из данного противоречия и доступных к настоящему времени аппаратных средств контроля физиологических параметров, определен рациональный состав комплекта регистрирующей аппаратуры. Он включает в себя: видеокамеру, инфракрасную камеру, головную гарнитуру с интегрированным датчиком частоты сердечных сокращений, микрофон с интегрированным датчиком частоты дыхания и стабилограф. Указанный набор датчиков, с одной стороны позволяет с требуемой достоверностью определять функциональное состояние человека-оператора, а с другой стороны не отвлекает его от выполнения основных обязанностей по предназначению. Вариант расположения датчиковой аппаратуры показан на рисунке 4.

Рис. 4. Автоматизированное рабочее место, оснащенное аппаратурой контроля текущего функционального состояния пользователя

Алгоритм нечеткой классификации во множестве описаний образов функциональных состояний операторов в деятельности может быть представлен следующим образом.

1) Выбрать из состава обучающей выборки b-й образ функционального состояния (ФС) и принять вектор ее характеристик за начало отсчета многомерной поверхности координат ФС.

2) По известным методикам оценки расстояний между образами параметров объектов конкретного типологического содержания определяются векторы расстояний между образами ФС из состава обучающей выборки (ОВ) и образа ФС, принятого за начало отсчета в данной ОВ. Полученные векторы расстояний рассматриваются как изоморфные соответствующим значениям параметров ФС при условии начала их координат в точке, определяемой характеристиками объекта.

3) В соответствии с алгоритмом многомерной размытой классификации вычисляются параметры шкалы оценок функций принадлежности ФС выделенным классам и вектора функций принадлежности остальных образов ФС из состава ОВ, для всех X.

4) Вычисляется степень близости полученных параметров и исходного вектора (характеристического вектора), заданного в информационном векторе ОВ, по величине дисперсионного отношения.

5) Если все образы ФС из состава ОВ просчитаны, то переход к п. 6. Если нет, то переход к п.1.

6) Определение оптимального с точки зрения безошибочности классификации начала отсчета параметров ФС из состава ОВ.

Относительно этой точки в дальнейшем приводится измерение координат классифицируемых функциональных состояний операторов. Данной точке отсчета будут соответствовать рациональные параметры шкалы классификации, а именно центры классов и весовые коэффициенты типологически различных групп понятий в описании ФС.

Обобщенная структурная схема многомерного размытого классификатора, в котором реализуются такие режимы работы как расчет параметров классификационной шкалы, внутреннее структурирование ОВ, контроль непротиворечивости ОВ, коррекция ОВ и собственно классификация новых объектов приведена на рисунке 5.

В результате работы классификатора, основанного на нечеткой логике и аппарате размытых множеств, система генерирует одно из 3-х возможных сообщений:

– пользователь подвергся вредоносному психофизиологическому воздействию – высокая «физиологическая цена» деятельности (интегральный показатель принял значение «красный»);

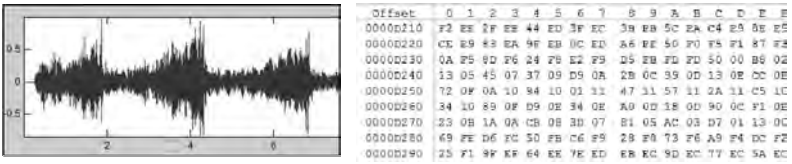
– существует вероятность оказания вредоносного психофизиологического воздействия – нормальная «физиологическая цена» деятельности (интегральный показатель принял значение «желтый»);

– пользователь не подвергался вредоносному психофизиологическому воздействию – низкая «физиологическая цена» деятельности (интегральный показатель принял значение «зеленый»).

Рис. 5. Структурная схема многомерного размытого классификатора

Таким образом, применение нечеткого классификатора позволяет осуществить подтверждение факта оказания вредоносного информационного воздействия на потребителей мультимедийного контента. Преимуществом применения нечеткого классификатора является возможность распознавания ранее неизвестных типов информационных закладок по вызываемым ими ответным физиологическим реакциям оператора. Бинарный образ скомпрометированного мультимедийного потока передается для дальнейшего исследования в специализированную лабораторию и, при обнаружении устойчивой связи между воздействием содержащегося в нем объекта на органы чувств испытуемого и ухудшением его психофизиологического состояния, принимается решение об обнаружении вредоносного воздействия неизвестного типа. Бинарный образ вредоносного объекта подается на вход блока вейвлет-анализа. Полученные параметры пополняют базу эталонов и передаются на вход нейросетевого классификатора для его дообучения.

2.3. Результаты экспериментальных исследований по обнаружению вредоносных конструкций в аудиопотоках. Рассмотрим процедуру обнаружения потенциально вредоносного контента в аудиопотоке на примере анализа фрагмента аудиозаписи суггестивного содержания (т.н. «громкий зикр») с параметрами: тип кодирования – PCM (*.wav), 16 бит, частота дискретизации – 44100 Гц. Его амплитудно-временное представление и бинарный образ изображены на рисунке 6.



а) б)

Рис. 6. Фрагмент аудиозаписи суггестивного содержания: а) амплитудно-временное представление; б) бинарный образ

Результат кадрирования бинарного потока, применения к нему вейвлет-преобразования на основе вейвлета Добеши 6-го порядка и получения аппроксимирующих коэффициентов (cA) представлен на рисунке 7.

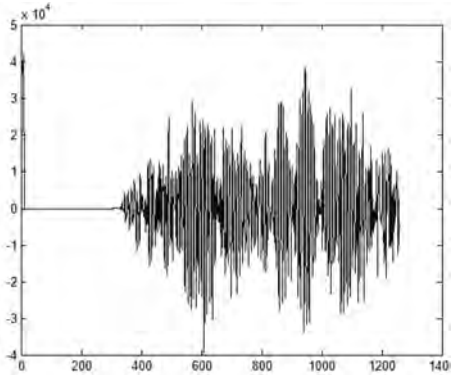


Рис. 7. Аппроксимирующие вейвлет-коэффициенты

Результат применения к полученным коэффициентам быстрого преобразования Уолша-Адмара представлен на рисунке 8. Расчетное значение показателя Херста для анализируемого аудиофрагмента: H=0,2.

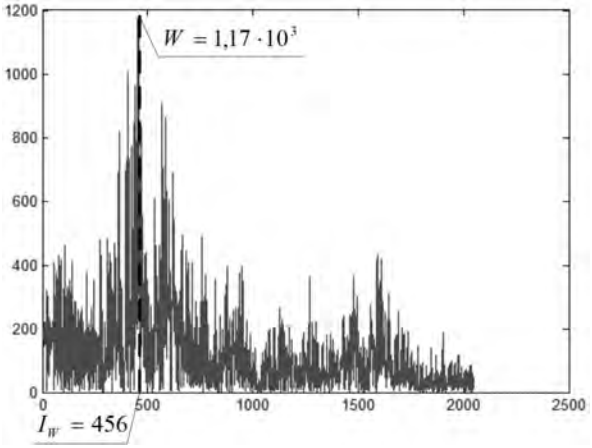


Рис. 8. КоэффициентыУолша-Адамара

Предварительно обученный нейросетевой классификатор с одним скрытым слоем нейронов характеризуется параметрами, представленными на рисунке 9.

Номер нейрона	Матрица весовых коэффициентов входов			Матрица весовых коэффициентов скрытого слоя нейронов	
1	-1,303	-3,417	-1,029	0,135	-0,731
2	0,370	3,821	0,148	-0,956	0,114
3	-2,649	3,642	-0,025	1,917	-1,655
4	0,567	2,547	-3,088	-0,196	-0,622
5	-1,655	-2,891	-1,822	0,127	-0,770
6	1,390	-0,384	-3,804	0,871	-0,439
7	1,415	-1,462	-2,346	-0,186	0,139
8	2,161	2,759	-1,663	0,351	-0,759
9	-1,178	-1,662	-3,690	1,238	-1,818
10	-1,419	2,375	-3,222	0,717	-1,012
11	-2,051	-2,361	2,866	-0,591	0,722
12	2,041	-1,788	2,896	-0,792	0,844
13	-4,571	-3,197	-0,625	-2,620	2,903
14	2,589	-2,685	-0,227	0,983	-0,247
15	2,316	4,122	-0,946	0,663	-1,161
16	2,865	0,232	2,928	-1,864	1,389
17	-3,911	-0,783	-1,499	0,141	-0,528
18	-1,324	-2,157	-4,723	-1,701	1,344
19	-2,510	2,215	1,807	-0,092	0,980
20	3,689	0,897	-1,279	0,765	-1,084

Рис. 9. Параметры нейросетевого классификатора

Отображение нейросетью полученных входных значений в признаковое пространство и решение задачи классификации продемонстрировано на рисунке 10.

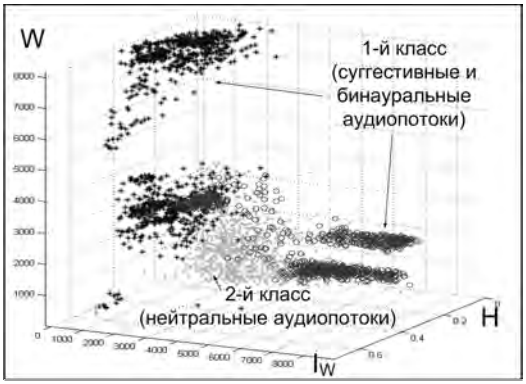


Рис. 10. Отображение нейросетью полученных входных значений в признаковое пространство

В приведенном примере веса выходных нейронов, соответствующих классам мультимедийного контента, приняли следующие значения: Y_1 (1-й класс, суггестивные мультимедийные объекты)=0,996;Y_2 (2-й класс, нейтральные мультимедийные объекты)=0,002, что полностью совпадает с априорной экспертной оценкой.

На рисунке 11 представлены результаты тестирования частных алгоритмов распознавания негативного контента в аудиопотоках на выборке общим объемом более 10000 фрагментов, содержавшей аудиообъекты суггестивного характера (зикры, мантры и т.д.), бинауральные воздействия, скрытые аудиовставки, а также аудиозаписи нейтрального содержания.

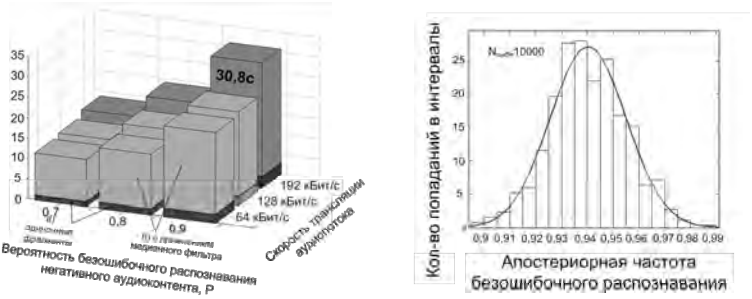


Рис. 11. Результаты тестирования частных алгоритмов распознавания негативного контента в аудиопотоках

При фиксированной апостериорной вероятности безошибочного распознавания P≥0,9 наибольшее время сбора и обработки информа-

ции ($\Delta t^{сб\&обр}$) относительно режима реального времени составило 30,8 с для аудиопотока в формате WAV качеством 192 кбит/с.

Практическая реализация разработанных алгоритмов была выполнена в виде аппаратно-программного комплекса, позволяющего осуществлять обнаружение потенциально вредоносных аудиоданных в различных форматах из Интернет-радиотрансляций, файлов с аудиоданными, звуковых дорожек файлов с видеоданными, звуковых дорожек Интернет-телевидения. Результаты фильтрации аудиопотока в режиме реального времени выводятся на экранную форму модуля обнаружения аудиовоздействий (рисунок 12).

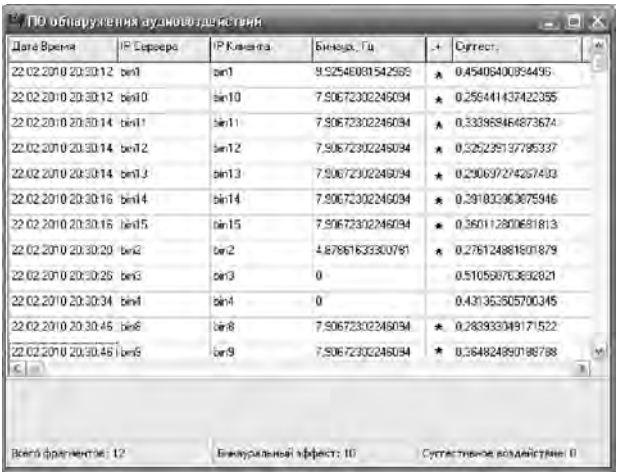


Рис. 12. Сигнализация об обнаруженных вредоносных свойствах аудиопотока

Столбцы экранной формы отражают информацию о времени и дате создания анализируемого файла, IP-адресе сервера и IP-адресе клиента между которыми осуществляется информационное взаимодействие, значение биоэффективной частоты (в Гц), на которой выявлено бинауральное воздействие, а также значение индекса суггестивности. В том случае, если распознаватель принимает решение о наличии в анализируемом аудиопотоке вредоносных вставок, то в столбце «.+.» таблицы, будет отображен символ «*».

2.4. Фильтрация текстов суггестивного содержания. Внушающее воздействие текста, помимо прочего, определяется особой упорядоченностью его элементов, сходной в некотором отношении со структурой фрактала. Подобная организация обеспечивает «естественность» восприятия и повышает эффективность внушения. Рассмотрим текст как линейно развертываемую во времени последовательность

фонетических единиц (звукобукв), каждая из которых может быть закодирована целым положительным числом. Для преобразования текста в численный ряд и его последующего компьютерного анализа могут быть использованы коды символов, определенные стандартом ASCII или Unicode.

Пусть текст представлен в виде целочисленного ряда длиной N. преобразуем его во временной ряд длиной N-1, исходя из логарифмических соотношений:

$$n=\ln\left(\frac{N_{i+1}}{N_i}\right),\ i=1,2,3,\ldots,N-1.$$

Среднее арифметическое для указанного ряда вычисляется по формуле:

$$M_k=\frac{1}{k}\cdot\sum_{i=1}^{k} n_i\,,$$

а накопленные отклонения как:

$$D_{k,n}=\sum_{i=1}^{k}(n_j-M_k),\ k=1,2,\ldots,i.$$

Тогда величина размаха определяется следующим образом:

$$R_k=\max\left(D_{k,n}\right)-\min\left(D_{k,n}\right),k\le n,$$

а среднеквадратическое отклонение:

$$S_k=\sqrt{\frac{1}{n}}\cdot\sum_{j=1}^{k}\left(n_j-m_k\right)^2.$$

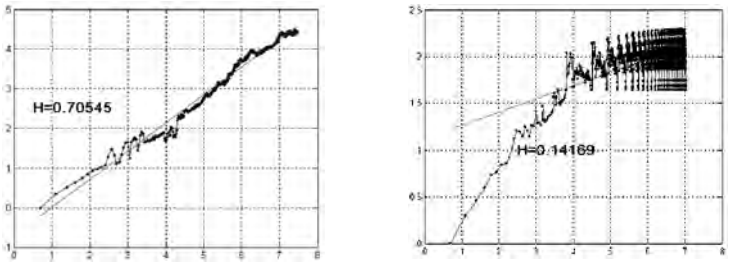
После этого каждый диапазон R_k нормируется путем деления на соответствующее значение S_k. Показатель Херста представляет собой тангенс угла наклона на графике зависимости $\ln(R_k/S_k)$ от $\ln(n)$.

В соответствии с проведенными экспериментальными исследованиями, для текстов, направленных на оказание внушения, значение оценки показателя Херста находится в области $0\le H\le 0{,}5$, что соответствует антиперсистентным рядам. Для нейтральных текстов информационного содержания значение оценки показателя Херста принадлежит области $0{,}5\ge H\ge 1$.

Помимо этого, графики, полученные в результате анализа суггестивных текстов методом нормированного размаха, обладают характерным общим свойством – наличием самоподобных периодически повторяющихся участков спад-подъем. Данный факт, а также низкие значения показателя Херста, являются отражением особой ритмической структуры текстов данного класса. Значения показателя Херста,

полученные в результате анализа внушающих текстов, тем ниже, чем короче формула внушения и чем чаще она повторяется в тексте.

Проведем сравнительный анализ текстов информационно-прагматического содержания: отрывка из романа «Отцы и дети» и лечебного заговора. На рисунке 13 представлены результаты оценки показателя Херста для указанных текстов.



а) б)

Рис.13. Оценка показателя Херста для текстов нейтрального и суггестивного содержания: а) для отрывка из романа «Отцы и Дети» И.С.Тургенева. H=0,71; б) для лечебного заговора. H=0,14

Полученные значения показателя H для большинства исследованных текстов, априорно отнесенных к классу суггестивных, не превышают 0,5, что соответствует антиперсистентным рядам. Помимо этого, графики, полученные в результате анализа суггестивных текстов методом нормированного размаха, обладают характерным общим свойством – наличием самоподобных периодически повторяющихся участков спад-подъем. Данный факт, а также низкие значения показателя Херста, являются отражением особой ритмической структуры текстов данного класса. Значения показателя Херста, полученные в результате анализа подобных текстов, тем ниже, чем короче формула внушения и чем чаще она повторяется в тексте. Существенным является тот факт, что указанные свойства проявляются при анализе текстов внушающего воздействия независимо от языка, на котором они составлены.

Проведенные экспериментальные исследования на больших выборках текстов позволили сформулировать решающее правило для определения принадлежности анализируемого текста к классу потенциально опасной информации в следующем виде:

$$U=\begin{cases}1, \text{ если } 0\le H\le 0{,}49\\ 0, \text{ если } 0{,}49<H\le 1'\end{cases}$$

где H– оценка показателя Херста.

К достоинствам описанного подхода следует отнести возможность перехода от интуитивной качественной оценки эмоционального и суггестивного оценивания текста к количественному представлению, что позволяет выявлять в автоматизированном режиме потенциально вредоносные текстовые документы.

3. Заключение. Таким образом, многообразие форм представления данных в современных информационных средах, способных содержать негативный контент, исключает возможность поиска эффективного распознающего механизма в рамках одной отдельно взятой математической модели. Представленная система реализует многомодельный подход к обнаружению потенциально вредоносного воздействия в информационных потоках.

Четкая классификация с последующим дообучением в рамках разработанной технологии осуществляется на основе нейронных сетей, обладающих такими преимуществами, как высокая скорость обработки входной информации, устойчивая работа при наличии ошибочных данных, высокая результативность решения задач классификации даже при малых объемах обучающих выборок.

Частные смысловые распознаватели наличия негативного контента в мультимедийных потоках данных построены на основе адаптированных алгоритмов, а именно: для текстовых данных – фрактального и фоносемантического анализа, для видеофайлов – быстрого преобразования Фурье (БПФ) и анализа дифференциальной яркости кадров, для аудиоданных – БПФ, вейвлетного преобразования на основе вейвлета Добеши и метода нормированного размаха Херста.

Для подтверждения вредоносного информационно-психофизиологического воздействия на потребителей мультимедийного контента используется нечеткий классификатор на основе аппарата размытых множеств. Наибольшая скорость выявления потенциально вредоносных информационных объектов достигается на уровне применения дообучаемого нейросетевого классификатора, а возможность обнаружения неизвестных ранее типов вредоносных воздействий обеспечивается применением нечеткого классификатора на основе аппарата размытых множеств.

Разработанное на основе изложенных методов и алгоритмов программное обеспечение целесообразно применять в местах логического подключения локальных вычислительных сетей к каналам сети Интернет, что позволит своевременно обнаруживать и при необходимости блокировать потенциально опасные мультимедийные объекты, не допуская их воздействия на конечного пользователя.

Литература

1. Военная доктрина Российской Федерации. Утверждена 26.12.2014 г.
2. Юсупов Р.М. Наука и национальная безопасность // СПб: Наука. 2011. 376 с.
3. Пояснительная записка "К проекту Федерального закона "Об информационно-психологической безопасности". URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=42885 (дата обращения: 20.01.2015).
4. Победители Конкурса лучших инновационных проектов в сфере науки и высшего профессионального образования Санкт-Петербурга в 2012 году. URL: http://knvsh.gov.spb.ru/closedcontests/view/15/ (дата обращения: 25.01.2015).
5. *Гнидко К.О., Горемыкин Д.В.* Исследование фрактальных свойств внушающих текстов в интересах защиты оператора автоматизированной системы военного назначения от вредоносного информационно-психофизиологического воздействия // Труды Военно-космической академии имени А.Ф.Можайского. 2009. С. 91–92.
6. *Гнидко К.О.* Воздействие динамических фрактальных структур в мультимедийных объектах на функциональное состояние человека // Труды II Всероссийской научно-практической конференции молодых ученых и специалистов «Инновационные подходы к развитию вооружения, военной и специальной техники». М.: ВА ГШ. 2012.
7. *Зелинский С.А.* Информационно-психологическое воздействие на массовое сознание // СПб.: Издательско-Торговый Дом "Скифия". 2008. 280 с.
8. *Ткачева Л.О.* Воздействие фрактальных динамических изображений на функциональное состояние человека // Вестник СПбГУ. 2010. Т. 12. № 2. С. 378–387.
9. *Касперски К.* Тайные рычаги подсознания. Методы психовизуальной атаки // Хакер. 2007. № 9(105). С. 134–137.
10. *Крапивенко А.В.* Технологии мультимедиа и восприятие ощущений // М.: Бином. Лаборатория знаний. 2009. 271 с.
11. *Гнидко К.О., Ломако А.Г., Пономарев Ю.А.* Особенности структурной организации суггестивных аудиопотоков // Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч1. Таганрог: ТИ ЮФУ. 2010. С. 203–205.
12. Рекламу Citroen запретили после эпилептического припадка у телезрителя. URL: http://medportal.ru/mednovosti/news/2012/01/19/epilepsy/ (дата обращения: 22.01.2015).
13. *Гнидко К.О. и др.* Обнаружение психоакустических воздействий на человека с учетом его индивидуальных физиологических особенностей // Материалы Всероссийской научно-практической конференции: «Теоретические и прикладные проблемы клинической психологии». СПб.: ЛГУ им.А.С.Пушкина. 2011. С. 421–426.
14. *Ростовцев Ю.Г., Гнидко К.О., Пилькевич С.В.* Генерация фрактальных сигналов заданной структуры для воздействия на функциональное состояние человека // Материалы IX межведомственной конференции «Научно-техническое и информационное обеспечение деятельности спецслужб». 2012. Т. 8. С. 58–63.
15. *Замарин А.И., Зайцев И.Е., Карелов И.Н.* Синтез нейросетевого алгоритма идентификации линейных корректирующих кодов // Известия ВУЗов – Приборостроение. 1998. Т. 41. № 8.

References

1. Voennaya doktrina Rossijskoj Federacii. [Military doctrine of Russian Federation]. 2014. (In Russ.).

2. Yusupov R.M. *Nauka i nacional'naja bezopasnost'* [Science and national security]. SPb: Nauka. 2011. 376 p.
3. Poyasnitel'naya zapiska «K proektu Federal'nogo zakona «Ob informacionno-psixologicheskoj bezopasnosti» [Explanatory note «To the draft of Federal Law on information-psychological security»]. Available at: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=42885 (accessed: 20.01.2015). (In Russ.).
4. Pobediteli Konkursa luchshix innovacionnyx proektov v sfere nauki i vysshego professional'nogo obrazovaniya Sankt-Peterburga v 2012 godu [Winners of the innovative projects competition in the field of science and higher professional education in Saint-Petersburg in 2012]. Available at: http://knvsh.gov.spb.ru/closedcontests/view/15/ (accessed: 25.01.2015). (In Russ.).
5. Gnidko K.O., Goremykin D.V. [Study of fraclal properties of suggestive texts in order to protect an operator of a military automated system from harmful information-psychological affects]. *Trudy Voenno-kosmicheskoj akademii imeni A.F.Mozhajskogo – Proceedings of Mozhaisky Military Space Academy*. Saint-Petersburg. 2009. pp. 91–92. (In Russ.).
6. Gnidko K.O. [Impacts of dynamic fractal structures in multimedia objects on the functional state of a person]. *Trudy II Vserossijskoj nauchno-prakticheskoj konferencii molodyh uchenyh i specialistov «Innovacionnye podhody k razvitiju vooruzhenija, voennoj i special'noj tehniki»* [Proceedings of II All-Russian scientific-practical conference of young scientists and specialists «Innovative approaches to the development of weapons, military and special equipment»]. M.: VA GSh. 2012 (In Russ.).
7. Zelinskij S.A. *Informacionno-psixologicheskoe vozdejstvie na massovoe soznanie* [Informational and psychological impact on the public consciousness]. SPb.: Izdatel'sko-Torgovyj Dom "Skifija". 2008. 208 p. (In Russ.).
8. Tkacheva L.O. [Impact of fractal dynamic images on the functional state of the person]. *Vestnik Sankt-peterburgskogo gosudarstvennogo universiteta – Herald of the St. Petersburg State University*. 2010. vol. 12. no. 2. pp 378–387. (In Russ.).
9. Kasperski K. [Secret levers of subconscious. Methods of psychovisual attack]. *Haker – Xaker*. 2007. vol. 9(105). pp. 134–137. (In Russ.).
10. Krapivenko A.V. *Texnologii mul'timedia i vospriyatie oshhushhenij* [Multimedia technology and the perception of sensations]. Moscow: Binom. Laboratoriya znanij, 2009. 271 p. (In Russ.).
11. Gnidko K.O., Lomako A.G., Ponomarev Yu.A. [Special features of the structural organization of suggestive audio streams]. *Materialy XI Mezhdunarodnoj nauchno-prakticheskoj konferencii «Informacionnaja bezopasnost'». Ch. 1* [Proceedings of the XI International scientific-practical conference. «Information Security». Part 1]. Taganrog: TI SFU. 2010. pp. 203–205. (In Russ.).
12. Reklamu Citroen zapretili posle e'pilepticheskogo pripadka u telezritelya [Citroen commercial banned after an epileptic seizure of the viewer]. Available at: http://medportal.ru/mednovosti/news/2012/01/19/epilepsy/ (accessed: 22.01.2015). (In Russ.).
13. Gnidko K.O. et al. [Detection of psychoacoustic effects on humans, taking into account their individual physiological characteristics]. *Materialy Vserossijskoj nauchno-prakticheskoj konferencii: «Teoreticheskie i prikladnye problemy klinicheskoj psihologii»* [Proceedings of the All-Russian Scientific-Practical Conference «Theoretical and applied problems of clinical psychology SPb.: LGU im.A.S.Pushkina. 2011. pp. 421–426. (In Russ.).
14. Rostovcev Yu.G., Gnidko K.O., Pil'kevich S.V. [Generation of fractal signals of given structure to influence the functional state of the person]. *Materialy IX*

mezhvedomstvennoj konferencii «Nauchno-tehnicheskoe i informacionnoe obespechenie dejatel'nosti specsluzhb» [Proceedings of the IX interdepartmental conference «Scientific and technical and information support of special services»]. 2012. vol. 8. pp. 58–63. (In Russ.).

15. Zamarin A.I., Zajcev I.E., Karelov I.N. [Synthesis of neural network algorithm for identification of linear error-correcting codes]. *Izvestiya VUZov Priborostroenie – Proceedings of the universities instrument engineering*. 1998. vol. 41. no. 8. (In Russ.).

Гнидко Константин Олегович — к-т техн. наук, докторант, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: информационно-психологическая безопасность, распознавание образов, извлечение знаний из неструктурированных массивов данных. Число научных публикаций — 27. greeny598@gmail.com; ул. Ждановская, 13, 197198, г. Санкт-Петербург; р.т.: +7(812) 237-19-60.

Gnidko Konstantin Olegovich — Ph.D., doctoral student, Mozhaisky Military Space Academy. Research interests: information-psychological security, image recognition, data mining. The number of publications — 27. greeny598@gmail.com; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812) 237-19-60.

Ломако Александр Григорьевич — д-р техн. наук, профессор кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: информационная безопасность, теоретическое и системное программирование, синтез и верификация корректности моделей программ. Число научных публикаций — 250. lomako_ag@mail.ru; ул. Ждановская 13, 197198, Санкт-Петербург; р.т.: +7(812) 237-19-60

Lomako Aleksandr Grigor'evich — Ph.D., Dr. Sci., professor of system for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: information security, theoretical and system programming, synthesis and verification of program models. The number of publications — 250. lomako_ag@mail.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812) 237-19-60.

РЕФЕРАТ

Гнидко К.О., Ломако А.Г. **Контроль потенциально опасного информационно-психологического воздействия на индивидуальное и групповое сознание потребителей мультимедийного контента.**

В современных подходах к обеспечению системной безопасности наблюдается существенный перекос в сторону технических элементов защищаемых систем. Вместе с тем, международный масштаб и стратегический характер приобретает проблема защиты человеческой психики от потенциально вредоносного мультимедийного контента.

В настоящей работе кратко изложены результаты теоретических и практических исследований в области построения автоматизированной системы мониторинга и фильтрации мультимедийных данных от контента, способного нанести вред психофизиологическому состоянию пользователей.

Представленная система реализует многомодельный подход к обнаружению потенциально опасных объектов в аудио-, видеопотоках и текстовых массивах. Для оперативного обнаружения сигнатур вредоносных объектов применяется дообучаемый нейросетевой классификатор прямого распространения. Частные смысловые распознаватели построены на основе алгоритмов фрактального и фоносемантического анализа, быстрого преобразования Фурье и анализа дифференциальной яркости кадров, вейвлетного преобразования и метода вычисления нормированного размаха. Для подтверждения факта вредоносного информационно-психофизиологического воздействия на потребителей используется нечеткий классификатор на основе аппарата размытых множеств.

Разработанное на основе изложенных методов и алгоритмов программное обеспечение может применяться в местах логического подключения локальных вычислительных сетей к каналам сети Интернет, что позволит своевременно обнаруживать и при необходимости блокировать потенциально опасные мультимедийные объекты, не допуская их воздействия на конечного пользователя.

SUMMARY

Gnidko K.O., Lomako A.G. **Monitoring of Potentially Dangerous Information-Psychological Affect on Individual and Group Consciousness of Multimedia Content Consumers.**

In the modern approach to system safety ensuring there is a significant bias towards technical elements of the systems being protected. At the same time, the problem of protection of the human psychics from potentially harmful media content currently has the international scope and strategic nature.

This paper summarizes the results of theoretical and practical study in the field of developing of automated systems for monitoring and filtering of multimedia data from the content that can harm psychophysiological states of its consumers.

This system implements a multi-model approach to the detection of potentially dangerous objects in the audio, video streams and texts. The direct distribution neural network classifier is used for prompt detection of malicious objects' signatures. Particular content-focused detectors use algorithms based on fractal methods, phonosemantic analysis, fast Fourier transform, differential frame brightness, wavelet transform and the method of computation of the normalized amplitude. A classifier based on fuzzy sets does confirmation of the fact of harmful effect.

The software developed on the basis of the methods and algorithms described can be used in points of logical connection of local area networks to the Internet network channels. It will enable timely detection and, if necessary, blocking of potentially dangerous multimedia objects, avoiding their impact on the end user.

УДК 004.75

С.В. Новиков, В.М. Зима, Д.В. Андрушкевич

ПОДХОД К ПОСТРОЕНИЮ ЗАЩИЩЕННЫХ РАСПРЕДЕЛЕННЫХ СЕТЕЙ ОБРАБОТКИ ДАННЫХ НА ОСНОВЕ ДОВЕРЕННОЙ ИНФРАСТРУКТУРЫ

Новиков С.В., Зима В.М., Андрушкевич Д.В. **Подход к построению защищенных распределенных сетей обработки данных на основе доверенной инфраструктуры.**
Аннотация. Предлагается подход к построению распределенных вычислительных сетей и организации защиты информации с использованием доверенной инфраструктуры. Отсутствие единой высокоуровневой платформонезависимой модели организации вычислительного процесса и защиты информации, а также необходимых механизмов, реализующих модель на уровне ее практического внедрения, порождает множество несогласованных между собой частных решений и приводит к неоправданному нагромождению технических и программных средств организации обработки информации в автоматизированных системах. Поэтому эволюционно развивающиеся системы, функционирующие на разных платформах в настоящее время, требуют внедрения доверенных решений в области защиты информации.
Ключевые слова: программные средства защиты информации, автоматизированная система, гетерогенная сеть, операционная система, доверенная среда, доверенная инфраструктура, прозрачное шифрование.

Novikov S.V., Zima V.M., Andrushkevich D.V. **Approach to Building Secure Distributed Networks of Data Processing based on Trusted Infrastructure.**
Abstract. An approach for building distributed computing networks and the organization of information security using trusted infrastructure is proposed. The lack of a single high-level platform-independent model of computing and information security, as well as the necessary mechanisms that implement the model at the level of its practical implementation raises many uncoordinated private decisions and leads to unnecessary pile of hardware and software organization of information processing of automated systems. Therefore, the evolutionary developing systems operating on different platforms currently require the implementation of trusted solutions in the field of information security.
Keywords: software data protection, automated system, a heterogeneous network, operating system, trusted environment, trusted in infrastructure, transparent encryption.

1. Введение. Информационные технологии сегодня развиваются столь стремительно, что уже трудно выделить сферу человеческой деятельности, в которой они не были бы востребованы. Любая современная организация, даже если она и не имеет удаленных филиалов, вовлекается в общий круг пользователей информационных услуг, в обязательном порядке использует глобальные коммуникации, имеет собственное виртуальное представительство в Сети, работает с современными средствами обмена данными в рамках собственного офиса. "Фактор Сети" незримо присутствует в управлении любого уровня и степени важности. В связи с этим проблема вовлечения Интернета в круг интересов любой организации, имеющей территориально распре-

деленную структуру, встает все острее. Не столько с точки зрения целесообразности такого шага, сколько с позиций обеспечения информационной безопасности, поскольку Сеть сегодня воспринимается часто как "агрессивное начало". Многие информационные системы являются уязвимыми к так называемым "внешним воздействиям". Сегодня уже пришло понимание того факта, что электронные средства хранения и передачи информации оказались даже более уязвимыми, чем обычные бумажные, так как их можно не только уничтожить, но и незаметно для владельца скопировать или изменить. Именно это является особо опасным для любой структуры.

Теми же проблемами обладают и каналы обмена данными. Мало того, что информация, в них циркулирующая, является по сути своей открытой и доступной для злоумышленника, так еще и сами средства обмена предоставляют последним возможность вторжения во внутренние ресурсы информационных систем. Понимая всю опасность, связанную с хранением и передачей данных по каналам связи, многие предприятия в мире расходуют на решение проблемы обеспечения информационной безопасности немалые средства. В России обеспечение информационной безопасности тоже превращается постепенно в общегосударственную проблему, так как "агрессивность" среды растет, внешние угрозы становятся все более изощренными. И хотя "фактор Сети" несколько преувеличен, опыт многих успешных внешних атак указывает на их немалую "внутреннюю" составляющую, тем не менее, игнорирование указанной проблемы может привести к невосполнимым потерям в управляемости каждой отдельно взятой структуры [1].

2. Проект доверенной инфраструктуры. Наличие развитой сетевой инфраструктуры на объектах гетерогенных, территориально распределенных автоматизированных систем (АС) является необходимым, но не достаточным условием создания интегрированного информационно-вычислительного пространства. Отсутствие единой высокоуровневой платформонезависимой модели организации вычислительного процесса и защиты информации, а также необходимых механизмов, реализующих модель на уровне ее практического внедрения, порождает множество несогласованных между собой частных решений и приводит к неоправданному нагромождению технических и программных средств организации обработки информации на объектах автоматизированных систем. Поэтому в настоящее время актуальными являются проблемы

разработки и внедрения, эволюционно развивающихся систем, функционирующих на различных платформах.

Одной из ключевых проблем создания доверенной среды в построении распределенных вычислительных сетей является решение вопроса о принципиальной допустимости и способах применения, в общем случае, недоверенных программно-аппаратных средств и компонентов в его составе. Объекты могут оснащаться разнородными аппаратно-программными платформами (АПП), функционирующими в составе защищенных центров обработки данных (ЦОД), выделенных специализированных серверов, а также рабочих станций. Неизбежным следствием при этом являются две возникающие задачи: интеграции разнородных информационно-вычислительных ресурсов и реализации унифицированной модели защиты процессов и данных в составе гетерогенных объектов. В статье предлагаются возможные технологии доверенной инфраструктуры, которая базируется на основе включения в АПП доверенного общесистемного программного обеспечения (ОСПО), в состав которого, наряду с компонентами интеграции разнородных приложений, обмена данными и управления вычислительным процессом, входят программные средства защиты информации. Также предложены возможные требования к организации доверенной среды путем создания доверенной инфраструктуры распределенных сетей обработки данных. Даны необходимые рекомендации по организации доверенной инфраструктуры критически важных объектов РФ.

На рисунке 1 представлена концепция доверенной инфраструктуры защищенных распределенных сетей. Таким образом, предлагается инфраструктура, которая будет состоять из контура, в состав которого будут входить: доверенный контроль, доверенный канал связи, доверенные сегменты распределенной сети, доверенные АРМ с различными платформами ОС, доверенное специальное программное обеспечение с НДВ, доверенная система шифрования, доверенная транспортная среда, доверенные администраторы всех сегментов сети, администратор доверенной инфраструктуры.

Для организации защиты информации на различных узлах распределенных сетей обработки данных предлагается введение данного контура с администраторским управлением на каждом сегменте контура, под управлением администратора доверенной инфраструктуры.

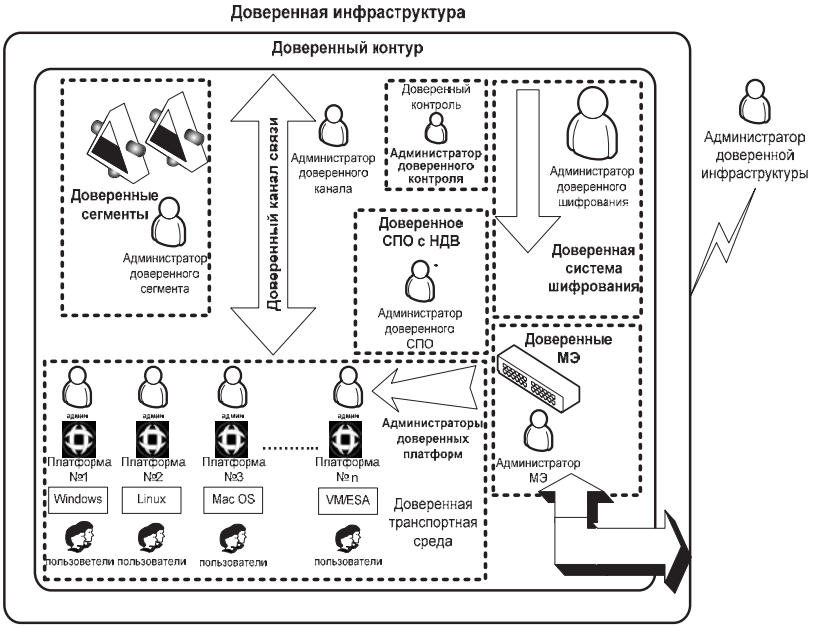


Рис. 1. Проект доверенной инфраструктуры защищенных распределенных сетей

В данной статье авторы предлагают рассмотреть некоторые из подходов защиты сегментов доверенной инфраструктуры, а именно:

- организацию защиты информации в доверенном контуре на различных платформах ОС;
- доверенные элементы распределенной информационной системы;
- двухуровневое шифрование в доверенной инфраструктуре;
- организация защиты контура в доверенной инфраструктуре.

3. Организация защиты информации в доверенном контуре на различных платформах ОС. Реализация унифицированных средств защиты в общем случае может достигаться применением организационных, технических и программных решений, а также их комбинацией. Причем применение технических средств защиты информации, разработанных для неоднородных программно-аппаратных платформ, в силу их ориентации на конкретные (специфические) интерфейсы используемого оборудования не может рассматриваться в качестве унифицированного решения проблемы. Поэтому унифицированные решения следует формировать на базе программных средств защиты (ПСЗ) информационных ресурсов, которые могут являться дополнением к уже

имеющимся в составе системы аппаратным (техническим) и программно-аппаратным средствам, а также осуществляемым мероприятиям организационного характера. Очевидно, что ПСЗ должны обеспечивать управление безопасностью при операциях с информационными объектами высших уровней абстракции (приложений уровня конечных пользователей, систем обмена данными, документооборота, приложений баз данных) [2].

Широко используемые в настоящее время программные компоненты защиты информации либо встраиваются в состав различных операционных систем (ОС) — встроенные ПСЗ — непосредственно разработчиками, либо подменяют собой стандартные обращения к объектам защиты (файлам, устройствам, исполняемым модулям) уровня ОС со стороны прикладных процессов (внешние ПСЗ). Недостатком применения встроенных ПСЗ является существенная зависимость построенной модели защиты от частных особенностей реализации разработчиком ОС средств управления безопасностью. При применении внешних ПСЗ возникает необходимость стабилизации (неизменности программной среды) конкретной версии используемой ОС. Поэтому для защиты объектов такого уровня должны использоваться унифицированные ПСЗ, служащие дополнением к недостающим механизмам защиты на уровне разнородных операционных систем и сетевых приложений [3].

Определим место унифицированных ПСЗ в общей архитектуре программного обеспечения объекта АС, имея в виду, что рассматриваемые ПСЗ предназначены для реализации унифицированной модели защиты в условиях изначальной неоднородности множества программных и технических компонентов, составляющих корпоративную сеть организации. В этих условиях унификация модели защиты на уровне разнородных элементов данного множества может достигаться средствами "промежуточного" слоя (middleware). Он образуется распределенными однородными (с точки зрения интерфейсов и выполняемых функций) компонентами общесистемного программного обеспечения (ОСПО), функционирующими под управлением всех операционных систем (базовых ОС), используемых в составе объекта АС. Указанное свойство является принципиальным отличием данного решения от большинства известных реализаций.

Перейдем от рассмотрения проблем защищенного функционирования отдельных средств вычислительной техники (СВТ) к проблемам защиты коммуникаций. Здесь в первую очередь следует отметить недостаточность применяемых в настоящее время средств фильтрации входящих/исходящих потоков данных между узлами вычислитель-

ных на сетевом уровне без адекватного решения проблемы безопасного взаимодействия конечных абонентов/приложений на прикладном уровне с использованием различных (разнородных) протоколов передачи данных [4]. В результате для гетерогенных корпоративных вычислительных сетей администратор безопасности, располагает набором разнородных инструментальных средств, в общем случае неадекватных решаемой проблеме.

Попытки практической реализации комплекса мер по обеспечению защиты информации на объекте путем использования предлагаемых программных продуктов различных классов наталкиваются на ряд противоречий концептуального характера. Они преимущественно связаны с неадекватностью имеющегося в распоряжении администратора безопасности набора инструментальных средств решаемым задачам по отображению избранной модели защиты на множество разнородных объектов вычислительной техники, сетевых средств и программного обеспечения различных производителей. Например, имеющиеся различия в используемых понятиях и формулируемых критериях информационной безопасности на уровне компьютерной лексики и терминов нормативных (регламентирующих) документов, определяющих политику безопасности для АС, создают проблему адекватного отображения нормативного уровня на уровень вычислительных систем. На рисунке 2 показана организация доверенной (защищенной) общесистемной транспортной среды в доверенной инфраструктуре [4].

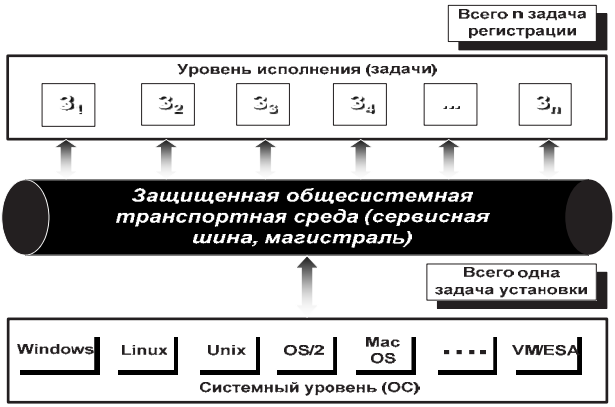


Рис. 2. Доверенная транспортная среда

Кроме того, существуют конструктивные различия в базовых средствах защиты информации уровня операционных систем и сетевых приложений различных производителей (IBM, Microsoft, SUN и др.),

отсюда — дополнительные сложности в реализации непротиворечивой модели защиты для гетерогенной вычислительной среды.

Необходимо отметить, что даже при проектировании вычислительных сетей, состоящих из однородного программного обеспечения и технических средств, использование одних только базовых средств защиты на уровне выбранной ОС оказывается недостаточным. Это происходит из-за наличия на уровне АС новых общесистемных свойств, затрагивающих принципы адресации ее элементов (системы как единого целого, объекта в составе территориально распределенной системы, ЛВС в составе объекта, вычислительного модуля в составе ЛВС, прикладной задачи в составе модуля), выбора атомарных единиц обмена данными, перечня защищаемых ресурсов и т. д. [5].

При непосредственном использовании компонентов защиты уровня отдельной ОС для решения задач создания территориально распределенных корпоративных вычислительных сетей и последующей обработки информации в контуре доверенной инфраструктуры возникают противоречия, к основным из которых можно отнести следующие:

1) базовые средства защиты информации на уровне ОС обеспечивают подключение пользователя к ресурсам отдельной ЭВМ, являющейся в общем случае лишь элементом в составе ЛВС (но не объекта в составе автоматизированной системы). В то же время на уровне АС необходим дополнительный, более важный с точки зрения вопросов безопасности этап: подключение пользователя-должностного лица к ресурсам информационной системы в соответствии с принятыми в АС соглашениями по адресации объектов, АРМ или отдельных программ. Это может относиться к отдельной программе, группе программ в АРМ, пользователю, группе пользователей и объекту в целом;

2) базовые средства защиты информации с точки зрения системы хранения на уровне ОС рассматривают файл в качестве элементарной единицы защиты данных. В то же время на корпоративном уровне АС единицами системы электронного документооборота являются формализованные сообщения, а также именованные в соответствии с общесистемными классификаторами документы. И то, и другое, как правило, не хранится в системе в виде отдельных файлов, более того, различные АС используют свои (как правило, с применением СУБД) специфические методы отображения множества элементов системы документооборота на файловые структуры;

3) средства защиты информации в составе ОС управляют доступом на уровне реальных (физических) устройств, подключенных к данному средству вычислительной техники. В то же время на уровне вычислительной сети объекта АС устройствами, как правило, являются

логические понятия. К ним относятся направления и каналы связи, распределенные хранилища данных, группы пользователей (например, «Администратор», «Группа (отдел) разработки приложений» и т.д.), объекты АС в целом;

4) ОС статически маршрутизирует (направляет) потоки данных на уровне отдельного средства вычислительной техники. В то же время на уровне объекта АС, как правило, требуется динамическая маршрутизация между всеми вычислительными средствами объекта, а также между объектами АС в целом с учетом возможности логической привязки пользователей (должностных лиц) к их рабочим местам и перенаправления информационных потоков в зависимости от складывающихся обстоятельств;

5) администрирование вычислительного процесса на уровне ОС ориентировано, прежде всего, на данное СВТ, реже — на группу однородных СВТ, в то время как на уровне объекта АС требуется администрирование приложений всей неоднородной вычислительной сети, состоящей из главных вычислительных модулей, специализированных серверов ЛВС, выделенных рабочих мест (АРМ) и функционирующих в их составе приложений (программ), а также каналов связи с контролем их работоспособности в составе системы.

На рисунке 3 представлена работа узла в доверенном контуре доверенной инфраструктуры.

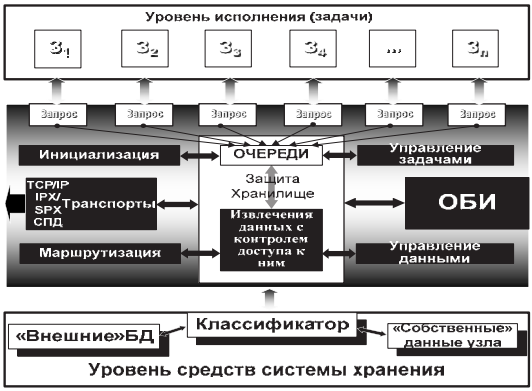


Рис. 3. Организация вычислительного процесса на доверенном узле

Отмеченные противоречия и дополнительные требования к системе защиты обусловливают необходимость дополнения базовых средств защиты информации уровня отдельных ОС некоторыми унифицированными средствами организации вычислительного процесса и управления обработкой информации на уровне объекта АС, инвариантными по от-

ношению к определенным операционным системам и обеспечивающими совместное функционирование "унаследованного", актуального и перспективного программного обеспечения [6].

4. Доверенные элементы распределенной информационной сети. На сегодняшний день основным принципом построения крупных информационных систем является объединение территориально распределенных ЛВС и отдельных компьютеров через сеть Интернет в общую распределенную информационную систему (РИС). Пользователи работают в едином информационном пространстве, разделяемом на зоны с различным набором прав на использование сервисов.

Как правило, используемые программно-аппаратные средства защиты информации разделяются на три категории:

- средства обеспечения доверенной загрузки;
- средства обеспечения доверенности компьютера;
- средства обеспечения защищенного соединения.

Процедуру загрузки, защищенную таким образом, назовем доверенной загрузкой операционной системы.

К средствам обеспечения доверенности компьютера относятся программно-аппаратные комплексы, включающие средства обеспечения доверенной загрузки, СЗИ НСД, средства обеспечения доступа к ресурсам, а также антивирусные средства.

На практике построение защищенных распределенных информационных систем имеет следующие особенности:

- выполнение требований политики ИБ, в частности запуск разрешенных для выполнения задач в рамках изолированной программной среды, необходимо контролировать как для локального, так и для удаленного (подключаемого) сегмента РИС, что не всегда реализуемо на практике;
- для обеспечения конфиденциальности, целостности и доступности данных с возможностью применения ЭЦП необходимо использовать сертифицированные ОС, СЗИ НСД и СКЗИ, а также обеспечить аттестацию рабочих мест пользователей и всей РИС;
- сертифицированные ОС имеют ограничения на установку и обновление компонентов ОС и прикладного ПО и зачастую предоставляют недостаточный функционал;
- стоимость сертифицированных ОС, СЗИ НСД и СКЗИ, а также процедуры аттестации часто превышает стоимость компьютерной техники и прикладного ПО на рабочем месте пользователя.

Таким образом, обеспечить защиту РИС, в частности государственных автоматизированных систем, средствами доверенной вычислительной среды на основе резидентного компонента безопасности в принципе возможно (хотя это требует значительных затрат и связано с рядом

сложностей), но для рабочих мест служащих и персональных компьютеров граждан, которые планируют работать с сервисами государственных автоматизированных систем оказывается слишком сложной.

В настоящее время существует принципиально новая концепция доверенного сеанса связи удаленных пользователей с сервисами доверенной среды РИС через сеть Интернет, развивающая концепцию доверенной вычислительной среды на основе резидентного компонента безопасности. Суть концепции состоит в предоставлении пользователю достаточных условий для защищенной работы с сервисами доверенной РИС на определенный период времени, при выполнении которых не требуется построение изолированной программной среды на компьютере пользователя, но в то же время не снижается класс защищенности РИС.

После выполнения описанных процедур по созданию доверенной среды средствами контроля целостности ОСПО из конфигурационных файлов базовой ОС извлекаются контрольные суммы зарегистрированных приложений и помещаются в специальный раздел (журнал) хранилища данных, доступный (только в режиме просмотра) администратору безопасности. В начале каждого сеанса работы, а также по особому регламенту в процессе работы средства контроля целостности ОСПО обеспечивают проверку наличия доверительной среды. При отрицательном результате производится автоматическая запись о факте нарушения целостности в журнал контроля целостности и завершение работы ядра ОСПО, а также всех зарегистрированных в доверительной среде приложений. Продолжение работы возможно только после восстановления доверенной среды.

Информация, относящаяся к работе ПСЗ ОСПО (пароли, журналы, эталонные значения контрольных сумм и т. д.), должна храниться в специализированном хранилище БД ОСПО и быть недоступной для непосредственного просмотра или модификации. Попытка атаки на уровне базовой ОС неминуемо ведет к нарушению доверенной среды, блокирует работу ядра ПСЗ и как следствие — доступ извне к защищаемой информации [7].

Основной проблемой, с которой сталкиваются специалисты при решении задач построения системы защиты на объектах АС, как указывалось выше, является необходимость перехода к единой и безопасной вычислительной среде, доверенной инфраструктуры в условиях неоднородности программно-аппаратных средств, а также наличия в ряде случаев "унаследованных" систем. При решении этой задачи, как правило, невозможно одновременно полностью отказаться от "старых" платформ. Поэтому необходимо построить всю систему таким образом, чтобы исключить или минимизировать возможность реализации угроз, возникающих из-за использования недоверенных "унаследо-

ванных" платформ.

В доверенной инфраструктуре также должны решаться задачи по защите информации от несанкционированного доступа. Для нейтрализации как явных, так и скрытых угроз в распределенных АС при участии авторов был разработан специальный программно-аппаратный комплекс защиты информации «Ключ-Ш» (далее – СПАК), обеспечивающий построение распределенных АС критической инфраструктуры.

5. Двухуровневое шифрование в доверенной инфраструктуре. Основой функциональной архитектуры СПАК являются подсистемы глобального шифрования и усиленной аутентификации, ориентированные на решение следующих групп задач [8]:

– двухуровневое «прозрачное» шифрование информации на жестких дисках АРМ;

– логическая привязка съемных носителей (Flash, CD, DVD) к заданной группе автономных АРМ за счет «прозрачного» шифрования информации на этих съемных носителях по закрытому ключу;

– использование электронных идентификаторов ruToken для аутентификации пользователей, а также хранения, переноса и резервирования ключевой информации. На рисунке 4 представлена функциональная архитектура доверенной системы шифрования.

Рис. 4. Функциональная архитектура доверенной системы шифрования

Двухуровневое «прозрачное» шифрование информации на жестких дисках АРМ предполагает наличие двух уровней:

– первый уровень — глобальное шифрование информации по секторам жестких дисков;

– второй уровень — шифрование виртуальных дисков, формируемых на основе информации из файла-контейнера.

Глобальное «прозрачное» шифрование информации в системном разделе жесткого диска АРМ выполняется по закрытому ключу, общему для всех зарегистрированных пользователей. При «прозрачном» шифровании логических и виртуальных дисков предполагается использование индивидуальных ключей.

Для управления «прозрачно» шифруемыми виртуальными дисками предусмотрены такие важные функции, как:

– поддержка возможности переноса файла-контейнера с зашифрованным виртуальным диском с одного защищенного АРМ на другой;

– подключение зашифрованного виртуального диска по сети, в процессе работы с которым передаваемая информация шифруется в режиме реального времени, и по сети передаются только зашифрованные информационные пакеты;

– перенос ключей шифрования виртуальных дисков в аппаратно защищенной памяти электронных идентификаторов ruToken с возможностью доступа к этим ключам только после предъявления соответствующего PIN-кода.

Кроме того, учтена необходимость логической привязки съемных носителей (Flash, CD, DVD) к заданной группе автономных АРМ за счет «прозрачного» шифрования информации на этих съемных носителях по закрытому ключу. Пользователи заданной группы автономных АРМ могут передавать зашифрованные носители для работы с ними с одного АРМ на другой. Вне заданной группы автономных АРМ информация на зашифрованных носителях будет недоступна.

Высокая скорость и стойкость шифрования обеспечивается за счет следующих факторов, положенных в основу построения используемых и запатентованных алгоритмов:

– перенос всех вычислений, требующих больших временных ресурсов, на этап инициализации криптографической подсистемы, который выполняется только в начале сеанса работы пользователя;

– зависимость операций криптографического преобразования не только от рабочих ключей, но и от преобразуемых данных и промежуточных результатов преобразования, что повышает степень псевдослучайности в алгоритме непосредственных преобразований;

– снижение сложности алгоритма непосредственных криптографических преобразований за счет повышения его стойкости.

Для фиксированного уровня стойкости используемые алгоритмы обеспечивают более низкую сложность алгоритмов непосредственного криптографического преобразования информации. За счет этого достигается более высокая скорость шифрования.

Для аппаратной поддержки процесса аутентификации и хранения ключей шифрования в составе СПАК используется сертифицированный электронный идентификатор ruToken, закрепляемый за каждым пользователем.

При формировании архитектуры СПАК изначально учитывались основы реализации технологических схем защищенной автоматизированной обработки информации:

– управление ключами шифрования на основе инфраструктуры открытых ключей;

– обеспечение подлинности электронных документов за счет формирования и проверки их электронных подписей;

– обеспечение конфиденциальности электронных документов за счет их шифрования.

Построение подсистемы управления ключами шифрования выполнялось исходя из следующих требований:

– должна быть обеспечена гибкость распределения ключей шифрования информации;

– подсистема управления ключами не должна требовать доверия взаимодействующих друг с другом сторон;

– скорость криптографических преобразований должна обеспечивать шифрование информации в режиме реального времени.

Реализация первых двух требований выполнена за счет асимметричного принципа построения ключей верхнего уровня, а реализация третьего требования – за счет использования ключей скоростного симметричного шифрования.

В подсистеме управления ключами шифрования СПАК используются следующие базовые уровни ключей:

– первичные пары асимметричных ключей (первичные ключи), включая личные ключи пользователей, формируемые в соответствии с российским стандартом цифровой подписи ГОСТ Р 34.10 и используемые для распределения ключей, а также выработки на основе цифровой подписи вторичных ключей симметричного шифрования;

– вторичные ключи симметричного шифрования (вторичные ключи), формируемые по алгоритму Диффи–Хеллмана на основе первичных пар асимметричных ключей, и используемые для шифрования носителей информации и информационного трафика;

– ключи доступа, используемые для защиты первичных ключей, связок ключей пользователя, а также базы данных СПАК.

Первый уровень ключей специального преобразования информации за счет асимметричного принципа построения обеспечивает гибкость распределения ключей и не требует доверия взаимодействующих друг с другом сторон.

Второй уровень ключей специального преобразования информации за счет симметричного принципа построения и использования скоростных алгоритмов криптографических преобразований обеспечивает шифрование информации в режиме реального времени.

Третий уровень ключей специального преобразования информации за счет многоуровневого шифрования обеспечивает надежную защиту ключей первых двух уровней.

Для каждого пользователя в СПАК по ГОСТ 34.10 генерируется личная пара асимметричных ключей, которая хранится в профиле пользователя в базе данных (БД) системы защиты. Закрытый ключ этой пары ключей зашифрован по ключу, генерируемому по специальному алгоритму (алгоритму SSE2) на основе пароля (PIN-кода) этого пользователя. Вводимый пароль (PIN-код) пользователя используется для расшифрования закрытого ключа личной пары асимметричных ключей. Открытый ключ личной пары асимметричных ключей подписан по закрытому первичному ключу АРМ.

Аутентификация пользователей в СПАК основана на использовании цифровой подписи. Для аутентификации пользователя модуль управления БД СПАК направляет агенту аутентификации запрос на цифровую подпись сгенерированного случайного числа, формируемую на основе личного закрытого ключа этого пользователя. Если пароль (PIN-код) был введен пользователем неправильно, то агент аутентификации не сможет правильно расшифровать личный закрытый ключ пользователя, а, следовательно, не сможет создать требуемую подпись. В противном случае проверка цифровой подписи даст положительный результат, и пользователь сможет продолжить работу. В случае положительной аутентификации пользователя система защиты обеспечивает доступ со стороны пользователя к защищенным информационным ресурсам АРМ в соответствии со схемой использования ключей при доступе к зашифрованным объектам.

Предполагается, что предварительно соответствующие зашифрованные информационные объекты должны быть созданы. Для создания зашифрованного информационного объекта генерируется первичная пара асимметричных ключей (по ГОСТ 34.10), которая закрепляется за данным объектом. В базе данных ПАК для каждой первич-

ной и личной пары асимметричных ключей используются следующие атрибуты:

– числовой идентификатор ключевой пары, а также дата и время ее создания;

– числовой идентификатор пользователя, создавшего ключевую пару;

– имя (символьный идентификатор) ключевой пары;

– идентификатор алгоритма шифрования объекта, для которого создана ключевая пара;

– описание ключевой пары;

– открытый и закрытый ключи.

Защищаемый объект шифруется по вторичному ключу симметричного шифрования, формируемому по алгоритму Диффи–Хеллмана на основе соответствующей объекту первичной пары асимметричных ключей. Первичная пара асимметричных ключей, закрепленная за объектом, защищается с помощью ключей доступа.

Система управления цифровыми сертификатами открытых ключей реализуется на основе использования удостоверяющего центра. В соответствии с международным признанным форматом для определения сертификатов открытых ключей (стандартом X.509 ITU), выдаваемый пользователю цифровой сертификат включает следующие элементы:

– версия, серийный номер и срок действия сертификата;

– информация о доверителе, выдавшем сертификата;

– информация о владельце сертификата (имя и фамилия, идентификатор, организация, адрес и др.);

– открытый ключ владельца сертификата;

– тип используемого алгоритма цифровой подписи;

– цифровая подпись всего содержимого сертификата, сформированная выдавшим сертификат удостоверяющим центром.

Ответственность за подлинность указанной в сертификате информации несет удостоверяющий центр, выдавший сертификат и сформировавший под ним свою подпись. Основными компонентами удостоверяющего центра являются центры сертификации, регистрации и сетевой справочник сертификатов [9]. На рисунке 5 показан пример использования ключей при доступе к зашифрованному объекту доверенной инфраструктуры.

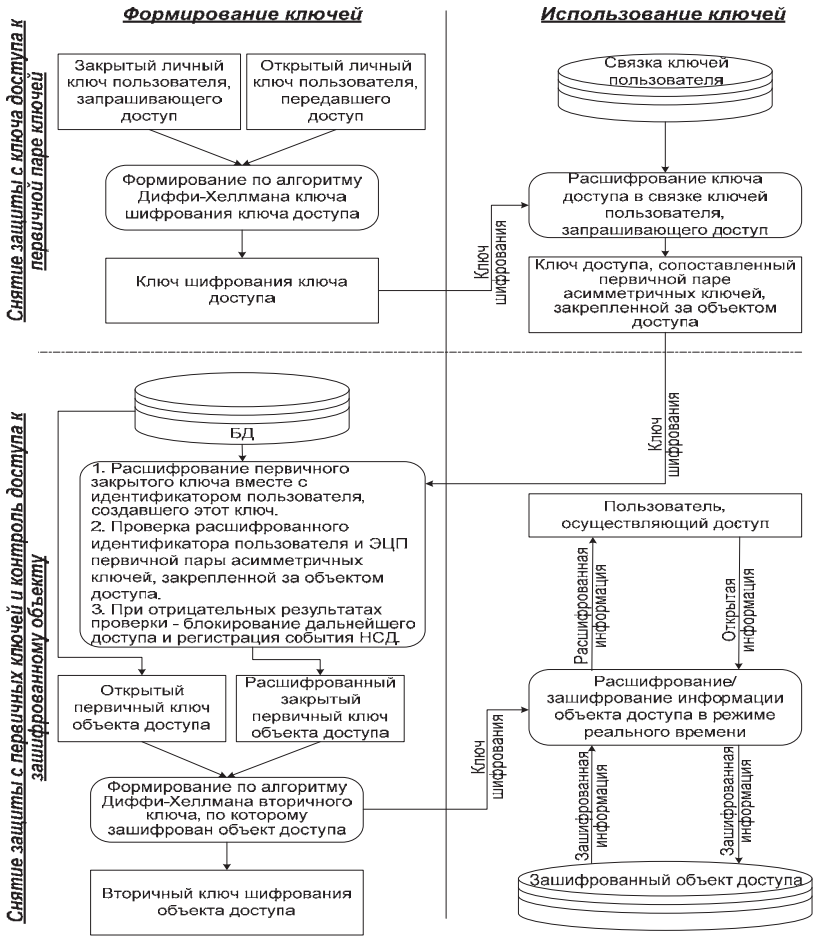


Рис. 5. Схема использования ключей при доступе к зашифрованному объекту

Центр сертификации обеспечивает формирование цифровых сертификатов. Кроме цифровых сертификатов, планируемых для использования, Центр сертификации формирует список отозванных сертификатов.

Центр регистрации предназначен для регистрации конечных пользователей. Основная задача Центра регистрации — регистрация пользователей и обеспечение их взаимодействия с Центром сертификации. В задачи Центра регистрации также входит публикация сертификатов и списка отозванных сертификатов в сетевом справочнике.

Центр регистрации является единственной точкой входа и регистрации пользователей. В качестве операционной платформы СПАК вследствие объективных причин предложено использование комбинированной операционной среды:

– для защищенного выполнения прикладных процессов и целевых функций АС – ОС Windows;

– для критичных функций настройки режимов защиты, управления ключами и конфигурирования криптомодулей — аналог ядра доверенной ОС Linux, реализованный как программный эмулятор аппаратного модуля доверенной загрузки.

СПАК основан на формальной и верифицированной модели управления доступом к защищаемым ресурсам АС. Показано, что разграничение доступа к информационным ресурсам (файлам, каталогам, томам NTFS, отчуждаемым носителям, портам ввода-вывода и принтерам) происходит в первую очередь согласно мандатному принципу контроля доступа, а дискреционные правила контроля доступа действуют только в пределах разрешений, установленных в соответствии с мандатным принципом. Эффективный доступ субъекта к информационным ресурсам определяется как результат пересечения атрибутов мандатного и дискреционного доступа. Представлены уровни, реализуемые в СПАК для защиты от обхода диспетчера доступа.

Таким образом, при разработке СПАК «Ключ-Ш» реализована технология построения комплексной системы информационно-компьютерной безопасности с учетом информационных рисков, основанная на учете всех исходных требований, существующих угроз и влияющих на безопасность факторов при комплексном использовании наиболее эффективных мер, методов и средств защиты. Применение СПАК «Ключ-Ш» в АС доверенной инфраструктуры позволяет снизить показатели информационных рисков до приемлемого уровня, при котором обеспечивается гарантированная степень защищенности распределенных АС.

6. Организация защиты контура в доверенной инфраструктуре. К средствам защиты неоднородной АС относятся, прежде всего, средства защиты "периметра" - межсетевые экраны (МЭ), антивирусной защиты, разграничения доступа, закрытия канала связи - связанные с защитой от "внешних атак". Хотя возможность "внешней угрозы" несколько преувеличена, она реальна. Основным "нарушителем" для любой АС является авторизованный пользователь с высоким статусом. Поэтому система безопасности должна строиться с учетом фактора "внутреннего нарушителя", как самого опасного субъекта. Напомним, что большинство удачных "внешних атак" было проведено с использованием внутреннего ресурса системы. Поэтому в АС необходимо предусмотреть механизмы, позволяющие строго регламентировать доступ к внутренним ресурсам системы на базе "ролевых сцена-

риев", должностных инструкций, ведения журналов безопасности и системных событий для предотвращения и выявления источников "внутренних атак". Здесь же важной является задача шифрования (закрытия) канала обмена между любыми абонентами АС. Это опять-таки задача СЗИ ОСПО. Если существует тесная связь между СЗИ на "периметре", антивирусного пакета и пр., то система безопасности будет работать непротиворечиво и прозрачно для пользователя, что является немаловажным фактором, влияющим в конечном итоге на работоспособность системы в целом. Самые общие задачи системы защиты информации ОСПО таковы:

- организация безопасного доступа объектов АС в каналы связи, в том числе открытые;

- построение единой политики безопасности в рамках гетерогенной распределенной сети АС;

- защита от НСД к информации, принимаемой, обрабатываемой, передаваемой и хранимой в АС по необходимому классу защищенности, в том числе - до сведений, содержащих государственную тайну, на выделенных локальных узлах АС;

- передача меток конфиденциальности в пределах защищенной наложенной сети АС, реализованной средствами ОСПО;

- осуществление защитных мер (в том числе организационных) по закрытию каналов передачи данных, а также возможных каналов утечки информации.

МЭ должен представлять собой программный комплекс, управляемый специально разработанной операционной системой. Одной из особенностей МЭ должна являться простота его установки, исчерпывающий набор настроек по умолчанию, которые позволяют системному администратору быстро организовать доступ в Интернет, решая одновременно проблему острой нехватки квалифицированного персонала на местах. Серверная часть является точкой доступа, обеспечивает безопасное и надежное, экономически оправданное взаимодействие с Сетью, генерацию собственной внутренней сети Интранет посредством полного и понятного механизма маршрутизации IP-пакетов с функциями фильтрации, механизма трансляции адресов (NAT) и прокси-фильтрами сетевого уровня по протоколам HTTP, HTTPS и FTP. Поэтому основными функциями МЭ являются:

- обслуживание локальных узлов АС и защиты их от попыток несанкционированного доступа (НСД);

- обеспечение возможности создания централизованной ведомственной АС на основе локальных сетей, оснащенных МЭ, и связанных через глобальную сеть Интернет;

- разграничение доступа к ресурсам и сервисам на основе заданных правил;

- обеспечения возможности сквозного контроля и управления состоянием АС;

- обеспечение возможности поддержания актуального состояния прикладного ПО АС посредством локальной и удаленной установки ПО;

- обеспечения возможности реализации единой политики безопасности АС [10].

Таким образом, МЭ должен отвечать всем необходимым требованиям, предъявляемым к межсетевым экранам как к средствам защиты периметра АС, а именно:

- контроль доступа с поддержкой динамической адресации;
- трансляция сетевых адресов;
- зависимость требований безопасности от интерфейса МЭ;
- подсчет трафика и генерация отчетов;
- удобство и простота управления МЭ авторизованным Администратором;
- интеграция с другими средствами защиты информации;
- "прозрачное" функционирование без потери производительности сети;
- обеспечение технической поддержки.

На рисунке 6 представлена схема применения доверенного МЭ – контура при выходе в сеть Интернет из доверенной инфраструктуры.

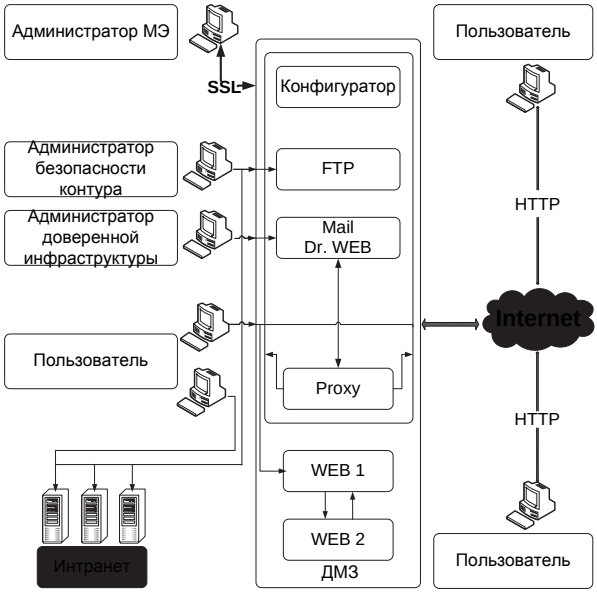


Рис. 6. Защита обработки данных в доверенном контуре

7. Заключение. Рассмотренный в статье подход к построению защищенных распределенных сетей обработки данных на основе доверенной инфраструктуры позволяет построить политику администрирования безопасности в распределенной системе на различных платформах. Под управлением администратора доверенной инфраструктуры будет производиться контроль всех действий в системе, включая фискальный. Применение перечисленных способов организации защиты информации в гетерогенных вычислительных сетях дает следующие преимущества:

1) пользователю предоставляется необходимый функционал и достаточный уровень защиты (близкий к уровню доверенного компьютера с набором сертифицированных ОС, СЗИ НСД и СКЗИ);

2) стоимость средств обеспечения доверенного сеанса значительно ниже стоимости оборудования рабочего места необходимого для реализации политики изолированной программной среды набором СЗИ;

3) клиент доверенного сеанса связи является мобильным загрузочным устройством, готовым к работе на любом недоверенном компьютере;

4) средства обеспечения доверенного сеанса не накладывают ограничений на работу пользователя с компьютером вне доверенного сеанса связи;

5) применение «Ключ-Ш» в АС позволяет снизить показатели информационных рисков до приемлемого уровня, при котором обеспечивается гарантированная степень защищенности распределенных АС.

Литература

1. *Ручкин В.Н., Фулин В.А.* Архитектура компьютерных сетей // Диалог-МИФИ. 2008. 76 с.
2. *Андерсон К., Минаси М.* Локальные сети. Полное руководство // СПб.: КОРОНА принт. 1999. 458 с.
3. *Косарев В.П., Еремин Л.В.* Компьютерные системы и сети // Финансы и статистика. 1999. С .260–281.
4. *Новиков С.В., Зима В.М., Андрушкевич Д.В.* Организация защиты информации в гетерогенных вычислительных сетях // Информационно-методический журнал «Инсайд». СПб.: ИД Афина. 2014. № 3. С. 21–28.
5. *Кульгин М.В.* Технология корпоративных сетей. Энциклопедия // СПб.: Питер. 2001. 699 с.
6. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов // СПб.: Питер. 2009. 352 с
7. *Суворов А.Б.* Телекоммуникационные системы, компьютерные сети и Интернет // СПб.: Феникс. 2010. 383 с.
8. *Зима В.М., Клюев А.В., Литвинов О.А., Ломако А.Г., Петров А.Т.* Основы защиты информации от несанкционированного доступа в автоматизированных сис-

темах конфиденциального делопроизводства // Труды СПИИРАН. Вып. 3. Т. 2. 2006. С. 84–95.
9. *Зима В.М., Молдовян А.А., Молдовян Н.А.* Компьютерные сети и защита передаваемой информации // СПб.: издательство СПбГУ. 1998. 328 с.
10. *Здирук К.Б.* Вопросы организации защищенной системы хранения и обработки данных в гетерогенных вычислительных сетях // Вопросы защиты информации. Журнал. М.: 2007. С. 46–52.

References

1. Ruchkin V.N., Fulin V.A. *Arhitektura komp'juternyh setej* [Architecture of computer networks]. Dialog-MIFI. 2008. 76 p. (In Russ.).
2. Anderson K., Minasi M. *Lokal'nye seti. Polnoe rukovodstvo* [LAN. Full guide]. SPb.: KORONA print. 1999. 458 p. (In Russ.).
3. Kosarev V.P., Eremin L.V. [Computer systems and networks]. *Finansy i statistika – Finance and statistics.* 1999. pp.260–281. (In Russ.).
4. Novikov S. V., Zima V. M., Andrushkevich D. V. [Organization of information security in heterogeneous computer networks]. *Informacionno-metodicheskij zhurnal "Insajd" – Information-methodical journal "Inside"*. SPb.: ID Afina. 2014. vol. 3. pp. 21–28. (In Russ.).
5. Kuligin M.V. *Tehnologija korporativnyh setej. Jenciklopedija* [Technology enterprise networks. Encyclopedia]. SPb.: Piter. 2001. 699 p. (In Russ.).
6. Olifer V. G., Olifer N.A. *Komp'juternye seti. Principy, tehnologii, protokoly. Uchebnik dlja vuzov* [Computer network. Principles, technologies and protocols. Textbook for high schools]. SPb.: Peter. 2009. 352 p. (In Russ.).
7. Suvorov A. B. *Telekommunikacionnye sistemy, komp'juternye seti i Internet* [Telecommunication systems, computer networks and Internet]. SPb.: Feniks. 2010. 383 p. (In Russ.).
8. Zima V.M., Klyuyev A.V., Litvinov O.A., Lomako A.G., Petrov A.T. [Framework for the protection of information from unauthorized access automated systems confidential records management]. *Trudy SPIIRAN – SPIIRAS Proceeding.* 2006. vol. 3. issue 2. pp. 84–95. (In Russ.).
9. Zima V.M., Moldovyan A.A., Moldovyan N.A. *Komp'juternye seti i zashhita peredavaemoj informacii* [Computer networks and the protection of information transmitted]. SPb.: izdatel'stvo SPbGU. 1998. 328 p. (In Russ.).
10. Zdiruk K. B. [Organization protected storage system and data processing in heterogeneous computer networks]. *Voprosy zashhity informacii. Zhurnal – The issues of information security. Journal*. M.: 2007. pp. 46–52. (In Russ.).

Новиков Сергей Витальевич — к-т воен. наук, доцент кафедры систем сбора и обработки информации Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: защита информации в автоматизированных системах специального назначения, представление обстановки на электронной карте ГИС, информационная безопасность. Число научных публикаций — 24. novikov1976@mail.ru; Ждановская улица д. 13, г. Санкт-Петербург, 197198, РФ; р.т. 7(812)347-9687.

Novikov Sergey Vitalyevich — Ph.D., associate professor of system for collecting and processing information department Mozhaisky military space Academy. Research interests: information security in automated systems for special purposes, the representation of the situation on the electronic map, GIS, information security. The number of publications — 24. novikov1976@mail.ru; 13, Zhdanovskaya street, St. Petersburg, 197198, Russia; office phone 7(812)347-9687.

Зима Владимир Михайлович — к-т техн. наук, профессор кафедры систем сбора и обработки данных Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: защита информации в информационных сетях, автоматизированных системах. Число научных публикаций —105. vladimir_zima@mail.ru; улица Ждановкая д. 13, г. Санкт-Петербург, 197198, РФ; р.т. +7(812)347-9687.

Zima Vladimir Mikhailovich — Ph.D., associate professor, professor of system for collecting and processing information department Mozhaisky military space Academy. Research interests: information security in data networks, automated systems. The number of publications — 105. vladimir_zima@mail.ru; 13, Zhdanovskaya street, St. Petersburg, 197198, Russia; office phone +7(812)347-9687.

Андрушкевич Дарья Владимировна — адъюнкт кафедры систем сбора и обработки информации Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: защита информации в информационных сетях, автоматизированных системах. Число научных публикаций — 8. andrushkevich.d@mail.ru; улица Ждановская д. 13, г. Санкт-Петербург, 197198, РФ; р.т. +7(812)347-9687.

Andrushkevich Daria Vladimirovna — Ph.D. student of system for collecting and processing information department Mozhaisky military space Academy. Research interests: information security in data networks, automated systems. The number of publications — 8. andrushkevich.d@mail.ru; 13, Zhdanovskaya street, St. Petersburg, 197198, Russia; office phone +7(812)347-9687.

РЕФЕРАТ

Новиков С.В., Зима В.М., Андрушкевич Д.В. **Подход к построению защищенных распределенных сетей обработки данных на основе доверенной инфраструктуры.**

В статье предлагается подход к построению распределенных вычислительных сетей и организации защиты информации с использованием доверенной инфраструктуры.

Приводится инфраструктура, которая будет состоять из контура, в состав которого будут входить: доверенный контроль, доверенный канал связи, доверенные сегменты распределенной сети, доверенные АРМ с различными платформами ОС, доверенное специальное программное обеспечение с НДВ, доверенная система шифрования, доверенные администраторы всех сегментов сети, администратор доверенной инфраструктуры.

Для организации защиты информации на различных узлах распределенных сетей обработки данных предлагается введение данного контура с администраторским управлением на каждом сегменте контура под управлением администратора доверенной инфраструктуры.

В данной статье анализируются некоторые из подходов защиты сегментов доверенной инфраструктуры, а именно: организация защиты информации в доверенном контуре на различных платформах ОС; доверенные элементы распределенной информационной системы; двухуровневое шифрование в доверенной инфраструктуре; доверенный контур в доверенной инфраструктуре, как защита периметра.

Результаты работы показывают, что подход к построению защищенных распределенных сетей обработки данных на основе доверенной инфраструктуры позволяет построить политику администрирования безопасности в распределенной системе на различных платформах. Под управлением администратора доверенной инфраструктуры будет производиться контроль всех действий в системе, включая фискальный.

SUMMARY

Novikov S.V., Zima V.M., Andrushkevich D.V. **Approach to Building Secure Distributed Networks of Data Processing based on Trusted Infrastructure.**

In article approach to creation of the distributed computer networks and the organization of information security with use of the entrusted infrastructure is offered.

The infrastructure, which will consist of the entrusted control, the entrusted communication channel, the entrusted segments of the distributed network entrusted an automated workplace with the OS various platforms, the entrusted special software with NDV, the entrusted system of enciphering, the entrusted administrators of all segments of a network, the administrator of the entrusted infrastructure, is presented.

For the organization of information security on various knots of the distributed networks of data processing introduction of the contour with administrator management on each segment of a contour under control of the administrator of the entrusted infrastructure is offered.

In this article some of approaches of protection of segments of the entrusted infrastructure, are analyzed namely: the organization of information security in the entrusted contour on the OS various platforms; the entrusted elements of the distributed information system; two-level enciphering in the entrusted infrastructure; the entrusted contour in the entrusted infrastructure, as defense of perimeter.

Results of work show that approach to creation of the protected distributed data processing networks on the basis of the entrusted infrastructure allows to construct policy of administration of safety in the distributed system on various platforms. Under control of the administrator of the entrusted infrastructure control of all actions in system, including the fiscal will be made.

УДК 004.045, 004.773

А. М. Романченко

ОБОБЩЕННАЯ СТРУКТУРНАЯ МЕТАМОДЕЛЬ ПРОТОКОЛА ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

Романченко А.М. **Обобщенная структурная метамодель протокола информационного взаимодействия.**

Аннотация. Данная работа посвящена разработке структурной метамодели произвольного протокола информационного взаимодействия. Эта метамодель может быть использована для создания формализованных моделей различных протоколов, построения автоматических декодеров, хранения и обмена информацией о протоколах. Ее использование позволяет упростить многие прикладные задачи анализа данных, сравнения различных протоколов, влияния ошибок в канале связи на правильность декодирования и т.д.

Ключевые слова: построение протоколов, моделирование протоколов, анализ протокольных данных, протоколы прикладного уровня.

Romanchenko A.M. **Generalized Structural Metamodel of Information Interaction Protocol.**

Abstract. This work is devoted to the development of structural meta-model arbitrary protocol information interaction. This meta-model can be used to create formal models of various protocols, construction of automatic decoders by model, storage and exchange of information on protocols. Its use simplifies many application tasks of data analysis, tasks of comparing various protocols, study effect of errors in the communication channel on correctness of decoding.

Keywords: construction of protocols, modeling of protocols, analysis of protocol data, application protocols.

1. Введение. Сегодня, несмотря на достаточно большое количество различных протоколов информационного взаимодействия, используемых при реализации большого спектра информационных технологий, постоянно возникает необходимость разработки новых протоколов, особенно прикладного уровня. Разработка нового протокола автоматически означает необходимость решения задач распознавания, декодирования, проверки целостности и анализа протокольных данных. В данной работе предлагается использовать обобщенную метамодель протокола информационного взаимодействия в качестве основы для разработки новых протоколов, их описания в виде некоторой реализации этой модели, использовании для обмена информацией, построения декодеров, распознавания и анализа.

Преимуществом использования обобщенной метамодели является возможность описания в рамках этой модели произвольного протокола и использования его в дальнейшем для решения конкретных прикладных и аналитических задач. При этом, если реализовать построение декодера на основе информации содержащейся в обобщенной метамодели, то добавление нового протокола в

программную реализацию или изменение существующего не потребует изменения декодера, достаточным будет добавления новой модели протокола. Также удобным является возможность ведения базы данных известных протоколов и построение на основе обобщенной метамодели математических и других моделей существующих и новых протоколов.

Обобщенная структурная метамодель протоколов, предположительно, не подходит для описания слабо структурированных протоколов высокой сложности, в которых могут присутствовать, или не присутствовать множество полей переменной длины, в том числе с вложенной информацией, подлежащей самостоятельному интерпретированию. К таким протоколам можно отнести HTTP, FTP, POP3 и другие аналогичной сложности. Но для таких протоколов и не требуется использовать обобщенный декодер или анализатор, так как для них существует множество стандартных библиотек обработки.

При проведении анализа существующих подходов к разработке и анализу протоколов не было обнаружено специализированных инструментов их проектирования и стандартного описания структуры протокола в формализованном виде. На практике почти все разработчики используют спецификацию протокола, то есть его текстовое описание. Очевидно, что информация о протоколе, представленная в форме текстового описания, не может быть использована для решения задач, возникающих на практике (подробно рассмотрены далее), так как невозможна ее автоматическая интерпретация.

Ранее в ряде работ [3, 4] уже предлагалось использование модели протокола на языке XML вместо спецификации. Основная идея, предложенная в этих работах, состоит в описании с помощью языка XML последовательности действий, составляющих протокол, и связи их с функциями программы, реализующей эти действия. Это, в основном, относится к многошаговым протоколам (например криптографическим), в которых взаимодействуют несколько пользователей. Описание данных протокола, предложенное в работе [4], содержит информацию только об их составе и недостаточно для их обобщенной обработки. Протоколы, описываемые в работе [3] (и другие протоколы семейства XMLP) фактически ограничены только текстовой формой, что не всегда эффективно на практике и существенно ограничивает разработчика. То есть XML в работе [3] используется не для описания формата протокола, а для представления данных протокола. Ни один из рассмотренных подходов, в отличие от предложенного в работе, не позволяет описать

структуру произвольного протокола, и построить единый декодер для множества моделей протоколов.

Ряд других работ по данной тематике предлагают описание протокола с помощью специализированных языков, таких как Ciecero [9], Promela++[5], LOTOS [7,8], Estelle [6] и других. Использование таких моделей потребует от разработчиков знания специфичного языка и связи его с основным языком разработки (C++, java, C#), поэтому применение такой модели для решения практических задач будет затруднительным, если вообще возможным. Язык XML, использованный для построения метамодели в данной работе, свободен от этих недостатков и легко интегрируется в программу на любом из указанных языков программирования. Язык XML достаточно прост для понимания, поэтому и начинающие специалисты и даже пользователи будут способны самостоятельно разработать протокол для своих нужд после освоения подхода предложенного в работе.

2. Разработка метамодели протокола с использованием языка XML/DTD. При проведении анализа подмножества существующих протоколов информационного обмена было выявлено, что все хорошо структурированные протоколы могут быть классифицированы по признаку вида содержащихся в них данных. На его основе можно выделить:

1. Информационные протоколы — протоколы, содержащие поля определенной длины, в которых находятся заранее известные данные, такими, например, являются многие телеметрические протоколы. Обычно поля являются числами различных форматов, но могут содержать и бинарные данные.

2. Транспортные протоколы — протоколы, предназначенные для «упаковки» произвольных данных. Обычно это требуется для передачи данных с верхних уровней эталонной модели взаимодействия открытых систем (ЭМВОС) на нижние уровни. Упаковка данных часто используется при адаптации существующих протоколов к передаче с помощью специфической аппаратуры, а также сопряжении разнородных сетей. Обычно в рамках транспортного протокола неизвестно, какая именно информация передается с ее помощью. Поля, в которые осуществляется упаковка данных, могут быть бинарными или текстовыми (например, в кодировке BASE64), постоянной или переменной длины.

3. Смешанные протоколы, в которых присутствуют как числовые поля с известным содержанием и правилами его интерпретации, так и поля с произвольными данными заранее неизвестной структуры.

4. Протоколы являющиеся «системой команд» некоторого устройства или программы.

Целью разработки обобщенной структурной метамодели протокола является предоставление возможности описания моделей всех приведенных видов протоколов. При этом информация, содержащаяся в модели, должна быть достаточной для построения декодера без модификации программы обработки для каждого протокола. Модель должна быть интуитивно понятной пользователю и доступной для генерации, интерпретации и изучения без использования специальных средств.

В качестве инструмента построения обобщенной модели протокола информационного взаимодействия, будет использован язык XML с использованием механизма DTD (data type definition). Выбор такого инструментария позволит достичь сразу нескольких основополагающих целей работы:

1. Стандартизацию, так как язык XML является широко распространенным и используется для описания моделей данных в рамках некоторой предметной области, формализованной с помощью этого же языка.

2. Возможность создания протоколов, их изучения и использования с помощью общедоступных инструментов, в том числе и общего назначения, например, любого текстового редактора. При этом все же рекомендуется воспользоваться специализированными инструментами для работы с файлами формата XML, способными автоматически проверять синтаксис файла и соответствие его файлу определения данных. Автором был использован в качестве такого инструмента «XML copy editor» - http://xml-copy-editor.sourceforge.net/.

3. Возможность автоматической проверки корректности описания протокола в рамках выбранной модели данных. Существование большого количества интерпретаторов формата XML, позволяющих извлекать информацию из модели конкретного протокола, дает возможность построения «на лету» декодера по конкретной реализации протокола с помощью обобщенной модели. Такие инструменты существуют для большинства распространенных языков программирования, в частности для C++ можно назвать:

- Xerces (http://xerces.apache.org/);
- Arabica (http://www.jezuk.co.uk/cgi-bin/view/arabica);
- TinyXML (http://sourceforge.net/projects/tinyxml/);
- pugixml (https://code.google.com/p/pugixml/);
- libxml++ (http://libxmlplusplus.sourceforge.net/).

Для построения обобщенной структурной метамодели протокола необходимо выяснить, из каких элементов может состоять протокол информационного обмена, какие эти элементы имеют характеристики, а также какие информационные поля имеет сам протокол.

Все структурные элементы, входящие в состав произвольного протокола, можно разделить на два вида — содержательные и служебные. Содержательные элементы предназначены для передачи информации с помощью протокола, служебные необходимы для функционирования самого протокола и использующей его инфраструктуры — программных и аппаратных средств. В качестве модели представления протокольных данных будем рассматривать поток байтов, представляющих протокольные блоки с возможными искажениями разных видов (инверсия, вставка/пропуск и т.п.) вследствие ошибок в канале связи. К служебным элементам произвольного протокола информационного обмена можно отнести заголовок (префикс), окончание (постфикс) и контрольную сумму. К содержательным полям протоколов можно отнести числовые поля разных форматов, текстовые или бинарные поля постоянной и переменной длины, поля флагов и т. п. Метамодель должна позволять описывать все эти элементы с детализацией, достаточной для построения декодера. Упрощенная структура метамодели в графическом виде приведена на рисунке 1. Рассмотрим элементы, представленные в ней и их характеристики более детально.

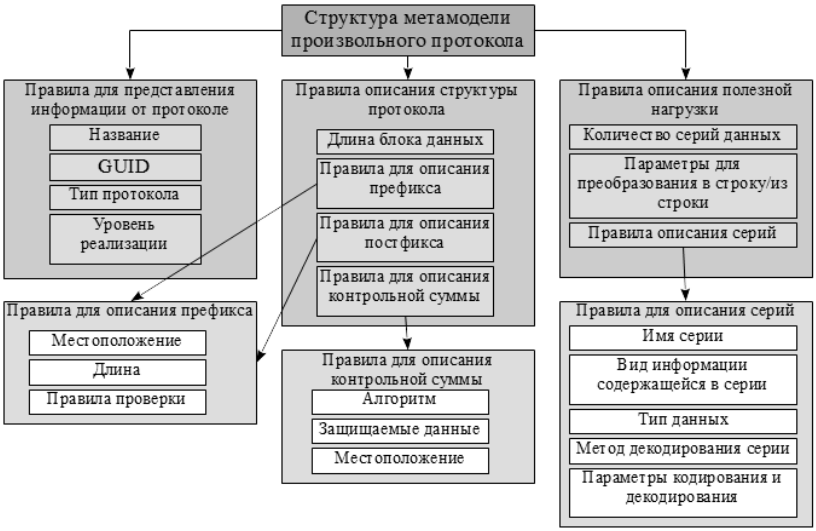


Рис. 1. Упрощенная структура метамодели протокола

Информационные характеристики протокола могут быть представлены следующим набором параметров:

– тип протокола, числовое поле, может принимать значения из множества: «информационный», «транспортный», «система команд», «смешанный» (информационно-транспортный), «другой»;

– уровень реализации протокола в рамках ЭМВОС, числовое поле, может принимать значения из множества: «физический/1», «канальный/2», «сетевой/3», «транспортный/4», «сеансовый/5», «представительский/6», «прикладной/7» или «неизвестный» если место функционирования протокола неизвестно или не определено;

– название протокола, текстовое поле переменной длины;

– глобальный уникальный идентификатор GUID — текстовая строка формата «XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX» где «X» - шестнадцатеричная цифра, использование GUID практически гарантирует уникальность различных протоколов даже при использовании большого их количества;

– длина блока данных, может быть константой или лежать в некотором допустимом диапазоне;

– число элементов (серий) данных, каждая серия содержит один из содержательных элементов полезной нагрузки, например числовое поле (время, температуру) или бинарное поле — произвольные данные, возможно, имеющие собственную сложную структуру.

Префикс может входить или не входить в состав протокола, как правило, его присутствие облегчает декодирование, но уменьшает объем полезной нагрузки, передаваемой протоколом. Можно выделить следующие содержательные характеристики описывающие префикс:

– наличие префикса;

– смещение от начала блока данных (обычно равно 0, то есть префикс является началом блока данных);

– длина (обычно используются длины от 1 до 4 байт);

– значение префикса.

Проверка префикса выполняется путем простого сравнения с эталоном, поэтому такое понятие как алгоритм проверки для этого элемента представляется излишним.

Постфикс имеет такие же характеристики, как и префикс, но используется для обозначения конца блока данных.

Серия данных (элемент полезной нагрузки) является наиболее важной частью любого протокола, определяет, что и как передается в его составе. Название «Серия» использовано потому, что набор

значений одного параметра в последовательных протокольных блоках данных образует серию данных, например серию отсчетов времени. Важнейшими характеристиками серии данных являются:

– имя серии, текстовое поле переменной длины;

– тип значения, четырехсимвольный код, подробно рассмотрен ниже;

– тип данных в серии, четырехсимвольный код, подробно рассмотрен ниже;

– параметры серии, определяющие длину поля данных, необходимы только для некоторых типов серий;

– тип декодера для серии данных.

При изучении существующих протоколов, были выделены ряд типов использованных в них серий, которые представлены на рисунке 2. Всего в нем отражено 17 основных типов, но при необходимости этот список может быть расширен, например 64 битными типами данных.

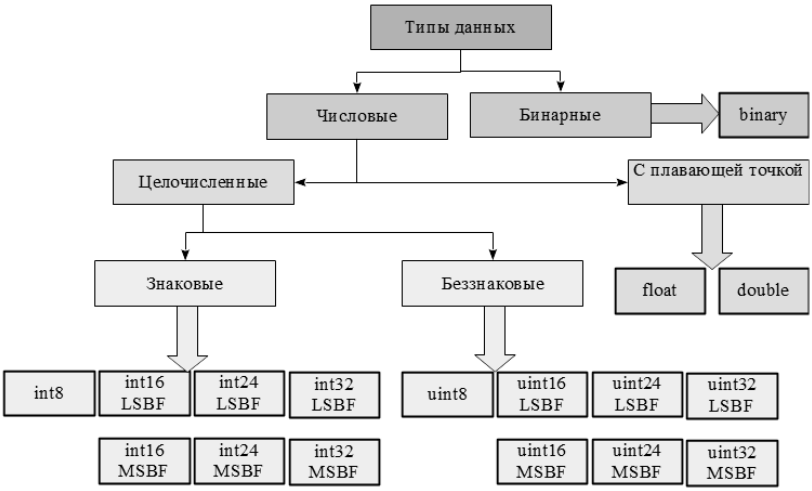


Рис. 2. Типы серий данных, использованных в метамодели

С точки зрения практической реализации для кодирования типа данных удобно использовать т. н. «четырехсимвольный код» или FourCC(four characters code). С одной стороны его использование достаточно наглядно при программной реализации протокола, особенно с использованием специального макроса. С другой стороны использование 4-байтных значений кода обеспечивает максимальную производительность и удобство манипуляции на большинстве

аппаратных платформ. Пример использования такого кодирования приведен в листинге 1 (язык C++).

```
#define DW_Make(btL, btM1, btM2, btH)
((static_cast<DWORD>(btH)<<24)|(static_cast<DWORD>(btM2)<<16)|
(static_cast<DWORD>(btM1)<<8)| (static_cast<DWORD>(btL)))

// пример кодирования типа int32 LSBF
static DWORD GetSID(void){return DW_Make(' ','L','I','4');}
```

Листинг 1. Пример использования FourCC для кодирования типа серии

Но использование кодов FourCC непосредственно в модели протокола неудобно из-за сложности запоминания четырехсимвольных аббревиатур, поэтому предлагается использовать специальный элемент для связи четырехсимвольного типа и его расширенного названия, удобного для использования в модели. Пример такой связи с помощью тега «ASSOC» представлен в листинге 2.

```
<ASSOC Type="item" From="int32LSBF" To=" LI4"/>
```

Листинг 2. Связь кода FourCC с интуитивно понятным названием типа данных, использованным при построении модели

Атрибут «From» обозначает название, использованное в модели, атрибут «To» - кодирование в программной реализации, обязательно должен иметь длину 4 символа. Атрибут «Type» означает, для какого элемента используется отображение, то есть данный механизм отображения можно использоваться не только для удобного кодирования типа данных, но и для других элементов, например типа серии.

Тип данных в серии предназначен для отражения того, какая именно информация в ней передаются. Например, температуру, считанную с первого датчика, можно сопроводить кодом типа данных, представленным в листинге 3. Использование такого типа кодирования имеет несколько важных преимуществ, например, дает возможность легко отображать структуру протокола в виде дерева, содержащего информацию о составе его полей, а также автоматически строить графические модели протокола.

```
// кодирование в модели
<SeriesType>' ','T','*','1'</SeriesType>

// кодирование в программе обработки
#define ADC_T1 DW_Make(' ','T','*','1')
```

Листинг 3. Пример кодирования типа информации в серии

Но самым важным преимуществом такого кодирования является возможность нахождения и специализированной обработки данных

нужных типов в составе различных (произвольных) протоколов. Это позволяет использовать унифицированные алгоритмы обработки любых протоколов, содержащих в своем составе серии нужных типов.

Характеристика «*тип декодера*» должна содержать всю необходимую информацию для правильного извлечения данной серии из пакета. Предлагается использование следующих видов декодеров:

– фиксированное смещение, для серий постоянной известной длины;

– фиксированное смещение и размер, для серий различной длины, например бинарных полей;

– относительное смещение от начала или конца пакета;

– фиксированное смещение, значение которого записано в другой серии.

На практике может потребоваться больше типов декодеров, поэтому приведенный список предлагается рассматривать в качестве основы для дальнейшего расширения по мере необходимости.

Контрольная сумма — важнейшая характеристика протокола позволяющая проверять его целостность, также в простых протоколах (причем фиксированной длины) может быть использована в качестве механизма синхронизации границы пакета. Имеет следующие характеристики:

– смещение начала данных от начала пакета;

– смещение конца данных от конца пакета;

– длина контрольной суммы в байтах;

– тип алгоритма;

– смещение, по которому располагается контрольная сумма от начала или конца пакета.

Важно понимать, что смещение начала данных от начала пакета, а конца данных от конца пакета, позволяет удобным образом работать с пакетами переменной длины.

Дополнительно к приведенным характеристикам предлагается использование в описании протокола механизма конвертации в строку, чтобы иметь возможность сохранять/загружать данные произвольного протокола в строковой форме. Предполагается, что каждый пакет будет соответствовать одной строке в сохраненных данных. Поля разделяются пробелом, бинарные/текстовые поля преобразуются в кодировку BASE64 или аналогичные. Характеристики механизма преобразования определяют, использовать ли нумерацию строк при сохранении и порядок сохранения данных, который может отличаться от порядка следования данных в пакете. Кроме правила конвертации предлагается использование правила проверки соответствия некоторой

строки протоколу, это правило должно определять алгоритм проверки и задавать параметры этого алгоритма. Предлагается использование следующих алгоритмов проверки корректности:

– подсчет количества разделителей (пробелов);

– проверка числа разделителей и допустимых символов;

– использование регулярного выражения, это наиболее прогрессивный способ проверки, пример такого выражения для протокола содержащего только числовые поля: «^(?>[+-]?\d+(?>\.\d+(?>e[+-]\d+)?)?(?>\s+)?){N}$», где N – это число серий данных увеличенное на 1.

Метамодель произвольного протокола в форме файла data type definition представлена в листинге 4.

```
<!ELEMENT protocols (ASSOC+, protocol)>
<!ELEMENT ASSOC EMPTY>
<!ATTLIST ASSOC Type (item) #REQUIRED>
<!ATTLIST ASSOC From CDATA #REQUIRED>
<!ATTLIST ASSOC To CDATA #REQUIRED>
<!ELEMENT protocol (Title, Prefix, Postfix, GUID, Length, SeriesCount, Series*, CRCType, FormatString, CheckString?)>
<!ATTLIST protocol type (DATA|TRANSPORT|COMMANDSYSTEM|MIX|OTHER) #REQUIRED>
<!ATTLIST protocol level (UNDEFINED|L1 |PHYSICAL|L2 |CHANNEL|L3 |NETWORK|L4 |TRANSPORT|L5 |SESSION|L6 |PRESENTATION|L7 |APPLICATION) #REQUIRED>
<!ELEMENT Title (#PCDATA)>
<!ELEMENT Prefix EMPTY>
<!ATTLIST Prefix present (YES|NO) #REQUIRED>
<!ATTLIST Prefix offset CDATA #REQUIRED>
<!ATTLIST Prefix type (None|Simple1B|Simple2B|Simple3B|Simple4B) #REQUIRED>
<!ATTLIST Prefix value CDATA #REQUIRED>
<!ELEMENT Postfix EMPTY>
<!ATTLIST Postfix present (YES|NO) #REQUIRED>
<!ATTLIST Postfix offset CDATA #REQUIRED>
<!ATTLIST Postfix type (None|Simple1B|Simple2B|Simple3B|Simple4B) #REQUIRED>
<!ATTLIST Postfix value CDATA #REQUIRED>
<!ELEMENT GUID (#PCDATA)>
<!ELEMENT Length EMPTY>
<!ATTLIST Length min CDATA #REQUIRED>
<!ATTLIST Length max CDATA #REQUIRED>
<!ELEMENT SeriesCount (#PCDATA)>
<!ELEMENT Series (SeriesName, SeriesType, SeriesParam?, DecodeType)>
```

```
<!ATTLIST Series VarType (int8| int16LSBF| int24LSBF| int32LSBF| int16MSBF|
int24MSBF| int32MSBF| uint8| uint16LSBF| uint24LSBF| uint32LSBF| uint16MSBF|
uint24MSBF| uint32MSBF| FLOAT| DOUBLE| Binary) #REQUIRED>
<!ELEMENT SeriesName (#PCDATA)>
<!ELEMENT SeriesType (#PCDATA)>
<!ELEMENT SeriesParam EMPTY>
<!ATTLIST SeriesParam Length CDATA #IMPLIED>
<!ATTLIST SeriesParam MinLength CDATA #IMPLIED>
<!ATTLIST SeriesParam MaxLength CDATA #IMPLIED>
<!ATTLIST SeriesParam DefaultLength CDATA #IMPLIED>
<!ELEMENT DecodeType (FIXEDOFFSET| FIXED| RELATIVEBE|
FIXOFF_SERIESLENGTH)>
<!ELEMENT FIXEDOFFSET EMPTY>
<!ATTLIST FIXEDOFFSET Offset CDATA #REQUIRED>
<!ELEMENT FIXED EMPTY>
<!ATTLIST FIXED Offset CDATA #REQUIRED>
<!ATTLIST FIXED Length CDATA #REQUIRED>
<!ELEMENT RELATIVEBE EMPTY>
<!ATTLIST RELATIVEBE OffsetFromBegin CDATA #REQUIRED>
<!ATTLIST RELATIVEBE OffsetFromEnd CDATA #REQUIRED>
<!ELEMENT FIXOFF_SERIESLENGTH EMPTY>
<!ATTLIST FIXOFF_SERIESLENGTH Offset CDATA #REQUIRED>
<!ATTLIST FIXOFF_SERIESLENGTH LengthIndex CDATA #REQUIRED>
<!ELEMENT CRCType (#PCDATA)>
<!ATTLIST CRCType databegin CDATA #REQUIRED
dataend CDATA #REQUIRED lengthvalue CDATA #REQUIRED
offsetvalue CDATA #REQUIRED
algtype (XOR|CRC8|ADD8|None|MD5) #REQUIRED>
<!ELEMENT FormatString (OrderData?)>
<!ATTLIST FormatString UseLineNumber (YES|NO) #REQUIRED>
<!ELEMENT OrderData EMPTY>
<!ATTLIST OrderData remap CDATA #REQUIRED>
<!ELEMENT CheckString EMPTY>
<!ATTLIST CheckString type (None| SpaceCount| SpaceAndExclude| RegEXP)
#REQUIRED>
<!ATTLIST CheckString param1 CDATA #REQUIRED>
<!ATTLIST CheckString param2 CDATA #REQUIRED>
```

Листинг 4. Метамодель произвольного протокола в форме файла DTD

В качестве иллюстрации применения данной метамодели для построения протоколов разных типов приводится два примера моделей информационного и транспортного протокола.

Простой информационный протокол содержит три числовых серии данных — три значения угловой скорости по ортогональным осям X, Y, Z, может быть отнесен к телеметрическим протоколам. Он имеет длину пакета 14 байт, префикс и контрольную сумму формата

CRC8. Данные в нем представлены тремя полями с плавающей точкой формата «float» (размерности 4 байта). Модель этого протокола приведена в листинге 5.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE protocols SYSTEM "Protocols.dtd">
<protocols>
<ASSOC Type="item" From="FLOAT" To=" F4"/>
<protocol type="DATA" level="APPLICATION">
<Title>3 GYRO</Title>
<Prefix present="YES" offset="0" type="Simple1B" value="0xec"/>
<Postfix present="NO" offset="0" type="None" value="0x00"/>
<GUID>7FAC6981-4F66-4728-B023-C9BE99529BC9</GUID>
<Length min="14" max="14" />
<SeriesCount>3</SeriesCount>
<Series VarType="FLOAT">
<SeriesName>Гир. X</SeriesName>
<SeriesType>' ',' ','W','X'</SeriesType>
<DecodeType> <FIXEDOFFSET Offset="1" /> </DecodeType>
</Series>
<Series VarType="FLOAT">
<SeriesName>Гир. Y</SeriesName>
<SeriesType>' ',' ','W','Y'</SeriesType>
<DecodeType> <FIXEDOFFSET Offset="5" /> </DecodeType>
</Series>
<Series VarType="FLOAT">
<SeriesName>Гир. Z</SeriesName>
<SeriesType>' ',' ','W','Z'</SeriesType>
<DecodeType> <FIXEDOFFSET Offset="9" /> </DecodeType>
</Series>
<CRCType databegin="0" dataend="12" lengthvalue="1" offsetvalue="13"
algtype="CRC8"/>
<FormatString UseLineNumber="YES" />
<CheckString type="None" param1="" param2=""/>
</protocol>
</protocols>
```

Листинг 5. Пример модели простого информационного протокола

Второй протокол относится к классу транспортных протоколов, то есть инкапсулирует произвольные данные протоколов других уровней. Он содержит одно бинарное поле длины 64 байта, защищенное контрольной суммой MD5 длиной 16 байт. Общая длина пакета составляет 80 байт. Модель данного протокола приведена в листинге 6.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE protocols SYSTEM "Protocols.dtd">
<protocols>
<ASSOC Type="item" From="Binary" To=" BIN"/>
<protocol type="DATA" level="APPLICATION">
<Title>Transport simple</Title>
<Prefix present="NO" offset="0" type="None" value="0x00"/>
<Postfix present="NO" offset="0" type="None" value="0x00"/>
<GUID>3738BE36-107D-4C74-80F9-086C9924100F</GUID>
<Length min="80" max="80" />
<SeriesCount>1</SeriesCount>
<Series VarType="Binary">
<SeriesName>Payload</SeriesName>
<SeriesType>' ','b','i','n'</SeriesType>
<SeriesParam Length="64" />
<DecodeType> <FIXED Offset="0" Length="64" /> </DecodeType>
</Series>
<CRCType databegin="0" dataend="63" lengthvalue="16" offsetvalue="64"
algtype="MD5"/>
<FormatString UseLineNumber="NO" />
<CheckString type="None" param1="0" param2="0" />
</protocol>
</protocols>
```

Листинг 6. Пример модели простого транспортного протокола

Для сравнения рассмотрим пример описания данных протокола из работы [4] см. листинг 7.

```
<object>
        <name>Session_State</name>
        <field type=”String”>id</field>
        <field type=”int”>Na</field>
        <field type=”int”>Nb</field>
        <field type=”key”>PrivateKey</field>
<field type=”key”>PublicKey</field>
</object>
```

Листинг 7. Пример описания данных предназначенных для использования высокоуровневых функций обработки

Очевидно, что использовать такую модель для обобщенного декодирования и других видов обработки невозможно из-за недостаточной информации о свойствах передаваемых данных, поэтому такая модель подходит только для использования частных обработчиков, которым известен не только состав, но и структура данных протокола.

3. Использование метамодели протокола при решении прикладных задач. Рассмотрим, как предложенная метамодель и модели протоколов, построенные с ее использованием, могут быть применены на практике.

Обмен информацией о протоколах — так как, по сути, предложенная модель представляет собой некий стандарт описания протокола, то его использование позволит различным разработчикам обмениваться информацией об используемых ими протоколах, быстро добавлять поддержку новых протоколов в своих продуктах.

Построение универсального декодера различных протоколов на основе их моделей. Для этого на первом этапе потребуется генерация программного протокола на основе данных, содержащихся в модели, и его последующее использование в составе универсальных декодеров, в том числе и мультипротокольных (то есть когда в едином потоке данных перемежаются данные нескольких протоколов). Снижение скорости декодирования примерно на 30%, по сравнению с построением уникального декодера каждого протокола, для большинства практических задач является малозначимым фактором в сравнении с упрощением реализации.

Предоставление в удобном виде для пользователя информации о том или ином протоколе, это может быть дополнением к другим способам описания протокола, например, вербальному или графическому.

Разработка графического «конструктора протоколов». Разработку протоколов с использованием метамодели можно упростить еще больше путем создания конструктора протоколов. Элементы протоколов в нем могут быть представлены графическими элементами, которые пользователь комбинирует в нужном порядке для создания нужного протокола. Генерация XML модели при этом будет выполняться программой-конструктором что позволит исключить ошибки синтаксиса, ускорит и облегчит разработку для начинающих специалистов.

Использование в задачах распознавания неизвестных данных.

Исследование устойчивости протоколов и их декодеров к искажению данных, вычисление времени восстановления, определение требуемых характеристик канала при использовании конкретного протокола и вычисление его числовых характеристик.

Сравнительный анализ однотипных протоколов при моделировании реальных информационных систем и воздействий на них.

Автоматическую упаковку любого протокола в любой транспортный протокол, и решение обратной задачи — устранение транспортного протокола из имеющегося блока данных.

Ведение базы данных протоколов в стандартном формате.

Список прикладных вариантов использования предложенной метамодели может быть расширен и дополнен, приведены только основные направления ее использования.

4. Заключение. В данной работе была предложена метамодель произвольного протокола информационного взаимодействия, позволяющая описывать единым образом протоколы разных типов, со степенью детализации достаточной для их содержательного и сравнительного анализа, построения автоматических декодеров, моделирования и т.д. По сравнению с текстовым описанием (спецификацией) протоколов, наиболее часто используемым сегодня, это является несомненным шагом вперед. Использование метамодели для построения моделей конкретных протоколов позволит выйти на новый уровень абстракции при решении многих прикладных и аналитических задач, например, создать и поддерживать пополняемую базу данных протоколов. В дальнейшем эта модель может быть использована в качестве основы для разработки стандарта описания произвольного протокола. Единственным условием использования метамодели является хорошая структурированность описываемого протокола.

Литература

1. *Назаров А.В., Козырев Г.И., Шитов И.В., Обрученков В.П., Древин А.В., Краскин В.Б., Кудряков С.Г., Петров А.И., Соколов С.М., Якимов В.Л, Лоскутов А.И.* Современная телеметрия в теории и на практике. Учебный курс // СПб.: Наука и техника. 2007. 672 с.
2. *Хантер Д., Кэгл К., Гиббонс Д., Озу Н.а, Пиннок Д., Спенсер П.* Введение в XML // Москва. Издательство ЛОРИ. 2006. 638 с.
3. *Bouzerda T., Marchand-Maille S.* A flexible framework for the development of XML protocols: Applications to MRML // Tech. Rep. no. 03.03. University of Geneva. Switzerland. 2003.
4. *Abdullah I.S., Menasc D.A.* Protocol specification and automatic implementation using XML and CBSE // In: Proc. IASTED Int. Conf. Communications, Internet and Information Technology (CIIT2003). Scottsdale. Arizona. USA. 2003. pp. 191–196.
5. *Basu A., Morrisett G., Von Eicken T.* Promela++: a language for constructing correct and efficient protocols // Proc. INFOCOM 98 17th Annual Joint Conf. IEEE Computer and Communications Societies. San Francisco. USA. 1998. pp. 455–462.
6. *Thees J.* Protocol implementation with Estelle- from prototypes to efficient implementations // Proc. Int'l. Workshop on the Formal Description Technique Estelle. France. 1998.
7. *Leduc G., Germeau F.* Verification of Security Protocols Using LOTOS-method and Application // Computer Communications. 2000. vol. 23 no. 12. pp. 1089-1103.

8. *Bolognesi T., Brinksmaa E.* Introduction to the ISO Specification Language LOTOS // Computer Networks and ISDN Systems. 1987. vol. 14. pp. 25–59.
9. *Huang Y., Ravishankar C.* Cicero: A Protocol Construction Language // Tech. rep. CSE-TR-171-93. Michigan. 1993. pp. 1–39.

References

1. Nazarov A.V., Kozyrev G.I.,Shitov I.V., Obruchenkov V.P., Drevin A.V., Kraskin V.B., Kudryakov S.G.,Petrov A.I., Sokovol S.M., Yakimov V.L., Loskutov A.V. *Sovremennaja telemetrija v teorii i na praktike. Uchebnyj kurs* [Modern telemetry in theory and in practice. training course]. Saint-Petersburg.: Science and Technology. 2007. 672 p. (In Russ.).
2. Hunter D., Cagle K., Gibbons D., Ozu N., Pinnock J., Spencer P. *Vvedenie v XML* [Beginning XML]. Moskva. Izdatel'stvo LORI. 2006. 638 p. (In Russ.).
3. Bouzerda T., Marchand-Maille S. A flexible framework for the development of XML protocols: Applications to MRML. Tech. Rep. no. 03.03. University of Geneva. Switzerland. 2003.
4. Abdullah I.S., Menasc D.A. Protocol specification and automatic implementation using XML and CBSE. In: Proc. IASTED Int. Conf. Communications, Internet and Information Technology (CIIT2003). Scottsdale. Arizona. USA. 2003. pp. 191–196.
5. Basu A., Morrisett G., Von Eicken T. Promela++: a language for constructing correct and efficient protocols. Proc. INFOCOM 98 17th Annual Joint Conf. IEEE Computer and Communications Societies. San Francisco. USA. 1998. pp. 455–462.
6. Thees J. Protocol implementation with Estelle- from prototypes to efficient implementations, Proc. Int'l. Workshop on the Formal Description Technique Estelle. France. 1998.
7. Leduc G., Germeau F. Verification of Security Protocols Using LOTOS-method and Application. Computer Communications. 2000. vol. 23 no. 12. pp. 1089-1103.
8. Bolognesi T., Brinksmaa E. Introduction to the ISO Specification Language LOTOS. Computer Networks and ISDN Systems. 1987. vol. 14. pp. 25–59.
9. Huang Y., Ravishankar C. Cicero: A Protocol Construction Language. Tech. rep. CSE-TR-171-93. Michigan. 1993. pp. 1–39.

Романченко Александр Михайлович — старший преподаватель кафедры систем сбора и обработки информации Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: криптография, информационная безопасность, сетевые технологии. Число научных публикаций — 15. rcrst@newmail.ru; ул. Ждановская, д.13, Санкт-Петербург, 197198, РФ; р.т.: +7(812)237-19-60.

Romanchenko Alexander Mikhailovitch — senior lecturer of the information acquisition and data processing department, Mozhaisky Military Space Academy. Research interests: cryptography, information security, network technology. The number of publications — 15. rcrst@newmail.ru; Zdanovskaya str.13, Saint-Petersburg, Russia, 197198; office phone: +7(812)237-19-60.

РЕФЕРАТ

Романченко А.М. **Обобщенная структурная модель протокола информационного взаимодействия.**

Данная работа посвящена разработке структурной метамодели произвольного протокола информационного взаимодействия, предназначенной для унифицированного представления протоколов разных типов. Она может быть использована в качестве стандарта описания произвольного структурированного протокола. Ее использование позволит разрабатывать, использовать, анализировать различные протоколы и протокольные данные единым способом, что существенно упростит решение многих прикладных и аналитических задач.

При анализе предметной области не были обнаружены стандарты, пригодные для описания произвольного протокола и автоматического использования при решении практических задач. Поэтому предложенное направление можно считать новым и перспективным. Разработанная метамодель не подходит для описания слабо-формализованных и слабо-структурированных протоколов, декодирование которых является контекстно-зависимым. Наибольший эффект можно ожидать от использования метамодели при описании новых прикладных протоколов, и описании протоколов транспортного уровня и ниже.

SUMMARY

Romanchenko A.M. **Generalized Structural Metamodel of Information Interaction Protocol.**

This work is devoted to the development of structural metamodel of any information interaction protocol designed for a unified view of different types of protocols. It can be used as a standard for describing arbitrary structured protocol. Its use will allow to develop, use, analyze different protocols and protocol data in a uniform way, which will significantly simplify the solution of many applications and analytical tasks. In the analysis of the subject area standards have not been found suitable for describing arbitrary protocol and automatic use in solving practical problems. Therefore, the proposed course can be considered as a new and promising.

Designed metamodel is not suitable to describe weakly formalized and weakly structured protocol, decoding of which is context-sensitive. The greatest effect can be expected from the use of meta-model in the description of the new application protocols, and the description of transport layer protocols and lower.

УДК 004.056, 519.816

А.В. КРАВЧУК

МОДЕЛЬ ПРОЦЕССА УДАЛЕННОГО АНАЛИЗА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ И МЕТОДЫ ПОВЫШЕНИЯ ЕГО РЕЗУЛЬТАТИВНОСТИ

Кравчук А.В. **Модель процесса удаленного анализа защищенности информационных систем и методы повышения его результативности.**
Аннотация. Рассмотрены подходы к проведению анализа защищенности информационных систем. Предложена модель процесса анализа защищенности информационных систем на основе теории принятия решений. Рассмотрены существующие методы решения проблемы марковских процессов принятия решений в условиях частично наблюдаемой среды.
Ключевые слова: анализ защищенности, тестирование на проникновение, компьютерная атака, марковские процессы, принятие решений, частичная наблюдаемость.

Kravchuk A.V. **The Model of Process of Remote Security Analysis of Information Systems and Methods of Improving it's Performance.**
Abstract. This article considers approaches to remote security analysis of information systems. The model of process of remote security analysis of information systems using decision making theory is proposed. Existing methods to solve partially observable Markov decision processes problem are reviewed.
Keywords: information security analysis, penetration testing, computer attack, Markov processes, decision making, partially observability.

1. Введение. Существующие средства удаленного анализа защищенности информационных систем (ИС) можно условно разделить на 2 класса:

– средства сбора сведений о сетях и обнаружения уязвимостей (Nmap, NetCat, Nessus, MaxPatrol и другие);

– средства тестирования на проникновение (Core Impact, Immunity Canvas, Metasploit Framework и другие).

Соответственно, анализ защищенности ИС предполагает выполнение двух проверок:

1. Проверка на наличие уязвимостей в ИС. Результаты данной проверки характеризуются высоким уровнем ошибок I рода (ложные срабатывания средства сбора сведений о сети и/или анализатора уязвимостей) [1]. Также имеют место ошибки II рода (пропуск уязвимых состояний ИС).

2. Для повышения достоверности анализа защищенности ИС проводится тестирование на проникновение (ТнП), позволяющее оценить информационную безопасность компьютерных сетей посредством формирования и исполнения различных компьютерных атак. Результаты ТнП также характеризуются ошибками II рода, которые обусловлены следующими факторами:

– неполнотой баз данных с эксплойтами (всегда существует вероятность существования эксплойта нулевого дня);

– ситуациями, в которых соотношения между уязвимостями, конфигурациями сети или составляющими её узлами позволяют нанести ИС более серьезный ущерб, нежели использование одиночных уязвимостей. Другими словами, ошибки II рода в данном случае обусловлены не двойками <уязвимость, эксплойт>, а составными компьютерными атаками (СКА). Под СКА будем понимать последовательные многоэтапные действия злоумышленника, включающие как действия по применению эксплойтов, так и удаленный сбор информации о компьютерной сети для формирования последующих этапов СКА, а также различные синтаксические преобразования вредоносного исполняемого кода [2, 3].

Одной из основных проблем при проведении анализа защищенности ИС является повышение результативности проводимого анализа защищенности, которое может быть достигнуто за счет автоматизации рассматриваемого процесса, а также за счет «интеллектуального» моделирования всех возможных сценариев организации СКА злоумышленником и выявления недостатков конфигурирования средств защиты информации (СЗИ). Целью ТнП является выявление максимального количества уязвимостей ИС и недостатков конфигурации СЗИ, последнее из которых возможно за счет использования рационального соотношения действий по сканированию сети и выявлению её уязвимых состояний, с одной стороны, и непосредственному применению эксплойтов, с другой стороны.

Таким образом, целью данной работы является построение модели процесса анализа защищенности ИС, которая соответствует процессу проведения СКА злоумышленником (далее – «модель СКА»). Модель СКА позволит адекватно отразить элементы компьютерной атаки и взаимосвязи между ними, а предлагаемые методы позволят повысить результативность анализа защищенности ИС.

2. Описание предлагаемой модели. Проведенный сравнительный анализ подходов к моделированию (СЗИ) и компьютерных атак позволил выделить следующие основные классы моделей, построенных с использованием теорий вероятностей; нечетких множеств; игр; графов; автоматов; сетей Петри; случайных процессов. Сравнительный анализ существующих моделей проводился в соответствии с основными фундаментальными проблемами системно-кибернетических исследований:

– построения исследовательской модели «система-среда»;

– анализа свойств системы;

– наблюдения системы;

– выбора альтернативных вариантов [4].

Пусть некоторый программный агент (ПА) управляет проведением СКА на целевую систему ЦС, под которой будем понимать компьютерную сеть, состоящую, по крайней мере, из одного узла. Рассмотрим ЦС, которая в произвольный момент времени может находиться в одном из N различных состояний, $S = \{s_0, s_1, \dots, s_N,\}$, где S – пространство состояний. Для дискретных систем запись уравнений в пространстве состояний основывается не на дифференциальных, а на разностных или рекуррентных уравнениях.

Состояние ЦС для ПА будет являться дискретной случайной величиной, то есть в результате проведения атакующих воздействий он может принять то или иное предположение о состоянии ЦС, причем неизвестно заранее, какое именно. С практической точки зрения пространство состояний представляет собой совокупность конфигураций узлов и топологии сети, а состояние ЦС может описываться следующими переменными: $Node = \{M_0, M_1, \dots, M_N\}$, $Port\_num = \{1 \dots 65535\}$, $Port\_state = \{open, closed, filtered\}$, $OS = \{WinXP, Linux - 2.2.6 \dots\}$, $Sys\_state = \{stable, vuln, compromised, updated\}$ и т.д.

ПА не имеет достаточной информации для того, чтобы сделать вывод о реальном состоянии ЦС. Он имеет возможность выполнять доступные ему действия. В каждый дискретный момент времени t_i в распоряжении ПА имеются множество допустимых действий $A = \{a_0, a_1, \dots a_M\}$, которое состоит из трех подмножеств:

– множества действий по применению эксплойтов, A_{exp};

– множества действий по сканированию сети, идентификации ОС, сервисов и их уязвимых состояний, A_{scan};

– множества действий по модификации синтаксических характеристик вредоносного кода, $A_{obfuscate}$.

Таким образом, $A = A_{\text{exp}} \cup A_{scan} \cup A_{obfuscate}$.

Фактическое состояние ЦС является скрытым от непосредственного наблюдения ПА. Отсутствие возможности прямого наблюдения состояния ЦС обусловлено следующими факторами:

1. Несмотря на различные реализации сетевых протоколов (в том числе стека протоколов в различных ОС) и клиент-серверной архитектуры, которые предоставляют широкие возможности по идентификации ОС, сервисов и их уязвимых состояний, в ходе протокольного обмена данными с ЦС даже при отсутствии влияния среды, под которой будем понимать СЗИ, имеет место априорная неопределенность идентификации состояния ЦС.

2. Существенное влияние на проведение СКА оказывает среда, представленная СЗИ (межсетевые экраны, системы обнаружения атак, антивирусное ПО, установленное на узлах сети, штатные средства ЗИ уровня ОС). По своим характеристикам среда является частично наблюдаемой.

При этом СКА должна закончиться в случаях:

– наступления некоторого события, которое его остановит (срабатывание СЗИ, неудачное применение эксплойта, обусловленное неудовлетворительными результатами идентификации уязвимых состояний ЦС);

– достижения цели СКА. Под целью СКА понимается перевод ЦС в некоторое терминальное (скомпрометированное) состояние и последующее выполнение деструктивных действий.

Каждое действие, выполняемое ПА, достигает намеченной промежуточной цели с вероятностью p_n. Значения p_n достигают максимальных значений при условии, что СЗИ не произвело ни одной записи об атаке, и минимальных, если СЗИ заблокировало сеанс связи (сессию). Для обозначения вероятности достижения ЦС состояния s_{t+1}, если в состоянии s_t ПА было выполнено действие $a \in A$, будем использовать выражение $T(s_t, a, s_{t+1}) = P(s_{t+1} | s_t, a)$ и называть его моделью перехода или функцией перехода. Модель перехода представляет собой трехмерную таблицу переходных вероятностей и может быть представлена динамической байесовской сетью.

В качестве допущения примем, что процесс проведения СКА является марковским процессом первого порядка, то есть текущее состояние ЦС зависит только от предыдущего состояния и не зависит от каких-либо более ранних состояний. Таким образом, вероятность перевода ЦС в состояние $s' = s_t$ из состояния $s = s_{t-1}$ зависит только от s и выполненного ПА действия a, а не от всей истории состояний и действий. Для оценивания фактического состояния ЦС ПА имеет возможность анализировать поступающие в ответ на выполняемые им действия символы наблюдения (реакции ЦС). На основании оценок состояния ЦС ПА принимает решение о дальнейших действиях. Для обозначения вероятности получения символа наблюдения $o \in O$ при нахождении ЦС в состоянии s после выполнения ПА действия a на предыдущем шаге будем использовать выражение $Z(s', a, o) = P(o_t = o \mid s_t = s', a_{t-1} = a)$ и называть его моделью наблюдения или функцией наблюдения.

Для учета результативности и скрытности СКА целесообразно использовать функцию вознаграждения (reward function) и функцию полезности (utility function). Функция полезности отображает последо-

вательность полученных символов наблюдений, выполненных ПА действий и состояний ЦС на вещественное число, которому в данной работе соответствует степень достижения цели программным агентом или результативность СКА. Она будет являться критерием или целевой функцией.

ПА должен принимать рациональные решения на основании анализа поступаемых символов наблюдения таким образом, чтобы максимизировать функцию полезности. В общем случае доход, полученный за несколько шагов, является случайной величиной, зависящей от начального состояния ЦС и принимаемых в каждый момент времени решений [5].

Условия ТнП накладывают ограничения на время проведения СКА. Будем считать, что временной интервал принятия решений конечен, то есть существует такое фиксированное критическое время $t_{\text{кр}}$, после которого проведение СКА не имеет смысла.

Конечность временного интервала принятия решений, с одной стороны, делает модель СКА более адекватной, а, с другой, значительно усложняет её, т.к. в данном случае оптимальное действие для конкретного состояния ЦС со временем может измениться. При выборе конечного временного интервала принятия решений оптимальная стратегия будет нестационарной. В случае бесконечного временного интервала оптимальная стратегия будет стационарной, т.к. нет смысла проводить различные действия для одного и того же состоянии ЦС в разное время. Следует отметить, что понятие «бесконечного интервала принятия решений» говорит лишь о том, что для выполнения действий не устанавливаются фиксированные сроки.

Несмотря на то, что временной интервал принятия решений конечен, может сложиться ситуация, когда $t_{\text{кр}} \longrightarrow \infty$ и в результате действий ПА ЦС не достигнет терминального состояния, то общая полезность, связанная с аддитивными вознаграждениями будет бесконечной. Для решения данной проблемы целесообразно использовать поправочный коэффициент $\gamma \in [0,1)$, называемый также коэффициентом обесценивания или коэффициентом переоценки. Он описывает предпочтение ПА текущих вознаграждений перед будущими вознаграждениями. Если коэффициент переоценки γ близок к 0, то вознаграждения, которые должны быть получены в отделенном будущем, рассматриваются как малозначащие. Он представляет модель изменения предпочтений злоумышленника во времени. Использование коэффициента обесценивания будет гарантировать, что значение функции полезности будет конечным. В реальных условиях проведения СКА количество шагов – конечно, однако введение коэффициента обесценивания по-

зволяет повысить производительность алгоритма поиска «оптимальной» стратегии.

С учетом сказанного выше функция полезности СКА примет вид:

$$U_h\left(s_0, s_1, \dots, s_{t_{\text{кр}}};\ a_0, a_1, \dots, a_{t_{\text{кр}}}\right) = R(s_0, a_0) + \gamma R(s_1, a_1) + \gamma^2 R(s_2, a_2) \dots + \gamma^{t_{\text{кр}}} R(s_{i-1}, a_{i-1}),\ i = \overline{0, t_{\text{кр}}}. \quad (1)$$

Тогда любая оптимальная стратегия в обобщенном представлении удовлетворяет следующему соотношению:

$$\pi^* = \underset{\pi}{argmax}\, M\left[\sum_{t=0}^{t_{кр}-1} (\gamma^t R(s_t, a_t) \mid \pi, s_0 = s)\right]. \quad (2)$$

Последним, не описанным свойством СКА недостающим для формирования её модели, является неопределенность среды. Если абстрагироваться от неопределенности среды, то представляется возможным рассматривать получаемые символы наблюдений, $o_k \in O$, в качестве состояний ЦС, $s_i \in S$.

Однако результаты проведенных экспериментов показывают, что данный подход неприемлем, поскольку ЦС может находиться в таких скрытых состояниях, что при одинаковых символах наблюдения, получаемых в ответ на атакующие воздействия ПА, перевод ЦС в другое состояние потребует различных действий. Данное противоречие между теорией и практикой возникает вследствие допущения о марковских свойствах процесса проведения СКА и неопределенностями среды межсетевого взаимодействия, обусловленных функционированием СЗИ и структурно-функциональными характеристиками используемых протоколов передачи данных.

Таким образом, возникает проблема потери информации об истории предыдущих действий и наблюдений. В пошаговом представлении история может быть представлена в виде $h_t = \{\langle a_0\rangle, \langle o_1, a_1\rangle, \dots, \langle o_{t-1}, a_{t-1}\rangle, \langle o_t\rangle\}$. Хранение истории предыдущих действий и наблюдений требует больших затрат памяти и приводит к усложнению и без того информационно насыщенной модели. Вместо этого представляется возможным свести всю необходимую информацию о предыдущих атакующих воздействиях и полученных символах наблюдений в доверительные состояния, которые позволят решить проблему потери информации об истории предыдущих действий и наблюдений.

Доверительное состояние, b – дискретное распределение апостериорных вероятностей на множестве фактических состояний ЦС S, сопоставляющее каждому состоянию ЦС вероятность нахождения в нём. Доверительное состояние b есть стохастический вектор в момент времени t:

$$b_t = \langle b(s_0), b(s_1), \dots, b(s_{N-1}) \rangle, \quad (3)$$

где $N = |S|$ - количество возможных состояний ЦС, а $b_t(s_i)$ представляет собой вероятность нахождения ЦС в состоянии $s_i, i = \overline{1,N}$ в момент времени t. В соответствии с основным постулатом теории вероятностей $0 \leq b_t(s_i) \leq 1 \; \forall \; s_i \in S$. Позиция элемента (значения вероятности) в стохастическом векторе соответствует номеру состояния ЦС. Во избежание понятийной путаницы, отметим, что $b_t \neq b_t(s_i)$ – в первом случае, b_t – это случайный вектор, сформированный из значений вероятностей нахождения ЦС в состояниях $s_i \in S$, а во втором, $b_t(s_i)$ – конкретное значение апостериорной вероятности нахождения ЦС в состоянии $s_i \in S$ в момент времени t.

Каждый элемент доверительного состояния можно представить в следующей форме:

$$b_t(s) = P(s_t = s | h_t, b_0), \quad (4)$$

В работе [6] было доказано, что в любой момент времени t доверительное состояние b_t является достаточной статистикой последовательности полученных ПА символов наблюдений и выполненных на их основании действий до момента времени t. Доверительное состояние можно рассматривать как текущее состояние информации о внутреннем состоянии ЦС или как информационный вектор ПА, на основании которого он принимает решения (проводит СКА).

Таким образом, история выполненных действий и полученных символов наблюдения может быть представлена в виде информационного стохастического вектора ПА или апостериорного распределения вероятностей, каждый элемент которого есть:

$$b_t(s) = P(s_t = s | o_t, a_{t-1}, o_{t-1}, \dots, a_0). \quad (5)$$

Динамика изменения информационного вектора b является критическим фактором для проведения ТнП.

Введение доверительных состояний позволяет произвести декомпозицию проблемы рационального выбора атакующих воздействий с учетом «оптимальной» стратегии и блока оценивания фактического состояния ЦС на основании получаемых символов наблюдений.

С учетом введенных параметров и характеристик предметной области и математического аппарата МППРЧНС представляется целесообразным представить реализацию решения научной задачи поиска рациональной стратегии проведения СКА в виде интеллектуального модуля, представленного на рисунке 1.

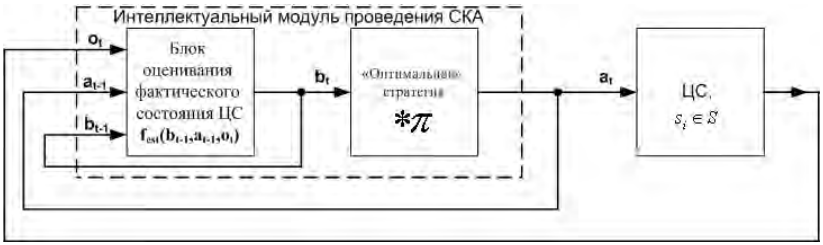


Рис. 1. Интеллектуальный модуль проведения СКА

Первый элемент интеллектуального модуля проведения СКА представлен блоком оценивания фактического состояния ЦС (БОФСЦС). Он отвечает за актуализацию распределения вероятностей нахождения ЦС в скрытых (ненаблюдаемых) состояниях, составляющих доверительного состояние ЦС. Поддержание распределения вероятностей в актуальном состоянии позволяет корректно отражать фактическое состояние ЦС и выполнять действия рациональным способом.

В качестве входных данных БОФСЦС принимает предыдущее доверительное состояние b_{t-1}, предыдущее атакующее воздействие a_{t-1} и текущий символ наблюдения o_t. На выходе БОФСЦС рекурсивным способом генерируется обновленное доверительное состояние или информационный вектор программного агента.

БОФСЦС позволяет рекурсивно рассчитать доверительное состояние за счет применения теоремы Байеса к двум базовым моделям: модели переходов $T(s, a, s')$ и модели наблюдения $Z(s, a, o)$. Если доверительное состояние не может быть рассчитано БОФС, то вероятность перехода $b_{t-1} \longrightarrow b_t$ будет равна нулю. При этом, учитывая введенные доверительные состояния, доверительная модель перехода $T(s, a, s')$ примет вид:

$$\begin{gathered}\tau(b, a, b') = P(b_t|a_{t-1}, b_{t-1}) = P(b_t = b'|a_{t-1} = a,\ b_{t-1} = b) = \\ = \sum_{o \in O} P(b'|a, b, o) * P(o|a, b\ ) == \sum_{o \in O} P(b_t = b'|a_{t-1} = \\ a, b_{t-1} = b, o_t = o) * P(o_t = o|a_{t-1} = a, b_{t-1} = b\ ),\end{gathered} \quad (6)$$

где:

$$P(b'|a, b, o) = P(b_t|a_{t-1}, b_{t-1}, o_t) = \begin{Bmatrix} 1, f_{est}(b_{t-1}, a_{t-1}, o_t) = b_t \\ \\ 0, \text{в противном случае} \end{Bmatrix}. \quad (7)$$

Стоит отметить, что при выполнении атакующих воздействий $A_{scan} \in A$ переход ЦС из одного состояния в другое отсутствует. Данный класс действий влияет только на динамику изменения информационного стохастического вектора ПА.

Тогда каждый элемент обновленного доверительного состояния b_t в момент времени t может быть вычислен рекурсивно на основании апостериорной вероятности нахождения ЦС в состоянии $s \in S,$ действия a_{t-1} и символа наблюдения o_t, полученного в результате выполнения действия a_{t-1}.

В соответствии с работами [7,8] обновленный элемент доверительного состояния или обновленную апостериорную вероятность нахождения ЦС в состоянии $s' = s_t$ можно вычислить по формуле:

$$\begin{aligned} b_t(s') = P(s' \mid b_{t-1}, a_{t-1}, o_t) = \frac{P(s', b_{t-1}, a_{t-1}, o_t)}{P(b_{t-1}, a_{t-1}, o_t)} = \\ = \frac{P(o_t \mid s', b_{t-1}, a_{t-1}) P(s' \mid b_{t-1}, a_{t-1}) P(b_{t-1}, a_{t-1})}{P(o_t \mid a_{t-1}, b_{t-1}) P(b_{t-1}, a_{t-1})} \\ = \frac{P(o_t \mid s', b_{t-1}, a_{t-1}) P(s' \mid b_{t-1}, a_{t-1})}{P(o_t \mid a_{t-1}, b_{t-1})} = \\ = \frac{1}{P(o_t \mid a_{t-1}, b_{t-1})} Z(s', a_{t-1}, o_t) \sum_{s \in S} T(s, a_{t-1}, s') * b_{t-1}(s), \end{aligned} \quad (8)$$

где $P(o_t \mid a_{t-1}, b_{t-1})$ –полная вероятность получения символа наблюдения o_t в момент времени t после выполнения действия a_{t-1} из доверительного состояния b_{t-1}, представляемая как нормирующий коэффициент [9]. Суммирование производится по всем состояниям, из которых выполнение программным агентом действия a_{t-1} приводит к переводу ЦС в состояние s'.Нормирующий коэффициент определяется как:

$$P(o_t \mid a_{t-1}, b_{t-1}) = \sum_{s' \in S} Z(s', a_{t-1}, o_t) \sum_{s \in S} T(s, a_{t-1}, s') * b(s_t). \quad (9)$$

Нормирующий множитель вводится для того, чтобы сумма вероятностей обновленного доверительного состояния b_{t+1} была равна 1.

Выражение (8) задает функцию перехода из информационного состояния b_{t-1} в информационное состояние b_t и представляет собой Байесовский фильтр. Результатом рекурсивного применения формулы (8) ко всем состояниям $s \in S$ станет обновленное доверительное состояние, представленное стохастическим вектором b.

Таким образом, введение БОФСЦС позволяет ПА производить принимать решения на основании доверительного состояния или информационного вектора вместо истории атакующих воздействия и полученных символов наблюдений.

Вторым элементом является «оптимальная» (рациональная) стратегия, отображающая множество доверительных состояний в множество атакующих воздействий ПА:

$$^{*}\pi: \mathcal{B} \longrightarrow A. \tag{10}$$

Данный элемент отвечает за формирование атакующих воздействий и представляет собой функцию от доверительного состояния ЦС, отображающую текущее доверительное состояние в атакующее воздействие. Другими словами, после того, как ПА вычисляет доверительное состояние ЦС, он должен выбрать атакующее воздействие на основании доверительного состояния ЦС.

Рассмотренные выше параметры и характеристики задачи последовательного принятия решений в случае частично наблюдаемой среды с моделью перехода, моделью наблюдения, доверительными состояниями и мгновенными вознаграждениями позволяют сформировать модель СКА на основе математического аппарата марковских процессов принятия решений в условиях частично наблюдаемой среды (МППРЧНС). СКА задается следующим кортежем из 7 элементов:

$$\text{СКА} = \langle S, A, O, T(s,a,s'),\ Z(s,a,o)R(s,a), b_0 \rangle, \tag{11}$$

где:

1. $S = \{s_0, s_1, \ldots, s_N\}$ – конечное множество фактических (скрытых от непосредственного наблюдения) состояний целевой системы. Под множеством состояний ЦС понимается множество конфигураций ИТКС и составляющих её узлов.

2. $A = \{a_0, a_1, \ldots, a_M\}$– конечное множество действий, доступных ПА.

3. $O = \{o_0, o_1, \ldots, o_K\}$ – конечное множество символов наблюдений, получаемых ПА при нахождении ЦС в состояниях $S = \{s_0, s_1, \ldots, s_N\}$.

4. $T(s,a,s'): S \times A \times S \longrightarrow [0,1]$ – модель перехода, задающая условные переходные вероятности между состояниями, то есть $T(s,a,s') = P(s_t = s' |\ s_{t-1} = s, a_{t-1} = a)$ представляет вероятность того, что ЦС будет переведена из состояния $s_{t-1} = s$ в состояние $s_t = s'$ в результате выполнения ПА действия $a_{t-1} = a \in A$. Поскольку T является распределением условных переходных вероятностей, то:

$$\sum_{s' \in S} T(s,a,s') = 1, \forall (s,a). \tag{12}$$

В данной работе в качестве допущения принимается, что модель перехода $T(s, a, s')$ инвариантна по времени, то есть стохастическая матрица T не изменяется со временем. Для учёта переходных вероятностей, зависящих от времени, переменная состояния s должна включать в себя привязанную ко времени переменную.

5. $Z(s', a, o): A \times S \times O \longrightarrow [0,1]$ – модель наблюдения. Для каждого результирующего состояния $s' \in S$, каждого действия $a \in A$, каждого символа наблюдения $o \in O$, модель наблюдения $Z(s', a, o)$ определяет вероятность получения символа наблюдения $o_t = o \in O$ в результате выполнения ПА действия $a_{t-1} = a \in A$, приводящего к переходу ЦС в результирующее состояние s'. Другими словами $Z(s', a, o) = P(o_t = o \mid s_t = s', a_{t-1} = a)$. Данная условная вероятность определена для всех троек вида (s', a, o), для которых имеет место:

$$\sum_{o \in O} Z(s', a, o) = 1, \forall (s', a). \tag{13}$$

6. $R(s, a): S \times A \longrightarrow \mathbb{R}$ – функция мгновенного вознаграждения, присваивающая некоторое числовое значение, являющееся оценкой результативности и скрытности и называемое доходом или вознаграждением, за выполнение программным агентом атакующего воздействия a при нахождении ЦС в состоянии s. Вознаграждение $r_t = R(s, a)$ в момент времени t может принимать как положительные, так и отрицательные значения. В качестве допущения в данной работе предполагается, что вознаграждение ограничено сверху и снизу, $R_{min} < R < R_{max}$. Целью ПА является максимизация суммы вознаграждений, получаемых в процессе проведения СКА в течение некоторого времени $t < t_{\text{кр}}$. В общем виде цель ПА может быть представлена как максимизация математического ожидания суммарного вознаграждения:

$$M\left[\sum_{t=0}^{t_{\text{кр}}-1} \gamma^t r_t\right], \tag{14}$$

где $M[\ ]$ – математическое ожидание, r_t – мгновенное вознаграждение в момент времени t, и γ: $0 \leq \gamma < 1$ – коэффициент переоценки, введение которого гарантирует ограниченность вознаграждений, определяет предпочтения ПА по непосредственному применению эксплойтов, либо по увеличению точности идентификации ЦС посредством действий по её сканированию, а также позволяет повысить производительность алгоритма поиска «оптимальной» стратегии проведения СКА. Учитывая, что фактические состояния ЦС являются непосредственно ненаблюдаемыми, ПА принимает решения на основе информационно-

го вектора b_t. Тогда функция мгновенного вознаграждения, в которой вознаграждение зависит от текущего доверительного состояния $b_t = b \in \mathcal{B}$ и действия $a_t = a \in A$, выполненного ПА, из данного доверительного состояния, примет вид:

$$R_B(b,a) = \sum_{s \in S} b(s) * R(s,a),\ \forall b(s): \sum_{s \in S} b(s) = 1. \quad (15)$$

Приведенная формула означает, что ПА получает вознаграждение$r = R_B(b,a)$ за предположение о том, что ЦС пребывает в некотором состоянии. Данное допущение оправдано, поскольку значение функции оценивания фактического состояния ЦС $f_{est}(b_t, a_t, o_{t+1})$ вычисляется на основании получения символа наблюдения и модели перехода состояний ЦС. С формальной точки зрения мгновенное вознаграждение для случая доверительных состояний, $r = R_B(b,a)$, есть не что иное, как математическое ожидание. Тогда задача выбора последовательности атакующих воздействий, составляющих СКА, сводится к максимизации математического ожидания дохода, получаемого в $t_{\text{кр}}$-шаговом процессе проведения СКА при заданном начальном доверительном состоянии b_0.

7. b_0 – начальное дискретное распределение вероятностей на множестве фактических состояний ЦС S, сопоставляющее каждому состоянию из множества S вероятность нахождения в нём ЦС. Для решения проблемы частичной наблюдаемости среды программный агент должен осуществлять выбор атакующих воздействий на основании множества доверительных состояний ЦС $\mathcal{B} = \{b_0, b_1, \dots, b_n\}$, а не её фактических состояний S.

Таким образом, все рассмотренные элементы модели: состояния ЦС S, атакующие воздействия A, символы наблюдений O, вознаграждения R и три распределения вероятностей T, O, b_0 формируют вероятностную модель процесса проведения СКА. При этом четыре последние элемента задаются с помощью соответствующих матриц.

С учетом приведенных рассуждений, графическое представление модели СКА на основе марковских процессов принятия решений в условиях частично наблюдаемой среды примет вид, приведенный на рисунке 2.

Модель, представленная на рисунке 2 требует дополнительных пояснений. В момент времени $t-1$ ЦС пребывает в некотором состоянии $s_i \in S$, где $i = \overline{1,N}$. ПА, зная распределение вероятностей нахождения ЦС в состояниях $s_i \in S$, b_{t-1} выполняет действие $a_{t-1} \in A$, что приводит к мгновенному получению вознаграждения $r_{t-1} = R_B(b_{t-1}, a_{t-1})$ и вызывает переход в некоторое новое (или в то же) состояние $s \in S$ с вероятностью $P(s_t = s' | s_{t-1} = s, a_{t-1} = a)$.

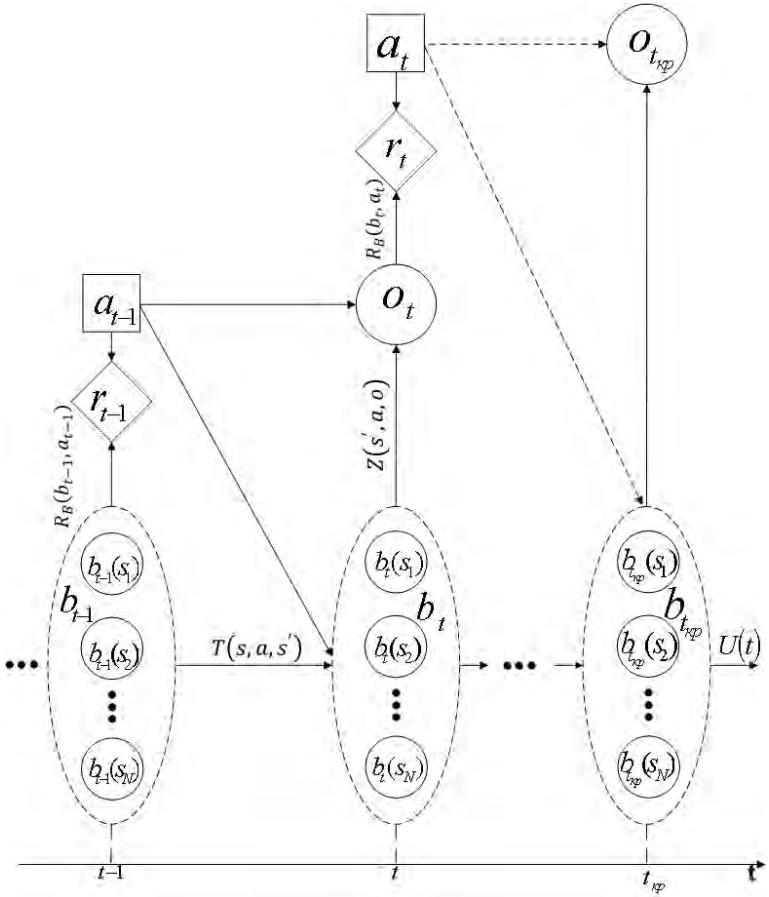


Рис. 2. Графическое представление модели СКА на основе МППРЧНС

Три компоненты модели S, A и T формируют ядро марковского процесса принятия решений и определяют динамику марковского процесса принятия решений в условиях частично наблюдаемой среды. В отличие от обычного марковского процесса принятия решений ПА не имеет возможности непосредственного наблюдения состояния ядра МППР в процессе принятия решений. Вместо этого ему предоставляется возможность получить символ наблюдения $o_t \in O$ с вероятностью $P(o_t = o \mid s_{t-1} = s, a_{t-1} = a)$.

В отличие от скрытой марковской модели, функционирующей автономно, МППРЧНС управляется действиями, выбираемыми про-

граммным агентом. Стоит отметить, что допущение о марковских свойствах процесса проведения СКА не всегда соответствует действительности. Для устранения этого недостатка были введены доверительные состояния. Соответственно, решение о выполнении действия ПА принимает на основании информации о доверительном состоянии ЦС.

Решением задачи МППРЧНС является нахождение оптимальной стратегии, то есть последовательности атакующих воздействий $\{A_t\}_{t=0,1,\dots,t_{\text{кр}}}$, приводящей к достижению цели СКА. Качество стратегии оценивается функцией полезности, являющейся математической функцией от мгновенных вознаграждений. Целью ПА является оптимизация функции полезности, которая в свою очередь является функцией параметров скрытности и результативности СКА.

Тем не менее, из-за частичной наблюдаемости, поиск строго оптимальной стратегии влечет чрезмерные затраты вычислительных мощностей, а в большинстве случаев нахождение строго оптимальной стратегии невозможно. Кроме того, возникает ряд проблем при применении аппарата МППРЧНС в сфере информационной безопасности в целом и в ТнП в частности. Во-первых, это необходимость корректно задать пространство состояний S, которое будет представлено конфигурационными параметрами сети и составляющих ее узлов. Во-вторых, необходимость задать на основании экспериментальных данных 2 таблицы с вероятностями $T(s, a, s')$, $Z(s', a, o)$, и одну $R(s, a)$ экспертным способом, а также начальное доверительное состояние b_0. И, наконец, в третьих, вычислять после каждого выполненного действия новое доверительное состояние. Другими словами, решение задачи МППРЧНС упирается в «проклятие размерности».

3. Анализ методов решения задачи МППРЧНС. Решением задачи МППРЧНС является «оптимальная» стратегия, обеспечивающая максимум ожидаемого суммарного дохода. Стратегия $\pi: \mathcal{B} \longrightarrow A$ задает действие a для каждого доверительного состояния $b \in \mathcal{B}$ и порождает функцию ценности (value-function) $V(b, \pi)$, которая определяет ожидаемую сумму вознаграждений за выполнение стратегии π, начиная с доверительного состояния b.

Функция ценности может быть вычислена по следующей формуле:

$$V(b, \pi) = \mathrm{M}\left[\sum_{t=0}^{t_{\text{кр}}-1} \gamma^t R(s_t, a_t) | b, \pi\right]. \quad (16)$$

Графически стратегия может быть представлена как граф, узлами которого являются доверительные состояния, а дуги – действиями ПА.

Для решения задачи МППРЧНС, то есть для вычисления оптимальной стратегии выбора действий, за последние десятилетия было предложено множество алгоритмов, которые можно разделить на два класса: алгоритмы времени, близкого к реальному, и автономные алгоритмы.

Автономные алгоритмы [10-13] определяют наилучшее действие, подлежащее выполнению, для всех возможных ситуаций, до начала проведения процесса принятия решения, то есть до начала ТнП. Использование перечисленных алгоритмов для проведения ТнП сопровождается определенными трудностями, основной из которых является необходимость повторного перерасчета всей стратегии при малейшем изменении в конфигурации компьютерной сети. Наиболее перспективными среди автономных алгоритмов на данный момент являются точечные алгоритмы (point-based), которые обеспечивают перерасчет функции ценности только для некоторых выбранных доверительных состояний $b \in \mathcal{B}$.

Алгоритмы времени, близкого к реальному [14-18], разработаны для преодоления «проклятия размерности» и осуществляют планирование только для текущего информационного вектора ПА или доверительного состояния. Другими словами, позволяют вычислять около оптимальные локальные стратегии на каждом шаге принятия решений во время исполнения алгоритма. В ряде работ, например в [19], они называются агентно-ориентированными алгоритмами поиска. Их основными недостатками является ограничения, связанные с работой в реальном времени. Наиболее перспективным среди алгоритмов времени, близкого к реальному, является детерминированный разреженный алгоритм частично наблюдаемого дерева (Determinized Sparse Partially Observable Tree, DESPOT).

Несмотря на большое количество существующих алгоритмов поиска около оптимальной стратегии выполнения действий, ни один из них, взятый по отдельности не может быть использован для моделирования ТнП для средних и больших сетей (50 и больше узлов). Для решения данной проблемы предполагается разработать комбинированный алгоритм.

4. Заключение. В работе рассмотрен новый подход к моделированию компьютерных атак с позиции злоумышленника или, другими словами, для моделирования процесса удаленного анализа защищенности информационных систем. Подход был проверен с использованием двух свободно распространяемых пакетов программ – SARSOP и DESPOT [20].

Стоит отметить, что проблема нахождения около оптимальной стратегии является NP-трудной [21]. На данный момент применение марковских процессов принятия решений в условиях частично наблюдаемой среды для моделирования ТнП ограничивается малыми сетями (до 20 узлов). Для его применения к сетям большей размерности требуются дополнительные способы аппроксимации как по количеству вариантов, из которых надо выбирать решения (множества доверительных состояний $\mathcal{B}$), так и по количеству итераций рекуррентного алгоритма вычисления максимального значения функции ценности.

Таким образом, для использования методов МППРЧНС для проведения удаленного анализа защищенности информационных систем в средних и больших компьютерных сетях требуется проведение дальнейших исследований по повышению производительности поиска рациональной (около оптимальной) стратегии.

Литература

1. *Кравчук А.В., Еремеев М.А.* Анализ методов распознавания вредоносных программ // Вопросы защиты информации. 2014. №3. С. 44–51.
2. *Кравчук А.В., Еремеев М.А., Потерпеев Г.Ю.* Модель и методы дистанционного контроля мобильных персональных устройств // Материалы 22-й НТК «Методы и технические средства обеспечения безопасности информации». СПб. 2013. С. 24–26.
3. *Кравчук А.В., Еремеев М.А.* Подход к моделированию компьютерных атак // Материалы 23-й НТК «Методы и технические средства обеспечения безопасности информации». СПб. 2014. С. 69–71.
4. *Калинин В.Н., Резников Б.А., Варакин Е.И.* Теория систем и оптимального управления. В 2 ч. Ч.1. Основные понятия, математические модели и методы анализа систем // Л.:ВИКИ имени А.Ф. Можайского. 1979. 319 с.
5. *Макаров И.М., Виноградская Т.М., Рубчинский А.А.* Теория выбора и принятия решений: Учебное пособие // М.: Наука. 1982. 328 с.
6. *Astrom K.J.* Optimal control of Markov processes with incomplete state information // Journal of mathematical analysis and applications. 1965. no. 10. pp. 174-205.
7. *Стратонович Р. Л.* Условные марковские процессы и их применение к теории оптимального управления // М.: Изд-во МГУ. 1966. 319 с.
8. *Jazwinski A.H.* Stochastic processes and filtering theory // New York: Academic Press. 1970. 391 p.
9. *Ross S., Pineau J.* Online Planning Algorithms for POMDPs // Journal of Artificial Intelligence Research. 2008. №32. pp. 663–704.
10. *Hauskrecht M.* Value-function approximations for partially observable Markov decision processes // Journal of Artificial Intelligence Research. 2000. №13. pp. 33–94.
11. *Pineau J., Gordon G., Thrun S.* Point-based value iteration: an anytime algorithm for POMDPs // Proceedings of the International joint conference on artificial intelligence (IJCAI-03). 2003. pp. 1025–1032.
12. *Braziunas D., Boutilier C.* Stochastic local search for POMDP controllers // Proceedings of the 19-th National conference on artificial intelligence (AAAI-04). 2004. pp. 690–696.
13. *Smith T., Simmons R.* Point-based POMDP algorithms: improved analysis and implementation // Proceedings of the 21th conference on uncertainty in artificial intelligence (UAI-05). 2005. pp. 542–547.

14. *Satia J.K., Lave R.E.* Markovian decision processes with probabilistic observation of states // Management Science. 1973. vol. 20(1). pp. 1–13.
15. *Barto A.G., Bradtke S.J., Singhe S.P.* Learning to act using real-time dynamic programming // Artificial Intelligence. 1995. vol. 72 (1). pp. 81–138.
16. *Washington R.* BI-POMDP: bounded, incremental partially observable Markov model planning. // Proceedings of the 4th European conference on planning. 1997. pp. 440–451.
17. *McAllester D., Singh S.* Approximate planning for factored POMDPs using belief state simplification // Proceedings of the 15th annual conference on uncertainty in artificial intelligence (UAI-99). 1999. pp. 409–416.
18. *Shani G., Brafman R., Shimony S.* Adaptation for changing stochastic environments through online POMDP policy learning // Proceedings of the workshop on reinforcement learning in non-stationary environments, ECML. 2005. pp. 61–70.
19. *Koenig S.* Agent-centered search // AI Magazine. 2001. vol. 22(4). pp. 109–131.
20. Approximate POMDP planning software. URL: http://bigbird.comp.nus.edu.sg/pmwiki/farm/appl/ (дата обращения 18.01.2015).
21. *Lusena C., Goldsmith J., Mundhenk M.* Nonapproximability results for partially observable Markov decision processes // Journal of artificial intelligence research. 2001. vol. 14. pp. 83–103.

References

1. Kravchuk A.V., Eremeev M.A. [Analysis of malware recognition methods]. *Voprosy zaschity informatcii – The question of information protection*. 2014. vol. 3. pp. 44–51. (In Russ.).
2. Kravchuk A.V., Eremeev M.A., Poterpeev G.J. [Model and methods of remote control of mobile personal devices]. *Trydy 22-oi naychno-tehnicheskoi konferencii Metody i tehnicheskie sredstva obespecheniya informacionnoi bezopasnosti* [Proceedings of the 22-th Scientific and Technical Conference on Methods and Technical Security Facilities]. SPb. 2013. pp. 24–26. (In Russ.).
3. Kravchuk A.V., Eremeev M.A. [Approach to modeling computer network attacks]. *Trydy 23-ei naychno-tehnicheskoi konferencii Metody i tehnicheskie sredstva obespecheniya informacionnoi bezopasnosti* [Proceedings of 23-th Scientific and Technical Conference on Methods and Technical Security Facilities]. SPb. 2014. pp. 69–71. (In Russ.).
4. Kalinin V.N., Reznikov B.A., Varakin E.I. *Teorija sistem i optimal'nogo ypravlenia. V 2 ch. Ch.1. Osnovnye ponyatia, matematicheskie modeli i metody analiza sistem* [Theory of systems and optimal control. Main definitions, mathematical models and system analysis methods]. L.:VIKI imeni A.F. Mozhayskogo. 1979. 319 p. (In Russ.).
5. Makarov I.M., Vinogradskaya T.M., Rubchinsky A.A. *Teoria vybora i prinyatia reshinii: Uchebnoe posobie* [The theory of choice and decision-making: tutorial]. M.: Nayka. 1982. 328 p. (In Russ.).
6. Astrom K.J. Optimal control of Markov processes with incomplete state information. Journal of mathematical analysis and applications. 1965. no. 10. pp. 174–205.
7. Stratonovich R. L. Conditional Markov Processes and Their Application to the Theory of Optimal Control. M.: MGU. 1966. 319 p.
8. Jazwinski A.H. Stochastic processes and filtering theory. New York: Academic Press. 1970. 391 p.
9. Ross S., Pineau J. Online Planning Algorithms for POMDPs. Journal of Artificial Intelligence Research. 2008. vol. 32. pp. 663–704.
10. Hauskrecht M. Value-function approximations for partially observable Markov decision processes. Journal of Artificial Intelligence Research. 2000. vol. 13. pp. 33–94.

11. Pineau J., Gordon G., Thrun S. Point-based value iteration: an anytime algorithm for POMDPs. Proceedings of the International joint conference on artificial intelligence (IJCAI-03). 2003. pp. 1025–1032.
12. Braziunas D., Boutilier C. Stochastic local search for POMDP controllers. Proceedings of the 19-th National conference on artificial intelligence (AAAI-04). 2004 pp. 690–696.
13. Smith T., Simmons R. Point-based POMDP algorithms: improved analysis and implementation. Proceedings of the 21th conference on uncertainty in artificial intelligence (UAI-05). 2005. pp. 542–547.
14. Satia J.K., Lave R.E. Markovian decision processes with probabilistic observation of states. Management Science. 1973. vol. 20(1). pp. 1–13.
15. Barto A.G., Bradtke S.J., Singhe S.P. Learning to act using real-time dynamic programming. Artificial Intelligence. 1995. vol. 72(1). pp. 81–138.
16. Washington R. BI-POMDP: bounded, incremental partially observable Markov model planning. Proceedings of the 4th European conference on planning. 1997. pp. 440–451.
17. McAllester D., Singh S. Approximate planning for factored POMDPs using belief state simplification. Proceedings of the 15th annual conference on uncertainty in artificial intelligence (UAI-99). 1999. pp. 409–416.
18. Shani G., Brafman R., Shimony S. Adaptation for changing stochastic environments through online POMDP policy learning. Proceedings of the workshop on reinforcement learning in non-stationary environments, ECML. 2005. pp. 61–70.
19. Koenig S. Agent-centered search. AI Magazine. 2001. vol. 22 (4). pp. 109–131.
20. Approximate POMDP planning software. Available at: http://bigbird.comp.nus.edu.sg/pmwiki/farm/appl/ (accessed 18.01.2015).
21. Lusena C., Goldsmith J., Mundhenk M. Nonapproximability results for partially observable Markov decision processes. Journal of artificial intelligence research. 2001. vol. 14. pp. 83–103.

Кравчук Алексей Владимирович — адъюнкт кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: защита информации, теория принятия решений. Число научных публикаций — 10. kvazikrav@yandex.ru; ул. Ждановская, д.13, Санкт-Петербург, 197198; р.т. +7(812)237-19-60.

Kravchuk Aleksey Vladimirovich — Ph.D. student of the information acquisition and data processing department, Mozhaisky Military Space Academy. Research interests: information security, decision making theory. The number of publications — 10. kvazikrav@yandex.ru; Zdanovskaya str.13, 197198, Saint-Petersburg, Russia; office phone +7(812)237-19-60.

РЕФЕРАТ

Кравчук А.В. **Модель процесса удаленного анализа защищенности информационных систем и методы повышения его результативности.**

Статья посвящена рассмотрению нового подхода к моделированию процесса удаленного анализа защищенности информационных систем и методам повышения его результативности. В основе предлагаемого подхода лежит теория принятия решений. Непосредственное моделирование реализовано с помощью марковских процессов принятия решений в условиях частично наблюдаемой среды (МППРЧНС). Для повышения результативности удаленного анализа защищенности информационных систем предлагается обзор существующих методов решения задачи МППРЧНС, их основных характеристик и возможностей по применению к тестированию информационных систем на проникновение (ТнП).

Моделирования анализа защищенности на основе МППРЧНС является новым подходом. Его сильной стороной является наиболее адекватное использование в модели характеристик предметной области. К основному недостатку, требующему разрешения, следует отнести необходимость подбора/разработки аппроксимирующих методов, позволяющих использовать модель МППРЧНС в компьютерных сетях средних и больших размеров.

SUMMARY

Kravchuk A.V. **The Model of Process of Remote Security Analysis of Information Systems and Methods of Improving it's Performance.**

The article is devoted to approval of new approach to modeling of process of remote security analysis of information systems and methods of improving it's performance. The heart of proposed approach is the decision theory. Direct modeling is performed using partially observable Markov decision processes (POMP). Review of existing methods to solve POMDP problem is carried out in order to improve the performance of remote security analysis of information systems. Also main characteristics and capabilities of these methods for using in penetration testing domain are provided.

Modeling of security analysis on POMDP basis represents a new approach. Main advantage is what it allows for using main characteristics of penetration testing process. It's main drawback, which have to be overcome, resides in necessity to select/develop approximation technique allowing for using POMDP model in computer networks of medium or big size.

УДК 510.2; 510.6:004.8:007.3

Д.Н. Бирюков, Ю.Г. Ростовцев

ПОДХОД К ПОСТРОЕНИЮ НЕПРОТИВОРЕЧИВОЙ ТЕОРИИ СИНТЕЗА СЦЕНАРИЕВ УПРЕЖДАЮЩЕГО ПОВЕДЕНИЯ В КОНФЛИКТЕ

Бирюков Д.Н., Ростовцев Ю.Г. **Подход к построению непротиворечивой теории синтеза сценариев упреждающего поведения в конфликте.**
Аннотация. В статье предложен подход к построению непротиворечивой теории синтеза сценариев упреждающего поведения в конфликте. Приведены доказательства непротиворечивости, разрешимости и модельной полноты теории частично упорядоченных гироматов с поуровневой координацией.
Ключевые слова: гиромат, интеллектуальная система, непротиворечивость, теорема Геделя.

Biryukov D.N., Rostovtsev Y.G. **Approach to Creation of the Consistent Theory of Synthesis Scenarios of Anticipatory Behavior in the Conflict.**
Abstract. In article approach to creation of the consistent theory of synthesis of scenarios of anticipatory behavior in the conflict is offered. Proofs of consistency, resolvability and model completeness of the theory of partially ordered giromats with tiered coordination are represented.
Keywords: gyromat, intellectual system, cybersystem, consistency, Gödel's theorem.

1. Введение. Проведенные исследования, связанные с вопросами проектирования системы, призванной обеспечить информационную безопасность защищаемой критической информационной инфраструктуры (КИИ) и способной синтезировать сценарии упреждающего поведения в условиях конфликта, показали, что такая киберсистема должна быть представлена в виде самоорганизующейся интеллектуальной многоагентной системы, важная роль в которой отводится памяти и механизмам работы с нею. Кроме того, определено, что данную киберсистему можно представить в виде совокупности совместно функционирующих гироматов, которая в свою очередь также может рассматриваться как гиромат. Следовательно, возникает вопрос, связанный с организацией взаимодействия между гироматами, составляющими саму киберсистему, а точнее с обработкой знаний, представленных в ее памяти (в “информационных средах” [1] гироматов; следует напомнить, что информационную среду интеллектуальной системы составляют база фактов и база знаний [1]). С одной стороны теорию, заложенную в основу проектируемой киберсистемы, хотелось бы сделать полной, но с другой стороны, хорошо известно (см. теорему Геделя о неполноте [2–4]), что в этом случае система станет противоречивой. Ввиду этого видится необходимым более подробно рассмотреть вопрос, связанный с построением непротиворечивой и

модельно полной теории интеллектуальной системы порождения сценариев упреждающего поведения в конфликте.

2. Синтаксическая и семантическая версии теоремы Геделя о неполноте. Теорема Геделя о неполноте имеет две версии – синтаксическую (объявленную и доказанную самим Геделем [5, 6]) и семантическую (чаще всего фигурирующую в популярных рассуждениях о данной Теореме). Семантическая версия исходит из того, что некоторые выражения языка выражают осмысленные утверждения, являющиеся истинными или ложными, и состоит в том, что существует истинная, но не доказуемая формула языка. Этот эффект называется семантической неполнотой. Таким образом, семантическая версия опирается на выделение из множества всех формул подмножества истинных формул.

Синтаксическая версия не опирается на то, что какие бы то ни было выражения языка имеют какой-то смысл, она смотрит на выражения как на синтаксические конструкции, то есть как на цепочки символов, организованные по определенным правилам [4], и состоит в том, что существует закрытая формула, которую нельзя ни доказать, ни опровергнуть (опровергнуть – означает доказать отрицание). Этот эффект называется синтаксической, или дедуктивной, неполнотой. Дедуктивная неполнота может иметь место лишь при условии синтаксической непротиворечивости (она же дедуктивная непротиворечивость) языка, означающей невозможность того, чтобы какая-либо формула была доказуема вместе со своим отрицанием: в противоречивом языке любая формула является доказуемой (в силу законов логики высказываний, каковые предполагаются действующими). Эффект, противоположный синтаксической неполноте и состоящий в том, что любая закрытая формула либо доказуема сама, либо имеет доказуемое отрицание, называется синтаксической, или дедуктивной, полнотой [3].

Используя понятия «непротиворечивость», «полнота» и другие понятия, опирающиеся на понятие доказуемости, в применении к языку, очень часто допускается то, что Бурбаки называет вольностью речи (abus delanguage). Дело в том, что в логико-математическом обиходе языком принято называть чисто синтаксическую конструкцию, позволяющую из всех слов в заданном алфавите выделять правильно построенные выражения (имена, переменные, термы, формулы и т.п.) и указывать правила обращения с ними. Язык, наделенный семантикой, – это уже объект другого рода, который можно называть интерпретированным языком. Язык плюс дедуктика – это объект еще одного рода, который принято называть теорией. Только к теориям применимы понятия, связанные с доказуемостью [3]. Обычно при этом термин «тео-

рия» применяют лишь в тех случаях, когда применяемая в рассматриваемом языке система формальных доказательств такова, что вмещает в себя все законы предикатной логики (в том числе законы логики высказываний). Если же язык снабжен и семантикой, и дедуктикой, его следует, по-видимому, называть интерпретированной теорией [2].

Таким образом, следует различать четыре категории объектов: языки, интерпретированные языки, теории и интерпретированные теории. Однако, если нет опасения путаницы, всех их можно называть просто языками, имея в виду, что точное значение термина язык в каждом конкретном случае понятно из контекста. Так, когда говорят о семантической версии теоремы Геделя, термином язык обозначается интерпретированная теория, а когда говорят о синтаксической версии этим термином обозначается теория [2]. Далее, ввиду выше указанного, предлагается использовать как термин “интерпретированная теория”, так и просто “теория”, так как при манипулировании знаниями “Решатель задач” [1] не оперирует семантикой, а применяет те правила вывода новых знаний к имеющимся знаниям, которые ему доступны (естественно, что сами правила вывода должны составляться с учетом семантики).

Разумеется, обе версии теоремы о неполноте предполагают выполнение некоторых естественных ограничений, налагаемых как на рассматриваемый язык, так и на систему формальных доказательств. Среди таких ограничений центральное место занимает предположение о непротиворечивости языка (теории). Для семантической версии нужна семантическая непротиворечивость, означающая, что никакое ложное утверждение не может быть доказуемым. Для синтаксической версии нужна синтаксическая непротиворечивость, означающая невозможность того, чтобы одновременно оказались бы доказуемыми и какое-то выражение и его отрицание.

Таким образом, можно следующим образом сформулировать синтаксическую версию теоремы Геделя о неполноте [3]: при определенных условиях, накладываемых на аксиомы и правила вывода, существует такое утверждение (формулируемое в рамках той же теории, что и аксиомы), что ни оно, ни его отрицание не выводимы из указанных аксиом по указанным правилам.

Важно подчеркнуть, что [2]:

– во-первых, и аксиомы, и утверждения, о которых говорится выше в теореме, представляют собой так называемые «формулы», т.е. просто комбинации знаков, или букв, образованные согласно некоторым принятым «правилам образования»;

– во-вторых, сами понятия «утверждение» и «отрицание утверждения» определены также совершенно формально как комбинации знаков, имеющие определенное строение (без ссылки на то, что эти комбинации на самом деле что-то утверждают или отрицают);

– в-третьих, правила вывода формулируются чисто комбинаторно в виде разрешенных преобразований одних цепочек знаков в другие;

– в-четвертых, таким же «внешним», комбинаторным образом формулируются и условия, накладываемые в рассматриваемой теореме на аксиомы и правила вывода.

Следовательно, вся теория имеет чисто комбинаторный характер, нигде не происходит апелляции к смыслу рассматриваемых знаков и знакосочетаний. Такая апелляция, разумеется, должна играть решающую роль при выборе тех или иных аксиом, правил преобразования и т. п., но ее нет в окончательных формулировках.

Именно, исходя из данных позиций, далее и будет рассматриваться теорема Геделя о неполноте и порядок ее доказательства применительно к проектируемой интеллектуальной системе.

И семантическая, и синтаксическая формулировки теоремы Геделя начинаются с презумпции, что формализованный язык рассматривается вместе с произвольной, но фиксированной системой формальных доказательств (т.е. с произвольной, но фиксированной дедуктикой). И когда говорится о доказуемости, подразумевается доказуемость относительно этой дедуктики [3] над конкретным алфавитом.

Пусть:

– $Б$ – алфавит языка ($Б^{\infty}$ – множество всех слов в алфавите, в множестве $Б^{\infty}$ обычно задается подмножество T, называемое множеством «*истинных утверждений*», пару $\langle Б, T \rangle$ – называют *фундаментальной парой*).

Следуя А. А. Маркову [7], под *алфавитом* понимается конечный список элементарных (т. е. считающихся не членимыми далее) знаков, называемых *буквами* этого алфавита. Конечная цепочка следующих друг за другом букв некоторого алфавита называется *словом* в этом алфавите.

– $Д$ – алфавит доказательств, т.е. будучи записанным, доказательство D становится словом в некотором алфавите $Д$; все доказательства образуют некую совокупность в $Д^{\infty}$; предполагается наличие алгоритма, позволяющего по произвольному слову в алфавите $Д$ узнавать, принадлежит оно D или нет.

– δ – *функция выделения доказанного*, у которой область определения Δ удовлетворяет соотношению $D \subseteq \Delta \subseteq Д^{\infty}$ и которая принимает свои значения в $Б^{\infty}$; предполагается наличие алгоритма, вычисляющего эту функцию; доказательство d из D называется доказательством слова $\delta(d)$.

Тройку $\langle Д, D, \delta \rangle$ и называют [3] *дедуктикой* над алфавитом $Б$.

Регулярный способ задания дедуктики охватывает обычные приемы задания понятия доказательства посредством «аксиом» и «правил вывода».

Теперь, опираясь на понятие дедуктики можно сформулировать понятие непротиворечивости, полноты, а также перефразировать саму теорему Геделя о неполноте.

*Непротиворечивость***.** Естественно потребовать, чтобы доказуемыми были лишь «истинные утверждения», т. е. слова, принадлежащие множеству *T*. Дедуктику $\langle Д, D, \delta \rangle$ называют *непротиворечивой относительно* (или *для)* фундаментальной пары $\langle Б, T \rangle$, коль скоро $\delta(D) \subseteq T$ (т.е. непротиворечивая дедуктика “порождает” только “истинные утверждения”).

Очевидно, что если имеется язык, то представляется весьма заманчивым найти такую непротиворечивую дедуктику, в которой каждое истинное утверждение было бы доказуемым. Теорема Геделя именно и утверждает, что при определенных условиях, налагаемых на фундаментальную пару, этого сделать нельзя.

*Полнота***.** Дедуктику $\langle Д, D, \delta \rangle$ называют *полной относительно* (или *для)* фундаментальной пары $\langle Б, T \rangle$, коль скоро $\delta(D) \supseteq T$.

Формулировка рассматриваемой теоремы Геделя приобретает такой вид [3]: *при определенных условиях, налагаемых на фундаментальную пару* $\langle Б, T \rangle$ *не существует дедуктики над* $Б$, *полной и непротиворечивой относительно* $\langle Б, T \rangle$.

Прежде чем приступить к рассмотрению роли указанной теоремы в вопросе организации архитектуры интеллектуальной системы порождения сценариев упреждающего поведения в конфликте, следует дополнительно обратить внимание на то, что необходимо наличие «определенных условий» для того, чтобы теория не могла быть одновременно и полной и непротиворечивой. Таким образом, необходимо определить имеют ли место эти “определенные условия” в проекти-

руемой системе. Для того, чтобы это определить, предлагается доказать теорему Геделя о неполноте применительно к теории, реализуемой в проектируемой интеллектуальной системе. При этом следует помнить о том, что киберсистема должна быть способной обучаться на примерах из других предметных областей (биосфера, политика, военное искусство и т.п.), а следовательно, ее память ("Информационная среда" [1]) должна содержать описание процессов (спецификации) из этих областей.

3. Непротиворечивость теории частично упорядоченных гироматов в условиях поуровневой координации. Безусловно желательно, чтобы теория, положенная в основу интеллектуальной системы порождения сценариев упреждающего поведения в конфликте, была непротиворечивой и обладала полнотой (модельной полнотой). Однако, исходя из вышерассмотренных положений теоремы Геделя о неполноте, можно сделать вывод, что это далеко не всегда возможно.

Докажем, что теория, заложенная в основу интеллектуальной многоагентной системы гироматов, взаимодействующих через изменение переменных и их значений в глобальной памяти, противоречива, либо неполна.

Доказательство предлагается осуществлять, основываясь на существовании неотделимых перечислимых множеств [2,8,4,9]. Фиксировав произвольную пару неотделимых перечислимых множеств и предположив синтаксическую полноту языка (теории), для каждого из указанных неотделимых множеств попытаемся найти такое перечислимое надмножество, чтобы эти надмножества оказались взаимно дополнительны. Тогда каждое из них будет, во-первых, разрешимым, а во-вторых, будет отделять исходные неотделимые множества, что невозможно.

На начальном этапе необходимо доказать возможность существование в памяти интеллектуальной системы (гиромата) перечислимых неотделимых множеств. Для этого сформулируем и докажем соответствующую теорему.

Теорема 1. В памяти гиромата могут существовать два непересекающихся перечислимых множества имен (спецификаций программ), которые не отделяются никаким разрешимым множеством [8] (иными словами: существует пара перечислимых неотделимых множеств).

Под гироматом следует понимать совокупность абстрактных программ, связанных по управлению через глобальную память и списки формальных параметров, именующих входные и выходные переменные.

Пояснения:

Определение. В теории множеств, теории алгоритмов и математической логике *перечислимое множество* – множество конструктивных объектов (например, натуральных чисел), все элементы которого могут быть получены с помощью некоторого алгоритма [10].

Объединение и пересечение перечислимых множеств перечислимы. *Всякое конечное множество перечислимо*. Если перечислимое множество бесконечно, то его можно перечислить (то есть расположить в вычислимую последовательность) без повторений [2].

Определение. Говорят, что множество U *отделяет* множество A от множества B, если $A \subset U$ и $B \cap U = \varnothing$. В случае, если все рассматриваемые множества являются подмножеством некоторого универсума, то дополнение к U будет отделять множество B от множества A [2].

Определение. Два множества называются *отделимыми*, коль скоро существует отделяющее одно от другого разрешимое множество. Если множества не пересекаются и не являются отделимыми, они называются *неотделимыми*.

Определение. Разрешимое множество – множество конструктивных *объектов* какого-либо фиксированного типа, допускающее проверку принадлежности к нему его элементов при помощи алгоритма [11].

Доказательство Теоремы 1:

1. Все программы вычислимых функций (“спецификации процессов”/“программы на формальном языке”), представленные в виде имен в Базе Знаний гиромата, а также вычислимые функции, описывающие функционирование самого гиромата, можно эффективно перенумеровать $p_0, p_1, p_2 \ldots$, тогда $P = \langle p_0, p_1, p_2 \ldots, p_n \rangle$ – упорядоченное множество всех спецификаций.

Пояснения:

Определение. Функция f с натуральными аргументами и значениями называется *вычислимой* [8], если существует алгоритм, ее вычисляющий, то есть такой алгоритм *A*, что:

– если *f(n)* определено для некоторого натурального *n*, то алгоритм *A* останавливается на входе *n* и печатает *f(n)*;

– если *f(n)* не определено, то алгоритм *A* не останавливается на входе *n*.

2. Существует универсальная функция $\Phi(p, x)$, которая применяет конкретную p-ю программу, реализующую вычислимую

функцию f к аргументу x, тогда очевидно, что $f(x) \simeq \Phi(p, x)$.

Пояснения:

Определение. Вычислимая функция $\Phi : N \times N \to N$ называется *универсальной*, если она в некотором смысле содержит в себе все вычислимые функции от одной переменной, т.е., если, например, для всякой вычислимой функции f из N в N существует такое число n, что для всякого x имеет место условное равенство: $f(x) \simeq \Phi(n, x)$, где знак "$\simeq$" в условном равенстве обозначает, что если обе части определены, то они равны.

В качестве n достаточно взять номер программы, вычисляющей f.

Интерпретация $\Phi(n, x)$:

- бери n;

- бери n-ю программу, вычисляющую f;

- вычисляй ее, применяя ее к x, результат и есть $\Phi(n, x)$.

3. Лемма**.**

Лемма 1. Существует такая вычислимая функция, которая принимает значения *0* и *1* и не имеет всюду определенного вычислимого продолжения.

Пояснения:

Существует Теорема. Существует вычислимая функция, которая не имеет всюду определенного продолжения [8,12].

Доказательство Леммы 1:

Гиромат является программой (совокупностью программ), одной из основных способностей которой является способность изменять под влиянием входных данных, регистрируемых через систему сенсоров, себя и свою семиотическую модель мира, представленную через переменные и их значения в глобальной памяти (см. замечание к Теореме 1).

1) Обозначим через $\Phi(n, (n + in))$ функцию изменения гиромата под воздействием входных данных (in) и исходя из текущего состояния и способностей гиромата (n); под n следует понимать гиромат как программу (вычислимую функцию) в конкретный момент времени.

2) $F\left[\Phi(n, (n + in))\right] = F[z]$ – функция оценивания, обнаруживающая "Задачу" (возможную атаку); если атака (подготовка к атаке) обнаружена, то $F[z] = 1$, иначе $F[z] = 0$.

3) Пусть $\psi(n,in)=1-F\left[\Phi\left(n,(n+in)\right)\right]$ – функция, определяющая необходимость реакции киберсистемы, если $\psi(n,in)=0$, то реакция необходима, иначе ($\psi(n,in)=1$) – нет.

4) Исходя из (2) и (3) очевидно, что $1-F[z]\neq z$.

Функция $\psi(n,in)$ и является функцией, принимающей значение 0 или 1 и не имеющей всюду определенного вычислимого продолжения.

Доказательство этого строится от противного:

5) Зафиксируем входные данные, т.е. $in=\overline{in}$, где $\overline{in}$ – конкретное значение, регистрируемое через систему сенсоров киберсистемы в конкретный момент времени (на определенном этапе эволюции гиромата); после того, как in зафиксировано, его можно вовсе отбросить и перейти к функциям от одной переменной, но для сохранения наглядности того факта, что гиромат изменяет свое состояние в зависимости от его текущего состояния и поступающих данных, параметр $\overline{in}$ будет оставлен.

6) Пусть $f\left(n,\overline{in}\right)$ вычислимая всюду определенная функция, продолжающая $\psi\left(n,\overline{in}\right)$.

7) $f\left(n,\overline{in}\right)\simeq\Phi\left(p,\left(n+\overline{in}\right)\right)$ при некотором конкретном $p\in P$, конкретном $\overline{in}$ и всех n – в силу универсальности Φ.

8) Поскольку $f\left(n,\overline{in}\right)$ всюду определена, то $f\left(p,\overline{in}\right)=\Phi\left(p,\left(p+\overline{in}\right)\right)$.

9) Так как $f\left(n,\overline{in}\right)$ продолжение $\psi\left(n,\overline{in}\right)$, то $f\left(p,\overline{in}\right)=\psi\left(p,\overline{in}\right)$, $\psi\left(p,\overline{in}\right)=1-F\left[\Phi\left(p,\left(p+\overline{in}\right)\right)\right]$, а следовательно $f\left(p,\overline{in}\right)=1-F\left[\Phi\left(p,\left(p+\overline{in}\right)\right)\right]$.

10) Тогда в силу (8) и (9) можно записать: $1-F\left[\Phi\left(p,\left(p+\overline{in}\right)\right)\right]=\Phi\left(p,p+\overline{in}\right)$, что, учитывая (4), не является верным, т.е. приходим к противоречию.

△ *Лемма 1.*

4. Существуют неотделимые перечислимые множества.

Пусть:

$$A = \{n \mid \varphi(n) = 0\},$$

$$B = \{n \mid \varphi(n) = 1\},$$

где $\varphi(n)$ – функция, удовлетворяющая условиям предыдущего пункта.

A и *B* требуемая пара множеств.

Во-первых, они перечислимы (так как они полные прообразы перечислимых множеств, а именно: одно – полный прообраз нуля, а другое – полный прообраз единицы; иными словами, если функция вычислима, то множество, на котором она равна *0*, можно перечислить, и множество, на котором она равна *1*, тоже можно перечислить).

Пояснения:

Определение. Пусть *f* – частичная функция с натуральными аргументами и значениями. *Образ* множества *A* при *f* определяется как множество всех чисел *f(n)*, для которых $n \in A$ и *f(n)* определено. *Прообраз* множества *A* при *f* определяется как множество всех тех *n*, при которых *f(n)* определено и принадлежит *A* [8].

Теорема. Прообраз и образ перечислимого множества при вычислимой функции перечислимы [8].

Во-вторых, они неотделимы. Их отделимость означала бы, что существуют такие взаимно дополнительные разрешимые $\overline{A}$ и $\overline{B}$, что $A \subset \overline{A}$ и $B \subset \overline{B}$, но тогда функция равная нулю на $\overline{A}$ и единице на $\overline{B}$, была бы вычислимым всюду определимым продолжением для φ, что невозможно ввиду доказанной леммы.

▲ *Теорема 1.*

Далее пара неотделимых перечислимых множеств, существование которых доказано в теореме 1, может служить инструментом для доказательства синтаксической версии теоремы Геделя.

Теорема 2. Непротиворечивая теория гироматов, взаимодействующих через изменение переменных глобальной памяти, неполна.

Доказательство Теоремы 2:

1. Теорию предполагаем полной (т.е. для любой формулы либо она доказуема, либо ее отрицание доказуемо).

2. Пусть (A, B) – пара неотделимых перечислимых множеств (см. теорему 1).

3. Рассмотрим функцию f, принимающую значение 0 на A, значение 1 на B и не определенную на остальных исходных данных. Ее график, как легко видеть, перечислим, поэтому она вычислима.

4. Пусть $F(x,y)$ – какая-либо верифицирующая ее формула.

Пояснения:

Функция f *верифицируема*, если для нее существует верифицирующая ее формула.

Определение. Теория (теория в общем случае – это язык, где не обязательно есть понятие истины, но обязательно есть понятие доказуемости) верифицирует функцию $f:\mathrm{N}\to\mathrm{N}$ посредством формулы $F(x,y)$ с двумя параметрами, коль скоро выполнимы два условия:

1) для любых m и n если $f(m)=n$, то $\vdash F(m,n)$;

2) для любых m, n_1 и n_2 если $\vdash F(m,n_1)$ и $\vdash F(m,n_2)$, то $\vdash (n_1=n_2)$.

Основное ограничение на язык, при котором доказывается синтаксическая версия теоремы Геделя, является требование верифицируемости вычислимых функций.

Естественность указанного требования обосновывается следующими соображениями [2]. Если функция f вычислима, то алгоритмический процесс перехода от аргумента m к результату n может быть прослежен и запротоколирован, и полученный протокол можно трактовать как формальное доказательство равенства $f(m)=n$. Поскольку алгоритм един для всех аргументов, то и полученному протоколу можно придать единообразную для всех аргументов форму, с пустыми местами, заполняемыми конкретными нумералами m и n. Требование верифицируемости функции f состоит по существу в том, чтобы рассматриваемый формализованный язык был в состоянии оформить указанную форму в виде доказуемой формулы с двумя параметрами. Сказанное касалось части (1) определения представимости. Что касается части (2), то ясно, что коль скоро предъявлены два протокола одного и того же алгоритма, первый из которых ведет от аргумента m к результату n_1, а второй – от того же самого аргумента к результату n_2, само это предъявление является наглядным доказательством равенства указанных результатов.

5. Положим:

$$\overline{A}=\{n\mid\vdash F(n,0)\},$$
$$\overline{B}=\{n\mid\vdash\neg F(n,0)\}.$$

Множества $\overline{A}$ и $\overline{B}$ очевидным образом перечислимы, так как они являются полными прообразами формул A и B, которые являются перечислимыми (см. (4) в доказательстве Теоремы 1).

6. Теорию предполагаем непротиворечивой.

Далее доказательство неполноты теории проводим от противного, т.е. предположим, что она полна, и придем к противоречию с неотделимостью множеств A и B (т.е. окажется что A и B отделимы).

В силу непротиворечивости – см. (6) ($\overline{A}$ и $\overline{B}$ не могут пересекаться, в противном случае для некоторого n было бы что-то доказуемо и его отрицание тоже было бы доказуемо) и полноты – см. (1) (имеет место либо $\vdash F(n,0)$, либо $\vdash \neg F(n,0)$) они взаимно дополнительны и перечислимы, а потому разрешимы.

Пояснения:

Теорема. (Теорема Поста). Подмножество А множества «конструктивных» объектов X *разрешимо* тогда и только тогда, когда А и его дополнение X\A перечислимы.

Если мы обнаружим, что $A \subset \overline{A}$ и $B \subset \overline{B}$, то A и B окажутся отделимыми, что неверно ввиду доказанной Теоремы 1 о существовании пары перечислимых неотделимых множеств.

Утверждение $A \subset \overline{A}$ вытекает из первой части определения верифицируемости и того, что $A = \{n \mid \varphi(n) = 0\}$ (так как $A = \{n \mid \varphi(n) = 0\}$ и для любых m и n если $f(m) = n$, то $\vdash F(m,n)$ – первая часть определения верифицируемости, то $\vdash F(n,0)$).

Убедимся в справедливости утверждения $B \subset \overline{B}$.

Если $p \subset B$, то $\varphi(n) = 1$, так как $B = \{n \mid \varphi(n) = 1\}$, а следовательно $\vdash F(n,1)$ – согласно первой части определения верифицируемости.

Предположим, что для $n \subset B$ имеем $\varphi(n) = 0$, тогда $\vdash F(n,0)$, а следовательно в силу второй части определения ферифицируемости было бы $\vdash (0 = 1)$, но такое невозможно в силу $0 \neq 1$, а значит формула $F(n,0)$ в данной теории недоказуема, а тогда согласно предположению о полноте теории (1), доказуема формула $\vdash \neg F(n,0)$, что приводит к $B \subset \overline{B}$.

Пояснения:

Лемма 2. Пусть формула $F(x,y)$ верифицирует функцию f, и пусть числа m и n таковы, что f определена на m и $f(m) \neq n$, тогда если язык полон, то $\vdash \neg F(m,n)$.

Определение. Теория полна если можно доказать либо формулу (всякую), либо ее отрицание. Для языка, соответственно, можно доказать истинность утверждения, либо его ложность.

Доказательство Леммы 2:

Поскольку f определена на m, то для некоторого числа p, отличного от n, будет $f(m) = p$. В силу первой части верифицируемости $\vdash F(m,p)$. Если бы было $\vdash F(m,n)$, то в силу второй части определения ферифицируемости было бы $\vdash (n = p)$, но такое невозможно в силу $n \neq p$. Итак, формула $F(m,n)$ недоказуема, а тогда, согласно предположению о полноте, доказуема формула $\neg F(m,n)$.

△ *Лемма 2.*

Таким образом, *A* и *B* отделимы, что неверно.

Следовательно, получаем, что если теория полна, то она противоречива, так как становится доказуемыми какое-то выражение ($\vdash F(n,0)$) и его отрицание ($\neg F(n,0)$).

▲ *Теорема 2.*

Таким образом, можно сделать вывод о том, что если проектируемая интеллектуальная самоорганизующаяся многоагентная система, состоящая из гироматов, будет построена таким образом, что взаимодействие между гироматами будет осуществляться через глобальные переменные (в общем случае – доступные всем гироматам), то в этом случае теория, заложенная в основу интеллектуальной системы, при ее полноте будет противоречивой, что подтверждено в результате доказательства Теоремы 2.

Так, например, пусть к множеству *A* относятся все спецификации, которые пригодны для защиты объектов КИИ, а к множеству *B* – спецификации пригодные, например, для осуществления атакующих воздействий на противоборствующую сторону (вариант “лучшая защита – это нападение” в данном примере не рассматривается) и пусть все эти спецификации находятся в единой общедоступной памяти и представлены в виде списка $P = \langle p_0, p_1, p_2 ..., p_n \rangle$. Тогда при детектировании через систему сенсоров подготовки к атакующим воздействи-

ям со стороны киберпротивника киберсистема должна выбрать пригодную спецификацию (спецификацию, принадлежащую множеству *A*), но этого однозначно сделать невозможно, так как все спецификации есть не более чем синтаксические конструкции, и у гиромата нет их семантической интерпретации (введение строгой семантической интерпретация в конечном бы итоге привило к возможности определения пригодности применения той или иной спецификации, но так как перечень задач решаемых гироматом заранее точно определить невозможно, так же как и невозможно заранее спрогнозировать состояние гиромата, то можно с большой долей уверенности заявить, что функция оценивания может (будет) претерпевать изменения, а следовательно "пригодность", напрямую связанная с семантической интерпретацией и процедурой оценивания, становится не постоянной и зависит от состояния памяти киберсистемы, т.е. от состояния самого гиромата).

Можно привести еще один достаточно грубый, но наглядный пример невозможности работы всех гироматов из состава киберсистемы с информацией из единой памяти на общих основаниях. Пусть, например, имеется уникальный гиромат, способный сформировать спецификацию защиты КИИ от каждого появляющегося атакующего воздействия, а также есть не менее уникальный гиромат, способный построить спецификацию "взлома" любой появляющейся системы защиты. Очевидно, что если объединить указанные гироматы, то будет получена противоречивая система, порождающая как спецификацию "защиты", так и спецификацию "взлома" (что равносильно отрицанию защиты).

Однако, если разделить информацию в памяти таким образом, чтобы у одного гиромата были только спецификации, относящиеся ко множеству *A*, а у другого гиромата – только спецификации, относящиеся ко множеству *B* (т.е., если бы каждый гиромат имел возможность работать только с переменными из своей локальной памяти), то в этом случае третий гиромат (гиромат - координатор), обладая информацией о распределении информации между двумя другими гироматами, точно мог бы обратиться к нужному множеству спецификаций. Следует отметить, что при этом, каждое из множеств спецификаций было бы разрешимым и отделялось бы друг от друга, предметной областью отдельно взятого гиромата (предметные области различных гироматов не должны пересекаться в рамках представленных в них спецификаций, что в свою очередь обеспечивает непротиворечивость). Обращаясь к определенному множеству спецификаций, представленных в памяти различных гироматов, гиромат-координатор сразу "знает" о потенциальной применимости или неприменимости специфика-

ций, представленных в них (т.е. он сразу может доказать либо $\vdash F(n,0)$, либо $\vdash \neg F(n,0)$, что означает полноту теории).

Если бы гиромат имел в своей памяти только спецификации одного вида (например “защиты”) и решал вопросы связанные только с их применением, тогда бы теория такого гиромата могла быть одновременно и полной и непротиворечивой (пример несоблюдения “определенных условий” из определений теоремы Геделя о неполноте, приведенных выше).

4. Заключение. В ходе информационно-технического конфликта киберсистема, способная к упреждающему поведению и призванная обеспечить требуемый уровень информационной безопасности защищаемой КИИ, должна быть способной к порождению непротиворечивых спецификаций различного типа и к манипулированию ими. Как показали результаты приведенных выше рассуждений, для удовлетворения данного требования в основу проектируемой интеллектуальной системы должна быть положена теория частично упорядоченных гироматов с поуровневой координацией. Как видится, именно такая организация системы должна позволить решить проблему противоречивости в условиях модельной полноты теории. Однако, в этом случае возникает вопрос, связанный с координацией работы гироматов в единой системе обеспечения информационной безопасности, а также с навигацией по совокупности знаний, представленных в памяти отдельно взятого гиромата.

К достижимым свойствам полноты и непротиворечивости системы частично упорядоченных гироматов с поуровневой координацией следует добавить разрешимость, доказанную в теории решетчатых систем.

Литература

1. *Финн В.К.* Искусственный интеллект: Идейная база и основной продукт // 9-ая национальная конференция по искусственному интеллекту. Труды конференции. М.: Физматлит. 2004. Т.1. С.11–20.
2. *Успенский В.А.* Теорема Геделя о неполноте и четыре дороги, ведущие к ней // Математическое просвещение. М.: МЦНМО. 2011. Серия 3. Вып. 15. С.35–76.
3. *Успенский В.А.* Теорема Геделя о неполноте в элементарном изложении // Успехи математических наук. 1974. №29:1. С.3–47.
4. *Успенский В.А.* Теорема Геделя – синтаксическая версия // Современная математика. Дубна. 2010. URL: http://www.mccme.ru/dubna/2010/courses/vau.htm (дата обращения:17.12.2014).
5. *Göde1 K.* Über formal unentscheidbare Sätze'der Principia Mathematica und verwandter Systeme // Monatshefte für Math. und Physik. 1931. vol. 38:1. pp.173–198.
6. *Клини С.К.* Введение в метаматематику // М.: Мир. 1957. 526 с.
7. *Марков А.А.* Теория алгорифмов // Труды Математического института имени В.А. Стеклова.1951. № 38. С.176–189.

8. *Верещагин Н.К.* Лекции по математической логике и теории алгоритмов. Вычислимые функции. 4-е изд., исправленное // М.: МЦНМО. 2012. Часть 3. 160 с.
9. *Беклемишев Л.Д.* Теоремы Геделя о неполноте и границы их применимости // Успехи математических наук. 2010. № 65:5. С.61–106.
10. *Барвайс Дж*. Справочная книга по математической логике. Часть 3: теория рекурсии // М.: Наука. 1982. 392 с.
11. *Успенский В.А*. Лекции о вычислимых функциях // М.: Государственное издательство физико-математической литературы. 1960. 492 с.
12. *Поспелов А.Д.* Основы теории алгоритмов // М.: МГУ имени М.В. Ломоносова. 2002. URL:http://allsorts.fatal.ru/science/education/storage/Algorithms/algorithms.pdf (дата обращения: 24.12.2014).

References

1. Finn V.K. [Artificial intelligence: a Conceptual framework and the main product]. *9-ya nacionalnaya konferenciya po iskusstvennomu intellektu. Trudy konferencii* [Proceedings of 9th national conference on artificial intelligence]. M.: Fizmatlit. 2004. vol. 1. pp. 11–20. (In Russ).
2. Uspenskiy V.A. [Gödel's theorem of incompleteness and four roads conducting to it]. *Matematicheskoe prosvesheniye – Mathematical education.* M.: MCCME. 2011. Series 3. vol. 15. pp. 35–76. (In Russ).
3. Uspenskiy V.A. [Gödel's theorem of incompleteness in an elementary statement]. *Uspehy matematicheskih nauk – Achievements of mathematical sciences.* 1974. no. 29:1. pp. 3-47. (In Russ).
4. Uspenskiy V.A. [Gödel's theorem – the syntactic version]. *Sovremennaya matematika – Modern mathematics.* Dubna. 2010. Available at: http://www.mccme.ru/dubna/2010/courses/vau.htm (accessed 17.12.2014). (In Russ).
5. Godel K. [On Formally Undecidable Propositions of Principia Mathematica and Related Systems]. *Monatshefte für Math. und Physik – Monthly journals on mathematics and physics.* 1931. vol. 38:1. pp. 173-198. (In Germany).
6. Kliny S.K. *Vvedenie v metamatematiku* [Introduction to metamathematics]. M.: Mir. 1957. 526 p. (In Russ).
7. Markov A.A. [Theory of algorifm]. *Trudy Matematicheskogo instituta imeny V.A.Steklova – Proceedings of the Mathematical Institute of V.A.Steklov*. 1951. no. 38. pp. 176–179. (In Russ).
8. Vereshagyn N.K. *Lekcii po matematicheskoj logike i teorii algoritmov. Vychislimye funkcii. 4-e izd., ispravlennoe* [Lectures on mathematical logic and theory of algorithms. Computing functions 4 ed., fixed.]. M.: MCCME. 2012. Part 3. 160 p. (In Russ).
9. Beklemishev L.D. [Gödel's theorems of incompleteness and limits of their applicability]. *Uspehy matematicheskih nauk – Achievements of mathematical sciences.* 2010. no. 65:5. pp. 61– 106. (In Russ).
10. Barwise J. *Spravochnaja kniga po matematicheskoj logike. Chast' 3: teorija rekursii* [The reference book on mathematical logic. Part 3: Theory of a recursion]. M.: Nauka. 1982. 392 p. (In Russ).
11. Uspenskiy V.A. *Lekcii o vychislimyh funkcijah* [Lectures about computable functions]. M.: Gosudarstvennoye izdatelstvo fiziko-matematicheskoy literatury. 1960. 492 p. (In Russ).
12. Pospelov D.A. *Osnovy teorii algoritmov* [Bases of the theory of algorithms]. *M.:* MGU imeny M.V.Lomonosova. 2002. Available at: http://allsorts.fatal.ru/science/education/storage/Algorithms/algorithms.pdf (accessed 24.12.2014). (In Russ).

Бирюков Денис Николаевич — к-т техн. наук, профессор кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: системный анализ, защита информации, интеллектуальная поддержка принятия решений. Число научных публикаций — 70. Biryukov.D.N@yandex.ru; ул. Ждановская, д. 13, г. Санкт-Петербург, 197198; р.т.: (812) 237-19-60.

Biryukov Denis Nikolaevich — Ph.D., professor of systems for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: system analyses, IT-Security, intelligent decision support. The number of publications — 70. Biryukov.D.N@yandex.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: (812) 237-19-60.

Ростовцев Юрий Григорьевич — д-р техн. наук, профессор, заслуженный деятель науки и техники Российской Федерации, заслуженный работник высшей школы Российской Федерации, профессор кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: системный анализ, теоритическая и прикладная кибернетика, методология знакового моделирования, радиотехника. Число научных публикаций — 350. s_pilkevich@eureca.ru; ул. Ждановская 13, Санкт-Петербург, 197198; р.т.: +7(812) 237-19-60.

Rostovtsev Yuriy Grigorievich — Ph.D., Dr. Sci., professor, honored scientist and technology of Russian Federation, honored worker of higher school of Russian Federation, professor of systems for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: system analyses, theoretical and applied cybernetics, the methodology of symbolic modeling, radio engineering. The number of publications — 350. s_pilkevich@eureca.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812) 237-19-60.

РЕФЕРАТ

Бирюков Д.Н., Ростовцев Ю.Г. **Подход к построению непротиворечивой теории синтеза сценариев упреждающего поведения в конфликте.**

При проектировании многоагентной интеллектуальной самоорганизующейся системы, способной синтезировать сценарии упреждающего поведения в конфликте, необходимо иметь непротиворечивую теорию, разрешающую вышеназванный синтез.

В работе показано, что искомая теория возможна при использовании системы частично упорядоченных гироматов с поуровневой координацией. При этом известно, что частично упорядоченные системы составляют решетки, которые в свою очередь модельно полны и разрешимы.

Сделан вывод о том, что наделенная способностью к моделированию сценариев упреждающего поведения киберсистема, с заложенной в нее теорией частично упорядоченных гироматов с поуровневой координацией, открывает возможности к упреждению в киберборьбе.

SUMMARY

Biryukov D.N., Rostovtsev Y.G. **Approach to Creation of the Consistent Theory of Synthesis Scenarios of Anticipatory Behavior in the Conflict.**

When designing multi-agent intelligent self-organizing system that can synthesize scenarios proactive behavior in the conflict, it is necessary to have a consistent theory, the above-mentioned resolution synthesis.

In work it is shown that the required theory is possible when using system of partially ordered giromat with pourovnevy coordination. Thus it is known that partially ordered systems make lattices which it is in turn model are full and solvable.

Thus, the cybersystem allocated with ability to modeling of scenarios of anticipatory behavior, with the theory of partially ordered giromats with tiered coordination, opens opportunities to anticipation in cyberfight.

УДК 004.056

И.Е. Горбачев, А.П. Глухов

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Горбачев И.Е., Глухов А.П. **Моделирование процессов нарушения информационной безопасности критической инфраструктуры.**

Аннотация. Рассматриваются принципы оценивания эффективности действий нарушителя в критической инфраструктуре. Представлен «операционный комплекс» моделирования процессов нарушения информационной безопасности. Исследованы неопределенности процесса моделирования нарушителя и пути их устранения. Разработана математическая модель агрегированного показателя эффективности действий нарушителя, которая снимает ряд ограничений существующих вероятностных моделей случайных явлений в области информационной безопасности. Модель носит название стохастического супериндикатора и предназначена для исследования конфликтных ситуаций в критической инфраструктуре.

Ключевые слова: критическая инфраструктура, информационная безопасность, операционный комплекс, модель нарушителя, процессы нарушения безопасности, показатель эффективности, стохастический супериндикатор.

Gorbachev I.E., Glukhov A.P. **Modeling of Processes of Information Security Violations of Critical Infrastructure.**

Abstract. Discusses the principles of evaluation the effectiveness of the malefactor in the critical infrastructure. The "operating complex" process modeling of security breach is presented. Investigated uncertainty modeling process of malefactor and ways to overcome them. A mathematical model of aggregate effectiveness of the malefactor, which removes some limitations of existing probabilistic models of random phenomena in the field of information security is developed. The model is called stochastic super indicator and is intended for research of conflict situations in critical infrastructure.

Keywords: critical infrastructure, information security, operating complex, model the malefactor, processes of a security breach, performance indicators, stochastic superindikator.

1. Введение. Информатизация критически важных объектов (КВО) на основе IP-технологии сделала обеспечение безопасности критической информационной инфраструктуры (КИИ) Российской Федерации (РФ) одной из наиболее острых проблем современности. Процесс информатизации обуславливает появление новых видов угроз информационной безопасности (ИБ), направленных, прежде всего, на системы управления и жизнеобеспечения КВО, которые наиболее подвергнуты деструктивным информационным воздействиям (ИВ). Повышенный уровень террористической угрозы в сочетании со стремительно возрастающим уровнем зависимости общества от промышленных систем требуют принятия скоординированных мер, направленных на снижение риска дезорганизации или полного прекращения функционирования КВО в условиях информационного конфликта. Одним из возможных направлений разрешения этой проблемы является проведение аудита ИБ КИИ КВО, основным

этапом которого является идентификация существующих угроз ИБ.

Актуальный перечень угроз ИБ должен определяться результатами моделирования возможных действий нарушителя ИБ КИИ. Согласно приказу ФСТЭК России от 14 марта 2014 г. N 31 [1], меры защиты информации, выбранные и реализованные в автоматизированных системах управления (АСУ) технологическим процессом (ТП) КВО, для АСУ 1, 2, 3 классов защищенности должны обеспечивать нейтрализацию угроз безопасности информации (УБИ) от нарушителя с высоким, не ниже среднего и низким потенциалами, соответственно.

В настоящее время не достаточна формализована методология оценивания уровня потенциала нарушителя и эффективности его ИВ. Фактически уровень определяется экспертно по известным только им критериям.

В статье рассмотрены следующие вопросы. Во втором разделе приведен краткий анализ нормативно-правовой базы РФ в данной предметной области. В третьем разделе рассматриваются особенности обеспечения ИБ КВО с учетом специфики АСУ ТП. Четвертый раздел посвящен разработке операционного комплекса моделирования процессов нарушения ИБ. В пятом разделе проведен анализ неопределенностей процесса моделировании нарушителя и оценивании эффективности его ИВ. В шестом разделе представлены рекомендации по моделированию нарушителя ИБ. В седьмом разделе раскрываются семантические аспекты исследования процессов нарушения ИБ и обосновывается показатель эффективности противодействия конфликтующих процессов – стохастический супериндикатор.

2. Анализ нормативно-правовой базы РФ, регламентирующей подходы к оцениванию уровня нарушителя ИБ. Подходы к оцениванию уровня опасности действий нарушителя ИБ в традиционных автоматизированных системах (АС) представлены на рисунке 1.

Классификация нарушителей ИБ (рисунок 1, первый подход) в настоящее время уже устарела, так как разрабатывалась без учета распределенной (сетевой) архитектуры современных АС. Второй подход (рисунок 1) позволяет классифицировать нарушителей ИБ не только по уровню полномочий доступа к защищаемой информации, но и учитывать сам факт наличия физического доступа в контролируемую зону предприятия. Однако данный подход оценивает нарушителя только по двум аспектам (в действительности их больше) и не позволяет с позиции квалиметрии измерить уровень потенциала нарушителя, а также оценить результативность его воздействий.

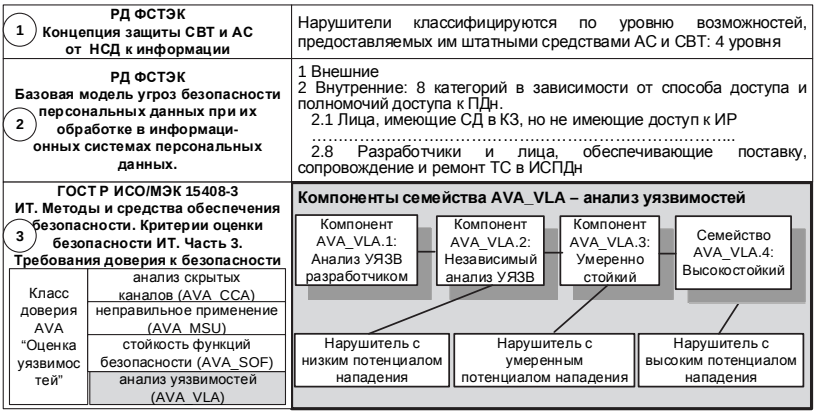


Рис. 1. Подходы к оцениванию уровня опасности действий нарушителя ИБ

В рамках подхода 3 (рисунок 1) предложено не ограничиваться рассмотрением способов взаимодействия нарушителя с объектом атаки и не делать никаких предположений относительно корректности реализации функций безопасности, а рассматривать ИВ исключительно в контексте результатов анализа уязвимостей АС. Основная цель этого анализа, проводимого в ходе аудита, – сделать заключение, что объект оценивания является стойким к нападению противника, обладающего низким, умеренным или высоким потенциалами нападения. Потенциал нарушителя должен определяться в ходе оценивания его возможностей, проводимого при определении актуальных угроз ИБ. Эти угрозы ИБ должны определяться по результатам моделирования возможных действий нарушителя, что требует произвести разработку методологических основ оценивания уровня потенциала нарушителя с учетом специфики АСУ ТП.

3. Особенности обеспечения ИБ КВО с учетом специфики АСУ ТП. В настоящее время становление направления, связанного с исследованием безопасности КВО, сдерживается отсутствием единых представлений о существе понятия ИБ АСУ ТП. Данные технологические системы имеют более высокие уровни риска по сравнению с традиционными АС, вплоть до нарушения работоспособности системы, выброса вредных веществ, техногенных катастроф и человеческих жертв. Поэтому помимо обеспечения конфиденциальности, целостности и доступности информации в первую очередь ставится вопрос о безопасности самого технологического процесса (ТП) в КВО.

На свойство безопасность ТП (рисунок 2) влияют элементарные свойства ТП и системы управления им – наблюдаемость, управляемость, идентифицируемость.

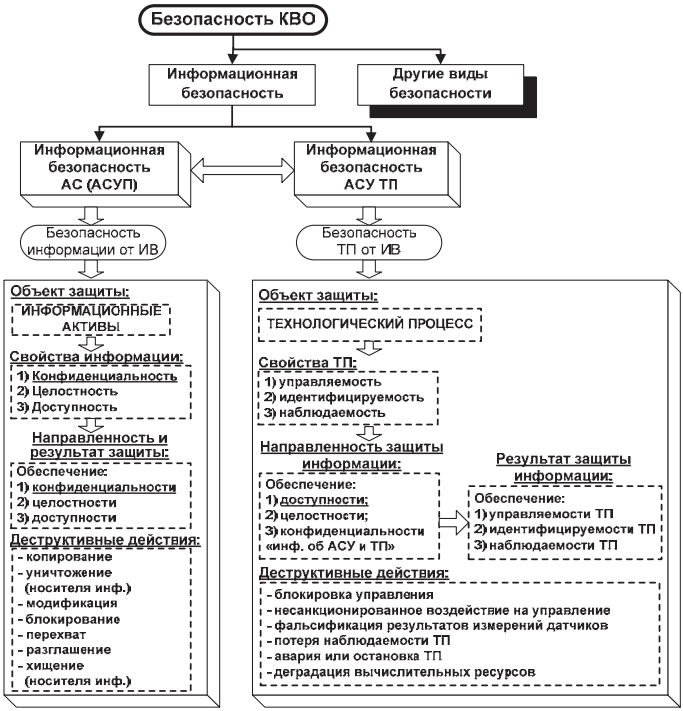


Рис. 2. Декомпозиция свойства безопасности АСУ ТП КВО

Поэтому целью защиты ТП является обеспечение требований управляемости, наблюдаемости и идентифицируемости ТП. При невыполнении этих требований возможны деструктивные действия на АСУ ТП, связанные с потерями:

- управляемости технологического процесса, включающей блокировку управления и/или несанкционированное управление;
- наблюдаемости технологического процесса: модификация параметров ТП и/или фальсификация измерений датчиков;
- работоспособности системы: авария (остановка) ТП и/или деградация вычислительных ресурсов.

Все деструктивные воздействия на АСУ ТП являются производными трех причин: нарушение доступности (отказ в обслуживании) критически важной информации, нарушение ее целостности (модифи-

кация) и конфиденциальности (утечки).

Критически важной информацией является закрепленная в документации на АСУ ТП «технологическую» информацию, уничтожение, блокирование или искажение которой может привести к нарушению функционирования АСУ ТП, а также информацию «об АСУ ТП и ТП», которая в случае ее хищения может быть использована для деструктивных информационных воздействий на АСУ ТП. «Технологической» информацией является:

- оперативная (динамическая) информация (телеметрия, телеизмерения, телеуправление) о протекании управляемого ТП;
- архивная (статическая) информация (нормативно-техническая документация, параметры ТП и другая архивная информация).

Под информацией «об АСУ ТП и технологическом процессе» понимается информация о составе, характеристиках управляемого процесса, характеристиках программного и программно-аппаратного обеспечения, размещении, коммуникациях.

Поэтому для АСУ ТП основным направлением защиты является обеспечение доступности и целостности технологической информации, а обеспечение ее конфиденциальности не актуально. Однако возникает смежная угроза нарушения конфиденциальности информации «об АСУ ТП и технологическом процессе».

4. Операционный комплекс моделирования процессов нарушения информационной безопасности. Руководствуясь основными принципами и методами квалиметрии, предлагается потенциал нарушителя охарактеризовать вектором $Y^{\Pi}_{\langle 3\rangle} = Y^{\Pi}_{\langle 3\rangle}(A'_{\langle k'\rangle}; A''_{\langle k''\rangle}, B'_{\langle l'\rangle})$, $k = k' + k''$, $A_{\langle k\rangle} =< A'_{\langle k'\rangle} + A''_{\langle k''\rangle} >$ [2, 3, 4].

С позиции теории эффективности целенаправленных процессов [5] вектор $Y^{\Pi}_{\langle 3\rangle}$ есть показатель *виртуального* качества результатов ИВ. Он включает в себя три группы компонент: $Y^{\Pi}_{\langle 3\rangle} =< v, r, \tau >$, характеризующих виртуальные (возможные) целевые эффекты, где v – показатель целевых эффектов (результативность ИВ), r – показатель расходов ресурсов (ресурсоемкость ИВ), τ – затраты операционного времени (оперативность ИВ). Каждая из компонент вектора $Y^{\Pi}_{\langle 3\rangle}$ зависит от векторов $A'_{\langle k'\rangle}, A''_{\langle k''\rangle}, B'_{\langle l'\rangle}$, где $A'_{\langle k'\rangle}$ – эксплуатационно-технические характеристики (ЭТХ) и параметры системы ИВ (СиИВ) нарушителя; $A''_{\langle k''\rangle}$ – ЭТХ и параметры процесса организации ИВ (ПрИВ) или технологии ИВ; $B'_{\langle l'\rangle}$ – характеристики условий функционирования (УФС) СиИВ.

Под СиИВ будем понимать совокупность программно-аппаратных средств ИВ. Под УФС СиИВ будем понимать совокупность факторов, оказывающих влияние на параметры и ЭТХ СиИВ (вектор $A'_{\langle k' \rangle}$), а также на характеристики ПрИВ (вектор $A''_{\langle k'' \rangle}$) и через них обусловливающие возможные (виртуальные) $Y^{\Pi}_{\langle 3 \rangle}$ результаты ИВ.

Применение нарушителем средств ИВ происходит в условиях активного противодействия системы защиты атакуемой АСУ ТП. Поэтому под условиями применения $B''_{\langle l'' \rangle}$ нарушителем СиИВ будем понимать совокупность механизмов защиты атакуемой АСУ ТП. Эти защитные механизмы влияют на ситуацию, в которой СиИВ придётся выполнять задачу, и тем самым обуславливают требуемые $Y^{\partial}_{\langle 3 \rangle}(B''_{\langle l'' \rangle})$ для нарушителя результаты ИВ т.е. $Y^{\Pi}_{\langle 3 \rangle} \in \{Y^{\partial}_{\langle 3 \rangle}\}$, где $Y^{\partial}_{\langle 3 \rangle} =< v^{T}, r^{\Pi}, \tau^{Д} >$, где v^{T} – требуемый (минимально допустимый) целевой эффект v, r^{Π} – предельные (максимально допустимые) затраты ресурсов r, $\tau^{Д}$ – директивное (максимально допустимое) время τ.

Соотношение $Y^{\Pi}_{\langle 3 \rangle} \in \{Y^{\partial}_{\langle 3 \rangle}\}$ представляет собой формальное выражение цели ИВ нарушителя. Содержательно цель ИВ определяется нарушением функционирования технологических процессов, специфика защиты которых были представлены в разделе 3.

Показатель эффективности ИВ будем описывать вектором $Y^{ИВ}_{\langle 3 \rangle} = Y^{ИВ}_{\langle 3 \rangle}(A'_{\langle k' \rangle}, A''_{\langle k'' \rangle}, B'_{\langle l' \rangle}, B''_{\langle l'' \rangle})$, где $A'_{\langle k' \rangle} = A'_{\langle k' \rangle}(B'_{\langle l' \rangle}, B''_{\langle l'' \rangle})$, $A''_{\langle k'' \rangle} = A''_{\langle k'' \rangle}(B'_{\langle l' \rangle}, B''_{\langle l'' \rangle})$, $B_{\langle l \rangle} =< B'_{\langle l' \rangle} + B''_{\langle l'' \rangle} >$, $l = l' + l''$.

Структурная схема операционного комплекса (ОпК) моделирования процессов нарушения ИБ изображена на рисунке 3.

Раскроем содержание основных элементов ОпК ИВ нарушителя в АСУ ТП:

- РУК – руководство нарушителя;
- ОУП – орган управления процессом ИВ;
- СиИВ – система ИВ – силы и средства ИВ;
- ПрИВ – процесс ИВ – технология (процесс организации) ИВ;
- УФС – условия функционирования СиИВ;
- УПС – условия применения нарушителем СиИВ;
- v – показатель целевых эффектов (результативность ИВ);
- r – показатель расходов ресурсов (ресурсоемкость ИВ);
- τ – затраты времени на ИВ (оперативность ИВ).

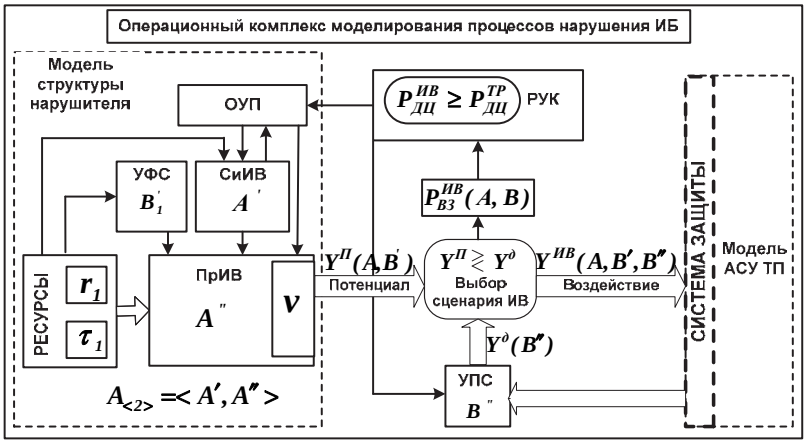


Рис. 3. Структурная схема операционного комплекса моделирования процессов нарушения ИБ

Следует понимать, что нарушитель (и реализуемые им ИВ) в инфотелекоммуникационном пространстве для защищаемой стороны представлен в виде опасных процессов – процессов нарушения ИБ. Эти деструктивные процессы совместно с процессами защиты (противодействия) образуют так называемые конфликтующие процессы, а исследование эффективности их противодействия друг другу – актуальная задача.

По сути, потенциал $Y^{\Pi}_{\langle 3\rangle}$ характеризует внутреннюю структуру нарушителя и может быть аналитически представлен иначе: в виде пары $< Str, Par >$, где Str – структура нарушителя, Par – значения его параметров $A'_{\langle k'\rangle}$, $A''_{\langle k''\rangle}$, $B'_{\langle l'\rangle}$. Знание структуры Str и параметров Par позволяет классифицировать противника по различным критериям. Поэтому характеристики нарушителя будем описывать вектором $< Str, Par, Klas >$, где $Klas$ – критерий классификации нарушителя. Применяя разное сочетание параметров $A'_{\langle k'\rangle}$, $A''_{\langle k''\rangle}$, $B'_{\langle l'\rangle}$ можно классифицировать нарушителя по множеству аспектов. Например, по параметру $A''_{\langle k''\rangle}$ – тип реализуемого нарушителем ИВ, по параметру $B'_{\langle l'\rangle}$ – вид удаленного подключения к АСУ ТП. Поэтому в ходе аудита ИБ необходимо, прежде всего, определить класс нарушителя, а затем уже оценить его потенциал. Приведем физический смысл переменных $A'_{\langle k'\rangle}$, $A''_{\langle k''\rangle}$, $B'_{\langle l'\rangle}$, $B''_{\langle l''\rangle}$.

$A'_{\langle k' \rangle}$ – параметры и ЭТХ СиИВ нарушителя:

- состав и структура СиИВ;
- уровень технической компетентности нарушителя;
- характеристики средств удаленной идентификации (например, реализуемые способы сканирования удаленных хостов, настройки временных параметров сканирования; идентификации состояния TCP и UDP портов и др);
- характеристики средств ИВ (например, реализуемые классы удаленных сетевых атак и способы их реализации; возможность реализации воздействия на различных уровнях модели ISO/OSI; направленность информационного воздействия: нарушение конфиденциальности, целостности или доступности информации и др).
- характеристики системы принятия решения и др.

$A''_{\langle k'' \rangle}$ – ЭТХ и параметры ПрИВ:

- математическое описание цели ИВ;
- момент времени начала и период проведения ИВ;
- тип реализуемого ИВ;
- условие начала реализации ИВ (реализуемые по запросу от объекта атаки (ОА) или по наступлению ожидаемого события на ОА; безусловные воздействия);
- наличие обратной связи с ОА: с обратной связью; без обратной связи (однонаправленное ИВ);
- уровень эталонной модели OSI, на котором реализуется ИВ;
- сценарий проведения ИВ;
- характеристики скрытности проведения ИВ и др.

Характеристики $B'_{\langle l' \rangle}$ условий функционирования СиИВ:

- наличие точки доступа к АСУ ТП;
- вид удаленного подключения через сеть Интернет (например, коммутируемое соединение на основе PSTN; соединение с использованием ISDN; локальное соединение по технологии xDSL; использование симметричных систем спутниковой связи; использование асимметричных систем спутниковой связи; использование сотовых сетей передачи данных и др);
- уровень знаний об ОА: число и характеристики хостов; порты и сервисы, функционирующие на хостах; типы и версии операционных систем; программное обеспечение (ПО); аппаратное обеспечение; топология сети и др;
- наличие уязвимостей: уязвимости системного ПО (в том числе протоколов сетевого взаимодействия); уязвимости прикладного ПО (в том числе средств защиты информации) и др.

5. Анализ неопределенностей процесса моделировании нарушителя и оценивании эффективности его ИВ. Процесс моделирования нарушителя включает неопределенности:

Тип 1. Математической структуры нарушителя – неопределенность потенциала нарушителя – $\hat{Y}^{\,П}(\hat{A},\hat{B}')$.

Тип 2. Критерия выбора нарушителем сценария ИВ – $\hat{Y}^{\,П} \gtrless \hat{Y}^{\,д}$.

Тип 3. Показателя качества результатов ИВ – $\hat{Y}^{ИВ}_{\langle 3\rangle} = \hat{Y}^{ИВ}_{\langle 3\rangle}(\hat{A}_{\langle k\rangle},\hat{B}_{\langle l\rangle})$.

В виду того, что как нарушителю, так и системе защите от него приходится действовать в условиях неопределенности, значения параметров векторов $\hat{A}_{\langle k\rangle}$ и $\hat{B}_{\langle l\rangle}$ оказываются случайными ($\wedge$ – символ случайной величины), а, следовательно, и вектора $\hat{Y}^{\,П}$ и $\hat{Y}^{\,ИВ}$ также будут случайными. Более того, априори случайными являются и допустимые значения $\hat{Y}^{\,д}_{\langle 3\rangle}$ вектора $\hat{Y}^{\,П}$, зависящие от системы защиты $\hat{B}''_{\langle l''\rangle}$ атакуемой АС, поскольку до проведения нарушителем ИВ сам нарушитель и поставленная им цель операции неизвестны.

Разрешение неопределенностей первого и второго типов позволяет построить модель нарушителя, а снятие неопределенностей второго и третьего типов – модель процессов нарушения информационной безопасности КИИ. На рисунке 4 приведена схематическая диаграмма, иллюстрирующая отношения перечисленных выше неопределенностей.

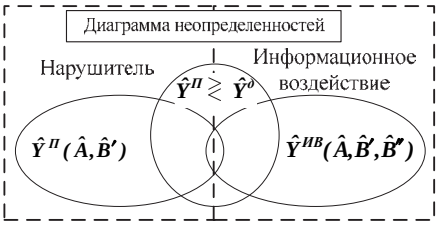


Рис. 4. Схематическая диаграмма, иллюстрирующая отношения неопределенностей процесса моделирования нарушителя и его воздействий

Рассмотрим более подробно неопределенности, с которыми приходится сталкиваться исследователю при моделировании действий нарушителя.

Во-первых, введение неопределенности в математическую структуру нарушителя, описываемую вектором $\hat{Y}^{\,П}_{\langle 3\rangle}$, позволяет отра-

зить при моделировании реальные условия неполноты сведений о нарушителе. Крайним случаем неопределенности является неструктурируемость, то есть невозможность построения соответствующей модели нарушителя, принадлежащей к тому или иному типу математической структуры. Для снятия этой "структурной" неопределенности можно предложить технологию маскирования информационных ресурсов АСУ ТП, представленной в [6]. Данная технология позволяет:

- обнаруживать скрытые каналы ИВ нарушителя на информационные ресурсы;

- формировать рефлексивное управление нарушителем с помощью обманной информационно-вычислительной среды, параметры которой описываются вектором $\hat{B}'^{*}_{\langle l' \rangle}$.

Целью маскирования является идентификация (построение модели) нарушителя, то есть определение значений параметров $\hat{A}'_{\langle k' \rangle}$, $\hat{A}''_{\langle k'' \rangle}$ и формирование вектора $\hat{Y}^{\Pi}_{\langle 3 \rangle}$. Это достигается созданием у нарушителя ложного представления об ОА путем подмены $\hat{B}'_{\langle l' \rangle}$ на $\hat{B}'^{*}_{\langle l' \rangle}$. Как следствие, реализуется возможность всестороннего исследования структуры; оценивания потенциала $\hat{Y}^{\Pi}_{\langle 3 \rangle}$; определения перечня своих защитных мер $\hat{B}''_{\langle l'' \rangle}$.

Во-вторых, существует неопределенность в задании базисных множеств и отношений, на основе которых строится модель нарушителя. Для задания количественной меры такой неопределенности можно использовать стохастический подход (стохастические структуры), базирующийся на фундаментальных положениях теории вероятностей и математической статистики, или подход с позиции теории нечетких множеств (нечеткие структуры).

Идея заключается в исследовании неопределенности выбора нарушителем того или иного сценария реализации ИВ. При данном подходе не ставится задача определения потенциала $\hat{Y}^{\Pi}_{\langle 3 \rangle}$, так как неизвестны значения параметров $\hat{A}'_{\langle k' \rangle}$, $\hat{A}''_{\langle k'' \rangle}$. Предлагается оценивать нарушителя в типах $U = \{U_i\}_{i=1}^{N}$ соответствующих возможных угроз ИВ и в "механизме выбора" $\zeta(\eta_j^i)$ сценария реализации конкретной угрозы $\eta_j^i \in U_i$. То есть в качестве модели нарушителя рассматривается его профиль $< U, \zeta >$. Перед выбором $\zeta(\eta_j^i)$ сценария нарушитель сталкивается:

- в процессе изучения специфики АСУ ТП и идентификации векторов $\hat{B}'_{\langle l' \rangle}$ и $\hat{B}''_{\langle l'' \rangle}$;

- при сравнении $\hat{Y}^{\Pi} \underset{<}{\geq} \hat{Y}^{\partial}$ и определении допустимых значений $Y^{\partial}_{\langle 3\rangle}(B''_{\langle l''\rangle})$ вектора $Y^{\Pi}_{\langle 3\rangle}$ своих потенциальных возможностей.

Представляется очевидным, что говорить о стохастической природе ИВ нерационально, так как нарушитель не осуществляет свой выбор случайным образом. Его выбор целенаправлен и обусловлен определенным критерием выбора.

Тогда можно говорить, что "механизм выбора" $\zeta(\eta^i_j)$ характеризуется наличием тех или иных неизвестных (случайных) факторов. В этом случае необходимо ввести допущение – аудитору ИБ известно множество U типовых угроз ИБ и сценариев их реализации. Это допущение вполне обосновано, так как перечень именно типовых угроз ИБ действительно известен.

Будем различать три типа возможных ситуаций.

К *первому типу* отнесем ситуацию, когда множество угроз U и критерий выбора ζ известны. В данной ситуации профиль нарушителя известен, остается только оперативно организовать соответствующую защиту.

Второй тип включает ситуацию, при которой множество угроз U известны, а критерий выбора ζ неизвестен. В данном случае процесс управления защитой похож на процесс игры. Решением такого рода задач занимается специальный раздел математики, носящий название «Теория игр». Под теорией игр часто понимают теорию математических моделей принятия оптимальных решений в условиях неопределенности и конфликта. Однако теория игр, как математический аппарат, страдает концептуальной неполнотой. Так, в реальном конфликте перечень возможных угроз U и сценариев их реализации как раз неизвестен, и наилучшим решением для нарушителя в конфликтной ситуации нередко будет именно выйти за пределы известных сценариев ИВ.

В *третий тип* входят ситуации, когда множество угроз U, а точнее сценариев их реализации, неизвестно. В данной ситуации система защиты должна уметь оперативно пресекать неизвестные ИВ путем своевременной настройки механизмов защиты и/или контрвоздействий. Для этого система защиты должна быть наделена принципиально новым свойством, позволяющим ей оперативно предвидеть реализацию неизвестных угроз U и своевременно готовиться к ним. Такое свойство называется "*Антиципация*", которое более подробно раскрывается в [7].

В-третьих, уровень неопределенности (случайности) показателя качества результатов ИВ $\hat{Y}^{ИВ}_{\langle 3\rangle} = \hat{Y}^{ИВ}_{\langle 3\rangle}(\hat{A}_{\langle k\rangle}, \hat{B}_{\langle l\rangle})$, использующего профиль $< U, \zeta >$, характеризуется вероятностью $P^{ИВ}_{ДЦ}$ достижения цели операции и является показателем эффективности ИВ. Действительно, векторы $\hat{A}_{\langle k\rangle}$, $\hat{B}'_{\langle l'\rangle}$, а, следовательно, и $\hat{Y}^{П}_{\langle 3\rangle}$ оказываются случайными. Более того, априори случайными являются и допустимые значения $\hat{Y}^{\partial}_{\langle 3\rangle}$ вектора $\hat{Y}^{П}_{\langle 3\rangle}$, поскольку до проведения нарушителем ИВ нам неизвестно какими должны быть результаты этого воздействия, чтобы поставленная нарушителем цель была достигнута, т.е.

$$\begin{cases} \hat{Y}^{П}_{\langle 3\rangle} = Y^{П}_{\langle 3\rangle}\left(\hat{A}_{\langle k\rangle}, \hat{B}'_{\langle l'\rangle}\right), \\ \hat{Y}^{\partial}_{\langle 3\rangle} = Y^{\partial}_{\langle 3\rangle}\left(\hat{B}''_{\langle l''\rangle}\right). \end{cases}$$

Так как в реальных условиях критерий пригодности ИВ принимает вид $G_{Ц} : \hat{Y}^{П}_{\langle 3\rangle} \in \{\hat{Y}^{\partial}_{\langle 3\rangle}\}$, то $P^{ИВ}_{ДЦ} = P(\hat{Y}^{П}_{\langle 3\rangle} \in \{\hat{Y}^{\partial}_{\langle 3\rangle}\})$. Как видно, факт пригодности результатов операции есть случайное событие. Поэтому мера достижения нарушителем цели операции является вероятностной характеристикой. Для вычисления $P^{ИВ}_{ДЦ}$ достаточно (но не необходимо) определить благоприятные для нарушителя с профилем $< U, \zeta >$ условия реализации угроз U. Под условиями реализации ИВ понимается наличие у нарушителя информации:

- о структуре и характеристиках ИТКС;
- о наличие уязвимостей программно-аппаратного обеспечения и системы защиты.

6. Рекомендации по моделированию нарушителя ИБ. Представленные выше способы оценивания потенциала нарушителя и эффективности его воздействия носят концептуальный характер и требуют дальнейших исследований. Направление дальнейших исследований – разработка методов снятия структурной неопределенности нарушителя. Однако реализация данных подходов в рамках аудита ИБ не всегда возможна, так как требует привлечения дополнительных технических средств и времени. Поэтому в ходе проведения аудита широко используются экспертные оценки нарушителя в типах U возможных угроз ИБ, которые он способен выполнить. Соответственно, модель нарушителя должна определять предпочтения нарушителя по выбору им потенциально возможных атакующих действий – элементарных

событий нарушения ИБ, из которых формируются различные сценарии реализации угрозы ИВ. То есть перед аудитором стоит задача в обоснованном уменьшении мощности множества U. При формулировке данной задачи могут быть приняты следующие допущения о наличии данных [8]:

- уровне знаний и компетентности нарушителя;
- начальном расположении нарушителя в ИТКС, определяющем список доступных ему хостов на основе некоторой формальной модели M ИТКС;
- начальных правах нарушителя, ограничивающих множество ИВ, на основе требуемых условий для реализации ИВ.

Будем различать априорную N^A и апостериорную N^P модели нарушителя. К первому типу отнесем модель, перечень параметров и их значения которой определены без привязки к структуре исследуемой АС. Структуру ее определяют гипотезы, выдвигаемые аудиторами на основании имеющихся априорных данных и своей компетенции. В результате априорная модель нарушителя, учитывающая его предпочтения по выбору потенциально возможных атакующих действий, выглядит следующим образом:

$$N^A = < Z, H, K, G > ,$$

где Z – начальные знания нарушителя о каждом атакуемом хосте и права доступа, которыми этот нарушитель обладает; H – хосты, к которым нарушитель имеет физический или удаленный доступы до начала проведения атак; K – уровень компетентности нарушителя, т.е. классы или списки доступных ему атакующих действий, как основанных на уязвимостях, обладающих разной критичностью, так и на различных методах сбора информации; G – основные цели нарушителя, например, нарушение управляемости, наблюдаемости или идентифицируемости ТП.

Для моделирования действий нарушителя, адекватного отображения его структуры, необходимо будет разработать типовую онтологическую модель для представления знаний о нарушителях. Далее, например, в ходе проведения аудита, “насыщать” ее экспертными данными (гипотезами) о нарушителе с привязкой к конкретной АСУ ТП, тем самым формируя базу знаний BZ^N о нарушителе.

Разработка апостериорной модели нарушителя N^P заключается в нахождении соответствия q между упорядоченным множеством N^A и множеством $V^{ПАО}$ или $q = (N^A, V^{ПАО}, Q)$, где $V^{ПАО}$ – множество уязвимостей программно-аппаратного обеспечения АС. Множество

$Q \subseteq N^A \times V^{ПАО}$ определяет способ, с помощью которого осуществляется соответствие между элементами множеств N^A и $V^{ПАО}$, и, как следствие, нахождение множества уязвимостей $V^N \subseteq V^{ПАО}$, которыми может воспользоваться нарушитель N^A. Множество V^N называется областью значений соответствия q. В результате апостериорная модель нарушителя N^P принимает вид: $N^A =< Z, H, K, G, V^N >$.

Другим решением нахождения множества V^N является изменение структуры онтологической модели нарушителя с учетом сведений, полученных из базы знаний уязвимостей BZ^V.

Для количественного оценивания значения показателя потенциала нарушителя предлагается воспользоваться идеей, описанной в [9], с учетом разработанного выше ОпК (см. рис. 3). Уровень потенциала нарушителя рассматривается исключительно в контексте результатов проведенного им анализа уязвимостей и делается предположение о том, что могут ли уязвимости, идентифицированные в процессе аудита, быть использованы нарушителем с разным уровнем потенциала. При анализе потенциала ИВ, потребного нарушителю для реализации уязвимости, необходимо экспертным путем оценить значения параметров идентификации и реализации уязвимости:

- уровень технической компетентности нарушителя $(A'_{\langle k' \rangle})$;
- качество средств удаленной идентификации и ИВ $(A'_{\langle k' \rangle})$;
- затраты времени на идентификацию и реализацию уязвимости $(A''_{\langle k'' \rangle})$;
- затраты времени на непосредственный доступ к ОА при идентификации и реализации уязвимости $(A''_{\langle k'' \rangle})$;
- объем знаний об ОА $(B'_{\langle l' \rangle})$.

7. Семантические аспекты исследования процессов нарушения ИБ с позиции теории стохастической индикации. Как отмечалось выше, неопределенность показателя качества результатов ИВ $\hat{Y}^{ИВ}$ характеризуется вероятностью достижения цели операции $P_{ДЦ}^{ИВ}$, что и является показателем эффективности ИВ. Для проведения собственно оценивания эффективности $P_{ДЦ}^{ИВ}$ ИВ нарушителя требуется определить требуемое значение $P_{ДЦ}^{ТР}$ показателя эффективности ИВ $P_{ДЦ}^{ИВ}$, сформулировать и реализовать критерий пригодности $G_{ЦЭ} : P_{ДЦ}^{ИВ} \geq P_{ДЦ}^{ТР}$.

Для количественного анализа приведенной выше ситуации построим ее математическую модель. Для этого применим методы теории стохастической индикации [3, 4].

Рассмотрим дважды неопределенное высказывание в виде предиката $\hat{y} > \hat{z}$, где $\hat{z}$ и $\hat{y}$ взаимно независимые случайные переменные. Определим вероятность случайного события $\hat{A} \simeq (\hat{y} > \hat{z})$:

$$P(\hat{z} < \hat{y}) = \int_{-\infty}^{\infty} F_{\hat{z}}(y)\, dF_{\hat{y}}(y); \tag{1}$$

$$P(\hat{y} > \hat{z}) = \int_{-\infty}^{\infty} R_{\hat{y}}(z)\, dF_{\hat{z}}(z), \tag{2}$$

где $\left.\begin{array}{l} F_{\hat{x}}(x) \overset{d}{=} P(\hat{x} < x) \\ R_{\hat{x}}(x) \overset{d}{=} P(\hat{x} \geq x) \end{array}\right\}$ – функция распределения $\hat{x}$.

Введем следующие обозначения:

$$\hat{\omega}_1 = \omega_1(\hat{y}) = F_{\hat{z}}(\hat{y}); \tag{3}$$

$$\hat{\omega}_2 = \omega_2(\hat{z}) = R_{\hat{y}}(\hat{z}). \tag{4}$$

Тогда, как видно из (1) и (2), $\left.\begin{array}{l} P(\hat{z} < \hat{y}) = M[\hat{\omega}_1] = \overline{\omega}_1 \\ P(\hat{y} \geq \hat{z}) = M[\hat{\omega}_2] = \overline{\omega}_2 \end{array}\right\} \Rightarrow \overline{\omega}_1 = \overline{\omega}_2$ (5).

Случайные величины $\hat{\omega}_1$ и $\hat{\omega}_2$ называются *стохастическими супериндикаторами* [3-5]. Поскольку каждому двухместному дважды неопределенному предикату соответствуют два супериндикатора, то для отличия их друг от друга они снабжены индексами (номерами).

Из соотношения (5) следует, что:

$$P(\hat{z} < \hat{y}) = \overline{\omega}_1 = \int_0^1 \omega\, dF_{\hat{\omega}_1}(\omega) = P(\hat{y} \geq \hat{z}) = \overline{\omega}_2 = \int_0^1 \omega\, dF_{\hat{\omega}_2}(\omega),$$

где $F_{\hat{\omega}_1}(\omega)$, $F_{\hat{\omega}_2}(\omega)$ – соответственно функции распределения $\hat{\omega}_1$ и $\hat{\omega}_2$.

Супериндикаторы $\hat{\omega}_1$ и $\hat{\omega}_2$ могут принимать бесконечное множество значений из интервала $(0,1]$ и имеют смысл апостериорной вероятности высказывания A в неопределенной ситуации $\hat{\aleph}$, задаваемой $\hat{y}$ и $\hat{z}$, соответственно.

Из всего сказанного можно сделать вывод, что безусловная (априорная) вероятность случайного события $\hat{A} \simeq (\hat{z} < \hat{y})$ равна математи-

ческому ожиданию его условной (апостериорной) вероятности или, другими словами, это его средневзвешенная достоверность. При этом, достоверность события $\hat{A}$ распределена на интервале $(0,1]$ с плотностью $\varphi_{\hat{\omega}_1}(\omega)$ или $\varphi_{\hat{\omega}_2}(\omega)$. Из сказанного следует, что не только ситуация неопределенна (случайны $\hat{z}$ и $\hat{y}$), но и степень истинности соответствующего высказывания (степень достоверности события $\hat{A} \simeq (\hat{z} < \hat{y})$ случайна и может принимать значения, отличные от 0 и 1 или $\overline{\omega}_1 \neq P(\hat{\omega}_1 = 1)$; $\overline{\omega}_2 \neq P(\hat{\omega}_2 = 1)$.

Таким образом, в приведенной трактовке неопределенность ситуации $\hat{\aleph}$, в которой нарушителю придется действовать, характеризуется возможными значениями супериндикатора $\hat{\omega}$, а случайность высказывания $\hat{A}$ характеризуется вероятностью P его достоверности.

Супериндикаторы $\hat{\omega}_1$ и $\hat{\omega}_2$ совмещают в себе свойства и функции $\omega(\hat{y})$ (3) случайного аргумента и случайной функции $\hat{\omega}(y)$ (4), т.е. представляют собой случайные функции случайных аргументов.

Физический смысл таких свойств стохастических индикаторов заключается в следующем. В предикате $\hat{z} < \hat{y}$ переменная $\hat{y}$ определяет границу "*неопределенного*" ("*случайного*") множества $\hat{A} = (-\infty, \hat{y})$, при попадании в которое случайной величины $\hat{z}$ индикаторы $\hat{\omega}_1$, $\hat{\omega}_2$ могут принять уже любые значения из интервала (0, 1]. Для практического применения математического аппарата стохастических супериндикаторов необходимо знать законы их распределения. Введем обозначения:

$$\hat{\omega}_2 \overset{d}{=} R_{\hat{y}}(\hat{z}); \quad \omega = \omega(y) = R_{\hat{y}}(z); \quad z = z(\omega) = R_{\hat{y}}^{-1}(\omega).$$

Тогда, если функции распределения $R_{\hat{y}}(y)$ и $R_{\hat{z}}(z)$ случайных величин $\hat{y}$ и $\hat{z}$ известны, то:

$$F_{\hat{\omega}_2}(\omega) \overset{d}{=} P(\hat{\omega}_2 < \omega) = P\{R_{\hat{y}}(\hat{z}) < R_{\hat{y}}[z(\omega)]\} = P[\hat{z} > z(\omega)] =$$
$$= R_{\hat{z}}[z(\omega)] = R_{\hat{z}}[R_{\hat{y}}^{-1}(\omega)], \quad \omega \in (0,1].$$

В результате $F_{\hat{\omega}_2}(\omega) = R_{\hat{z}}[R_{\hat{y}}^{-1}(\omega)]$.

Как было показано выше, соотношение $Y^{\Pi}_{\langle 3\rangle} \in \{ Y^{\partial}_{\langle 3\rangle} \}$ представляет собой формальное выражение цели ИВ нарушителя. Введем следующие обозначения: $v^{T} \overset{d}{=} \hat{z}_1$; $r^{\Pi} \overset{d}{=} \hat{z}_2$; $\tau^{Д} \overset{d}{=} \hat{z}_3$.

Тогда критерий пригодности результатов ИВ, проводимого нарушителем, примет вид:

$$G_{ЦР}: \ (\hat{Y}_{\langle 3\rangle} \in \{\hat{Y}^{\partial}_{\langle 3\rangle}\}) \simeq (\hat{Y}_{\langle 3\rangle} \gtrless \hat{Z}_{\langle 3\rangle}) \simeq [(\hat{y}_1 \geq \hat{z}_1) \cap (\hat{y}_2 \leq \hat{z}_2) \cap (\hat{y}_3 \leq \hat{z}_3)] .$$

В результате, *вероятность достижения нарушителем цели операции* будет определяться выражением:

$$P^{ИВ}_{ДЦ} = P\left(\hat{Y}_{\langle 3\rangle} \in \left\{\hat{Y}^{\partial}_{\langle 3\rangle}\right\}\right) = P\left(\hat{Y}_{\langle 3\rangle} \gtrless \hat{Z}_{\langle 3\rangle}\right) = \begin{cases} \int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty} \Phi_{\hat{Y}_{\langle 3\rangle}}\left(Z_{\langle 3\rangle}\right) dF_{\hat{z}_{\langle 3\rangle}}\left(Z_{\langle 3\rangle}\right), \\ \int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty} \overline{\Phi}_{\hat{z}_{\langle 3\rangle}}\left(Y_{\langle 3\rangle}\right) dF_{\hat{Y}_{\langle 3\rangle}}\left(Y_{\langle 3\rangle}\right). \end{cases} . \qquad (6)$$

По структуре выражений (6) видно, что $P^{ИВ}_{ДЦ}$ представляет собой математическое ожидание одной из случайных величин: $\hat{\omega}^{\langle 3\rangle}_1 \overset{d}{=} \Phi_{\hat{Y}_{\langle 3\rangle}}(\hat{Z}_{\langle 3\rangle})$ или $\hat{\omega}^{\langle 3\rangle}_2 \overset{d}{=} \overline{\Phi}_{\hat{z}_{\langle 3\rangle}}(\hat{Y}_{\langle 3\rangle})$, называемых соответственно первым и вторым стохастическими супериндикаторами третьего ранга. Соответственно:

$$P^{ИВ}_{ДЦ} = \overline{\omega^{\langle 3\rangle}_i} = M_{\hat{\omega}^{\langle 3\rangle}_i} = M\,[\,\hat{\omega}^{\langle 3\rangle}_i\,] = \int\limits_0^1 \omega\, dF_{\hat{\omega}^{\langle 3\rangle}_i}(\omega) , \ [i = 1,2].$$

В связи с этим вероятность $P^{ИВ}_{ДЦ}$ имеет смысл средней условной (*апостериорной*) вероятности достижения цели операции.

Следует обратить внимание, что математическое ожидание $M\left[\hat{\omega}^{\langle 3\rangle}_i\right]$ случайной величины $\hat{\omega}^{\langle 3\rangle}_2$ (стохастического супериндикатора третьего ранга) дает прогноз лишь средних результатов будущих массовых опытов, тогда как закон распределения $F_{\hat{\omega}^{\langle 3\rangle}_2}(\omega)$ супериндикатора $\hat{\omega}^{\langle 3\rangle}_2$ позволяет прогнозировать результаты единичных опытов.

Если известен закон распределения $F_{\hat{\omega}^{\langle 3\rangle}_2}(\omega)$, то могут быть определены два важных показателя эффективности уникальных ИВ, называемые гарантируемыми вероятностями достижения её цели:

$$\omega^{\Gamma}_{ДЦ}(\gamma)=\begin{cases}\omega^{\Gamma}_{1}(\gamma)\overset{d}{=}R_{\hat{\omega}^{\langle 3\rangle}_{1}}(\gamma)=F_{\hat{\omega}^{\langle 3\rangle}_{1}}(1-\gamma);\\ \omega^{\Gamma}_{2}(\gamma)\overset{d}{=}R_{\hat{\omega}^{\langle 3\rangle}_{2}}(\gamma)=F_{\hat{\omega}^{\langle 3\rangle}_{2}}(1-\gamma),\end{cases}$$

где γ– уровень гарантии (*гарантийная вероятность*).

Поскольку при определении гарантируемой вероятности $\omega^{\Gamma}_{ДЦ}(\gamma)$ используется закон распределения супериндикатора $\hat{\omega}^{\langle 3\rangle}_{2}$, то этот показатель позволит оценить в будущем эффективность уникальных (единичных) операций, в отличие от вероятности $P^{ИВ}_{ДЦ}$, достаточно полно характеризующей эффективность лишь массовых операций. По своей природе реализация сценария ИВ уникальна, что говорит о большой значимости показателя $\omega^{\Gamma}_{ДЦ}(\gamma)$. Стоит отметить, что при немногократном и особенно при одноразовом применении нарушителем средства ИВ (для реализации единичного ИВ) отклонения показателя $\hat{\omega}^{\langle 3\rangle}_{2}$ эффективности ИВ от его среднего значения $\omega^{\Gamma}_{ДЦ}(\gamma)$ можетт оказаться существенным и тогда надо считаться с возможностью появления неожиданностей в каждом отдельном случае.

В определении показателя эффективности операции $\omega^{\Gamma}_{ДЦ}(\gamma)$ фигурируют две вероятности: гарантируемая – ω^{Γ} и гарантийная – γ. Для уяснения их различия дадим их частотные трактовки.

Поскольку $\omega^{\Gamma}_{ДЦ}(\gamma)$ – это наименьшее (с вероятностью γ) из значений условной вероятности $\hat{\omega}^{\langle n\rangle}=\Phi_{\hat{Y}_{\langle n\rangle}}(\hat{Z}_{\langle n\rangle})$, принимаемых ею при фиксации условий применения $B''_{\langle l''\rangle}$ нарушителем средств ИВ, т.е. при фиксации значения $\hat{Z}_{<n>}$ вектора $\hat{Z}_{\langle n\rangle}$, то $\omega^{\Gamma}_{ДЦ}(\gamma)$ имеет смысл минимально возможной (с вероятностью γ) доли реализации условий применения нарушителем средств ИВ, в которых цель операции достигается с вероятностью $\hat{\omega}^{\langle n\rangle}\geq\omega^{\Gamma}_{ДЦ}(\gamma)$. Например, следующая запись $\omega^{\Gamma}_{ДЦ}(0{,}8)=0{,}1$ соответствует $\omega^{\Gamma}_{2}(0{,}8)\overset{d}{=}R_{\hat{\omega}^{\langle 3\rangle}_{2}}(0{,}8)=P(\hat{\omega}^{\langle 3\rangle}_{2}\geq 0{,}8)=0{,}1$. Это означает, что в данный момент с вероятностью $P^{ИВ}_{ДЦ}\geq 0{,}8$ успех реализации уникального ИВ возможен только в 10% случаев.

В зависимости от динамики обстановки требования $P^{ТР}_{ДЦ}$ к показателю эффективности $P^{ИВ}_{ДЦ}$, так и сам $P^{ИВ}_{ДЦ}$ будут меняться, и как след-

ствие, они будут являться случайными величинами – $\hat{P}_{ДЦ}^{ТР}$, $\hat{P}_{ДЦ}^{ИВ}$. В результате показатель эффективности действий нарушителя принимает вид $P_{Н}^{*}(\hat{P}_{ДЦ}^{ИВ} \geq \hat{P}_{ДЦ}^{ТР})$. Эта ситуация соответствует задаче, требующей рассмотрения предиката вида $\hat{\omega}_i \geq \hat{\omega}_j$ (где $\hat{\omega}_i$, $\hat{\omega}_j$ – индексные супериндикаторы), вычисления вероятности $P(\hat{\omega}_i < \hat{\omega}_j)$ и анализа её стохастических свойств, аналогичного приведенному выше применительно к вероятности $P(\hat{y} > \hat{z})$. Для решения таких задач потребуется трансформировать распределения супериндикаторов $\hat{\omega}_i$, $\hat{\omega}_j$, которые в этом случае будут называться индикаторами *первого порядка*, в индикаторы $\hat{\omega}_{ij}^{[2]}$, $\hat{\omega}_{ji}^{[2]}$ *второго порядка* и реализовать следующую процедуру:

$$P(\hat{\omega}_j > \hat{\omega}_i) = \int_0^1 R_{\hat{\omega}_j}(\omega) dF_{\hat{\omega}_i}(\omega) = \int_0^1 \omega dF_{\hat{\omega}_{ji}^{[2]}}(\omega) = \overline{\omega_{ji}^{[2]}}.$$

8. Заключение. Процесс познания возможных нарушений ИБ бесконечен и, следовательно, на любой период времени знания исследователя содержат элемент неопределенности, а число ступеней (уровней) этого анализа может неограниченно расти. Действительно, все вероятностные модели случайных явлений строятся в предположении, что основные условия эксперимента известны. Так, в "элементарной" теории вероятностей – это комплекс $\aleph$ условий "эксперимента", в аксиоматической теории – это *пространство U элементарных событий*, в математической статистике – это *генеральная совокупность*.

Это допущение легло в основу существующих в настоящее время вероятностных моделей случайных явлений, присущих понятию ИБ. Эти модели строятся в предположении, что известны:

– условия проведения операции, например, условия проведения сценария ИВ;

– законы распределения и значения числовых характеристик исследуемых случайных величин (векторы $\hat{A}'_{\langle k' \rangle}, \hat{A}''_{\langle k'' \rangle}, \hat{B}'_{\langle l' \rangle}$).

Однако используемые в настоящее время вероятностные модели дают прогнозы лишь средних результатов будущих массовых опытов, поэтому вероятность $P_{ДЦ}^{ИВ}$ успеха ИВ, вычисленная в данных условиях, будет достаточно полно характеризовать эффективность лишь массовых воздействий, что концептуально не верно.

По своей природе реализация сценария ИВ уникальна, так как наилучшим решением для нарушителя в конфликтной ситуации будет именно выйти за пределы известных сценариев ИВ. С другой стороны,

если условия $\aleph$ проведения нарушителем ИВ (векторы $B'_{\langle l' \rangle}$, $B''_{\langle l'' \rangle}$.) до его проведения неизвестны (с достаточной полностью), то задача определения вероятностей $P_{ДЦ}^{ИВ}$ исходов ИВ становится неопределенной. Для разрешения данной проблемы – прогнозирования результатов единичных опытов, эффективен математический аппарат теории стохастической индикации. Он служит основой для разработки методов оценивания эффективности уникальных операций, для исследования которых известные вероятностные методы малопригодны.

Штатное функционирование технологического процесса зависит от качества работы множества других производственных процессов, нарушение которых является целью ИВ нарушителя. Тогда можно говорить, что выходом разработанного операционного комплекса является множество стохастических супериндикаторов, соответствующих множеству целей ИВ нарушителя. В комплексе эти супериндикаторы дают некую интегральную оценку-индикатор. Физический смысл этого индикатора характеризуется качеством системы защиты по противодействию нарушителю; относительной оценкой защищенности АСУ ТП и мерой неопределенности ситуации, в которой действует нарушитель.

Исследование в динамике значений индикатора, принимаемых им в ходе функционирования операционного комплекса, позволит в дальнейшем выявлять как сам факт присутствия нарушителя в АСУ ТП, так и доступные ему сценарии ИВ. Следует отметить прогностические возможности операционного комплекса, позволяющие исследовать нарушителя в текущий момент времени, а также генерировать с опережением новые модели нарушителя, исследовать их возможности и предлагать различные варианты защиты.

Литература

1. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России). URL: http://fstec.ru (дата обращения: 27.01.2015).
2. *Горбачев И.Е., Еремеев М.А., Андрушкевич Д.В.* Методологические основы оценивания эффективности действий сторон информационного конфликта в инфотелекоммуникационных системах // Материалы 23-й научно-практической конференции “Методы и технические средства обеспечения безопасности информации”. С-Пб.: Издательство Политехнического университета. 2014. С. 11–13.
3. *Горбачев И.Е., Еремеев М.А.* К вопросу о применении стохастического супериндикатора в задачах оценивания защищенности информации в автоматизированных систем // Проблемы информационной безопасности. Компьютерные системы. 2013. № 2. С. 20–25.
4. *Горбачев И.Е., Еремеев М.А.* Подход к применению методов стохастической индикации в задачах оценивания эффективности защиты информации в автоматизированных системах // Материалы 22-й научно-практической конференции “Методы и технические средства обеспечения безопасности информации”.

СПб.: Издательство Политехнического университета. 2013. С. 14–16.
5. *Петухов Г.Б., Якунин В.И.* Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем // М.: АСТ. 2006. 504 с.
6. *Горбачев И.Е., Еремеев М.А.* Особенности технологии маскирования информационных ресурсов с применением обманных систем и управлением поведением нарушителя // Материалы 23-й научно-практической конференции “Методы и технические средства обеспечения безопасности информации”. С-Пб.: Издательство Политехнического университета. 2014. С. 13–15.
7. *Бирюков Д.Н., Ломако А.Г.* Подход к построению системы предотвращения киберугроз // Проблемы информационной безопасности. Компьютерные системы. 2013. №2. С. 13–19.
8. *Чечулин А. А.* Методика оперативного построения, модификации и анализа деревьев атак // Труды СПИИРАН. 2013. Вып. 3(26). С. 40–53.
9. ГОСТ Р ИСО/МЭК 18045-2013. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий // М.: Госстандарт России. 2014.

References

1. Oficial'nyj sajt Federal'noj sluzhby po tehnicheskomu i jeksportnomu kontrolju (FSTJeK Rossii) [Official website of the Federal Service for Technical and Export Control (FSTEC Russia)]. Available at: http://fstec.ru. (accessed 27.01.2015). (In Russ.).
2. Gorbachev I.E., Eremeev M.A., Andrushkevich D.V. [Methodological bases of evaluation of efficiency of actions of the parties to the conflict in information systems infotelecommunication]. *Materialy 23 nauchno-prakticheskoy konferenciyi “Metody I tehnicheskiye sredstva obespecheniya bezopasnosti informacii”* [Materials of the 23nd scientific and practical conference "Methods and Technical Means of Safety of Information"]. SPB: St. Petersburg Polytechnical University, 2014. pp. 11–13. (In Russ).
3. Gorbachev I.E., Eremeev M.A. [On the question of the application of stochastic superindikatora in problems of estimation of information security in automated systems]. *Problemy informatsionnoy bezopasnosty. Kompyuternie sistemy – Problems of information security. Computer systems*. SPB: St. Petersburg Polytechnical University. 2013. vol. 2. pp. 20–25. (In Russ).
4. Gorbachev I.E., Eremeev M.A. [Approach to the use of stochastic methods in problems of estimation indicating the effectiveness of the protection of information in automated systems]. *Materialy 22 nauchno-prakticheskoy konferenciyi “Metody I tehnicheskiye sredstva obespecheniya bezopasnosti informacii”* [Materials of the 22nd scientific and practical conference "Methods and Technical Means of Safety of Information"]. SPB: St. Petersburg Polytechnical University. 2013. pp. 14–16. (In Russ).
5. Petuhov G.B., Jakunin V.I. *Methodological bases of the external design of targeted processes and dedicated systems*. [Methodological bases of the external design of targeted processes and dedicated systems]. Moscow: AST. 2006. 504 p. (In Russ).
6. Gorbachev I.E., Eremeev M.A. [Features of technology of masking of information resources with use of deceptive systems and management of behavior of the malefactor]. *Materialy 23 nauchno-prakticheskoy konferenciyi “Metody I tehnicheskiye sredstva obespecheniya bezopasnosti informacii”* [Materials of the 23nd scientific and practical conference "Methods and Technical Means of Safety of Information"]. SPB: St. Petersburg Polytechnical University. 2014. pp. 13–15. (In Russ).
7. Biryukov D.N., Lomako A.G. [Approach to creation of system of cyber-threats preventing]. *Problemy informatsionnoy bezopasnosty. Kompyuternie sistemy – Problems of information security. Computer systems*. SPB: St. Petersburg Polytechnical University. 2013. vol. 2. pp. 13–19. (In Russ).
8. Chechulin A.A. [Technique of rapid construction, modification and analysis of attack

trees]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2013. vol. 3(26). pp. 40–53. (In Russ).
9. GOST R ISO/MJeK 18045-2013. [Information technology. Methods and means of ensuring safety. Methodology for Information Technology Security Evaluation]. M.: Gosstandart Rossii. 2014. (In Russ.).

Горбачев Игорь Евгеньевич — к-т техн. наук, докторант кафедры систем сбора и обработки информации, Военно-космическая академия, имени А.Ф. Можайского. Область научных интересов: исследование операций, информационная безопасность, искусственный интеллект, информационные конфликты в инфотелекоммуникационном пространстве. Число научных публикаций — 60. gie1976@mail.ru; ул. Ждановская, д. 13, 197198, Санкт-Петербург; р.т.: +7(812) 347-96-87.

Gorbachev Igor' Evgen'evich — Ph.D., doctoral student of system for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: research of operations, artificial intelligence, information security, the information conflicts in infotelekommunikatsionny space. The number of publications — 60. gie1976@mail.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812) 347-96-87.

Глухов Александр Петрович — к-т техн. наук, начальник департамента информационной безопасности, ОАО «РЖД». Область научных интересов: информационная безопасность, охрана объектов железнодорожного транспорта. Число научных публикаций - 40. gie76@yandex.ru; ул. Ждановская, д. 13, 197198, Санкт-Петербург; р.т.: +7(812) 347-96-87.

Gluhov Aleksandr Petrovich — Ph.D., head of department of information security, JSC «RZhD». Research interests: information security, protection of railways. The number of publications — 40. gie76@yandex.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812) 347-96-87.

РЕФЕРАТ

Горбачев И.Е., Глухов А.П. **Моделирование процессов нарушения информационной безопасности критической инфраструктуры.**

Нарушитель в критической инфраструктуре представлен в виде опасных процессов – процессов нарушения информационной безопасности. Эти деструктивные процессы совместно с процессами защиты образуют так называемые конфликтующие процессы, а исследование эффективности их противодействия является актуальной задачей. Существующие вероятностные модели случайных явлений в области информационной безопасности существенно ограничены и обладают концептуальными недостатками для разрешения этой задачи.

Для исследования сценариев информационных воздействий нарушителя разработан операционный комплекс моделирования процессов нарушения информационной безопасности. Одним из требованием к качеству комплекса являлось наличие у него прогностических возможностей, позволяющих генерировать с временным опережением новые модели нарушителя, исследовать их возможности, проектировать различные варианты защиты, и, как следствие, предотвращать информационные воздействия.

С этой целью обоснована математическая модель стохастического супериндикатора – агрегированного показателя качества процессов нарушения, семантический аспект которого характеризуется эффективностью противоборства конфликтующих процессов. Данный супериндикатор позволяет исследовать деструктивные процессы, характерные массовым информационным воздействиям с информативной выборкой и, как следствие, выдать прогнозы средних результатов будущих массовых опытов.

С другой стороны, рациональным решением для нарушителя в конфликтной ситуации является выход за пределы известных сценариев информационных воздействий, что говорит об их уникальности и, как следствие, их скрытности. Для исследования этих процессов известные вероятностные методы малопригодны, в то время как стохастического супериндикатор позволяет оценивать уникальные процессы и давать прогноз их развития.

Исследование в динамике значений индикаторов каждого моделируемого процесса, принимаемых ими в ходе функционирования операционного комплекса, позволит в дальнейшем выявлять факт присутствия нарушителя в критической инфраструктуре, доступные ему сценарии информационных воздействий, и как следствие, реализовать внешнее проектирование системы защиты.

SUMMARY

Gorbachev I.E., Glukhov A.P. **Modeling of Processes of Information Security Violations of Critical Infrastructure.**

Malefactor in the critical infrastructure is presented as dangerous processes - processes of information security violations. These destructive processes, together with the processes of protection form the so-called conflicting processes and study the effectiveness of their counter is an urgent task. Existing probabilistic model of random phenomena in the field of information security are severely limited and have conceptual difficulties to resolve this problem.

To investigate the effects of malefactor information scenarios the operating complex for process modeling of information security was developed. One of the requirements for the quality of the complex is the presence of a prognostic features to generate a timing advance new models malefactor explore their opportunities to design various security options, and as a result, to prevent information exposure.

The mathematical model of the stochastic super indicator – aggregate quality indicator for processes violations, semantic aspect which is characterized by the confrontation of conflicting processes, is justified. This allows to explore super indicator destructive processes of typical mass information influences with informative sample and, consequently, to give the results of future projections of average mass experiments.

On the other hand, a rational decision for the malefactor in a conflict situation is going beyond the known effects of scripting information that speaks to their uniqueness and, as a consequence, their stealth. To investigate these processes known probabilistic methods are not suitable, while stochastic super indicator allows to evaluate the unique processes and provide a forecast of their development.

Study the dynamics of the indicator values of each of the simulated process, adopted by them in the course of the operation of complex operational, will further identify the fact of the presence of the malefactor in the critical infrastructure, information available to him scenarios impacts, and as a consequence, to implement the external design of the protection system.

УДК 004.931, 004.942

А.А. ПЛАТОНОВ, В.И. ТИМОФЕЕВ

КОНТРОЛЬ ЦЕЛОСТНОСТИ ДИНАМИЧЕСКИХ ОБЪЕКТОВ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ МЕТРИЧЕСКИХ ЭТАЛОНОВ

Платонов А.А., Тимофеев В.И. **Контроль целостности динамических объектов вычислительных систем с использованием метрических эталонов.**
Аннотация. В статье предлагается подход к контролю целостности динамических объектов по их метрическим эталонам. Создание эталона основывается на последовательном преобразовании процесса от дампа памяти до автомата переходов на графе состояний с расчетом структурных, информационных и операционных метрик. Это позволяет выявлять нарушения функциональных состояний объекта в памяти вычислительной системы. Представлен алгоритм контроля целостности динамических объектов антивирусного средства Dr.Web.
Ключевые слова: целостность, метрика программного обеспечения, формальная грамматика, продукционная система, конечный автомат, распознаватель.

Platonov A.A., Timofeev V.I. **Monitoring of Integrity of Dynamic Objects of Computing Systems with Use of Metric Standards.**
Abstract. In article approach to monitoring of integrity of dynamic objects on their metric standards is offered. Creation of a standard is based on sequential conversion of process from a memory dump to the machine gun of transitions on a state graph with calculation of structural, information and operational metrics. It allows to reveal violations of the functional statuses of object in memory of the computing system. The algorithm of monitoring of integrity of dynamic objects of anti-virus means of Dr.Web is provided.
Keywords: integrity, software metrics, the formal grammar, productional system, finite state machine, recognizer.

1. Введение. Для обеспечения информационной безопасности автоматизированных систем (АС) и предотвращения возникновения скрытых каналов доступа (СКД) к информационным ресурсам АС необходимо обеспечивать целостность, конфиденциальность и доступность всех информационных объектов в АС.

Среди всех информационных объектов в АС выделяют статические объекты и динамические объекты. К первым относят программные файлы и сетевые пакеты, то есть объекты, которые в течение относительно длительного времени функционирования АС могут оставаться неизменными. Вторую группу составляют вычислительные процессы и потоки – программные образы, постоянно находящиеся в оперативной памяти. Особенностью второй группы является непрерывно меняющиеся характеристики (исполняемый код и данные) информационных объектов в режиме времени близком к

реальному. Данная особенность приносит с собой дополнительный ряд угроз, которым подвержены динамические объекты. Наиболее актуальная, из которых заключается в трудности контроля целостности вычислительных процессов.

В таких обстоятельствах следует учесть, что для контроля целостности статических объектов (файлы, пакеты) АС существует достаточно много надежных способов. Эти способы основаны на использовании контрольных сумм и криптографических методов шифрования. Методы контроля динамически изменяемых объектов практически отсутствуют, если не считать механизм защиты виртуальной памяти, используемый в операционных системах (ОС).

Механизм защиты виртуальной памяти в основном направлен на обеспечение доступности и конфиденциальности динамических объектов. Это снижает угрозу нарушения целостности динамических объектов, но не устраняет ее полностью. При этом необходимо отметить, что самая распространенная в мире ОС компании Microsoft имеет закрытый код. Это обуславливает отсутствие возможности проверить эффективность данного механизма, а также затрудняет сертификацию этой ОС на предмет наличия скрытых функциональных возможностей этого механизма.

Актуальность поставленной задачи обусловлена необходимостью своевременного выявления фактов нарушения целостности динамических объектов в АС, и несовершенстве существующих методов по контролю целостности.

2. Назначение контроля целостности динамических объектов. Контроль целостности динамических объектов предназначен для реализации мер по защите вычислительных процессов от информационных атак, которые направлены на их уничтожение или модификацию.

Основные направления информационных атак, а также цели таких атак представлены на рисунке 1. Атака, проведенная на динамические объекты АС, может с большой степенью скрытности изменить весь функциональный набор такого объекта или нейтрализовать его.

Рис. 1. Направление вредоносного воздействия на информационные объекты

Под динамическими объектами подразумеваются вычислительные процессы и потоки. Контекст вычислительного процесса включает в себя: виртуальное адресное пространство (память), исполняемый код, дескрипторы объектов, данные, приоритет, максимальный и минимальный размер рабочей области, первичный поток и его потомки (дочерние потоки).

Исследование существующих методов контроля целостности динамических объектов показало, что основным направлением в этой области является метод слежения за вызовом системных функций, а реализуется такой метод с помощью эвристик, закладываемых в специальные программы, так называемые системные мониторы (СМ).

Суть таких эвристик заключается в том что, из всех API (Application Programming Interface) функций выбираются наиболее критические, связанные с доступом к памяти, а также возможные их комбинации. Выбор производится, как правило, на основании статистики и экспертных оценок. Если при работе операционной системы будут возникать такие критические комбинации, то системный монитор немедленно прекратит работу приложения, инициирующего такую комбинацию, и выдаст сигнал администратору безопасности для дальнейшего анализа.

Разработка эвристик и дальнейшая их реализация в системных мониторах должна также учитывать наличие rootkit-программ, которые в своем составе почти всегда имеют API-перехватчик и NativeAPI-перехватчик. Этот факт также имеет большое влияние на эффективность работы системных мониторов.

Вычислительные процессы могут в процессе своей работы

использовать критически важные функции без зловредного умысла а, следовательно, реакция системных мониторов на них будет неоднозначна.

Все вышесказанное позволяет сделать вывод о том, что существующие методы контроля целостности не в полной мере соответствуют задаче поддержания неизменности функциональных возможностей динамического объекта [1].

Для решения задачи контроля целостности предлагается:

1. Создание инвариантного эталона динамического объекта независимого от его состояния.
2. Выявление нарушений целостности динамического объекта на основании сравнения текущего состояния объекта с эталоном.

3. Структурированный эталон динамического объекта. Проведенный системный анализ динамических объектов показал, что универсальной моделью, отражающей процесс, является управляющий граф, который вместе с дампом памяти являются исходными данными для решения задачи контроля целостности. Идея многомодельности программ позволяет интерпретировать универсальную модель в виде формальных грамматик и продукционных правил, конкретизированных под решаемую задачу, а также автомата, реализующего эти модели [1]. Особенности представления процессов в виде таких моделей позволит выявить разного рода воздействия на них, и осуществить контроль целостности.

Для создания эталона динамического объекта необходимо выполнить ряд действий:

– выбрать множество состояний динамического объекта, разнесенных по времени и свойствам;

– рассчитать для каждого из множества состояний объекта метрики, и на их основании построить множество метрических моделей;

– обобщить данные из множества метрических моделей одного объекта, и создать его эталонную метрическую модель.

В соответствии с системным подходом к интерпретации вычислений, различают: формальную модель языка структур, задаваемую грамматикой, формализацию логических свойств вычислений, задаваемую продукционными системами и формальную модель реализации системы действий представленную автоматными моделями вычислений [2].

Общая система многомодельного представления вычислительного процесса представлена на рисунке 2.

Основой для разработки трех моделей вычислительного

процесса являются дамп памяти $C =< \sigma, K >$, где σ – состояние памяти, а K – активный оператор, и управляющий граф программы $G(V, E)$, где V – количество вершин (состояний), а E – число дуг (переходов). Анализ графа позволяет создать регулярную грамматику, систему нормальных продукций, а также конечный автомат.

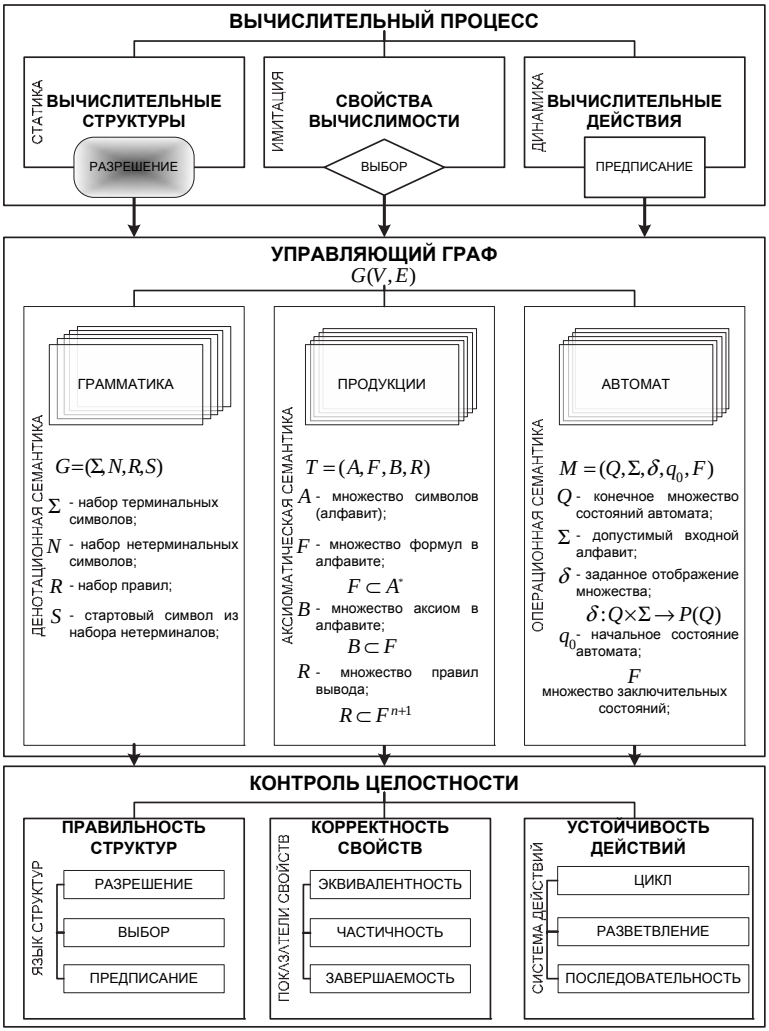


Рис.2. Система многомодельного представления вычислительного процесса

Каждая из предлагаемых моделей, позволяет контролировать один из трех компонентов, выбранного базиса. Под контролем в нашем случае подразумевается слежение за правильностью вычислительных структур, корректностью свойств вычислимости и устойчивостью вычислительных действий. Реализация этого контроля происходит на основании присущих каждой из моделей специфических характеристик.

С точки зрения правильности вычислительных структур, задаваемых в «Разрешениях», различают функциональное («Разрешение разрешений»), логическое («Разрешение условий») и алгебраическое («Разрешение предписаний») программирование. Каждый из этих видов программирования имеет соответствующее понятие правильности исполняемого кода.

Вывод о корректности вычислений можно сделать на основании свойств эквивалентности, частичной правильности и завершаемости.

Общая устойчивость действий вычислительного процесса зависит от выполнения частных участков кода, поэтому разобьем исполняемый код на различные сочетания базовых конструкций языков программирования: «Цикл», «Разветвление» и «Последовательность». Это позволит более тщательно контролировать изменения выполнения инструкций в любой момент времени.

Все вышесказанное, позволяет перейти от общей структурированной модели вычислительного процесса к частной, представленной на рисунке 3. На этом рисунке отображены конструкции основного базиса на множестве численных показателей метрического пространства программ [3].

В аспекте вычислительной структуры и свойств вычислимости программы можно ограничиться рассмотрением её топологических и информационных мер, в основе которых лежат топологические характеристики граф-модели программы, а также структуры и модели данных [4-6].

Именно эти меры удовлетворяют подавляющему большинству требований, предъявляемых к метрическим показателям: общность применимости, адекватность рассматриваемому свойству, существенность оценки, состоятельность, количественное выражение, воспроизводимость измерений, малая трудоёмкость вычислений, возможность автоматизации оценивания.

И, наконец, именно топологические и информационные меры наиболее употребимы в целях построения метрического эталона динамического объекта, чувствующего структурные искажения и нарушения свойств объекта [5].

Для отражения вычислительных действий базовых конструкции управления, которые применяются в языках программирования, был выбран вероятностный аппарат, введенный в работе Карповского Ефима Яковлевича [7].

ТИПЫ		МЕТРИКИ	
СТРУКТУРА	РАЗРЕШЕНИЕ	ТОПОЛОГИЯ	Метрика Маккейба $C = e - n + 2$ Метрика Майерса $[Z(G), Z(G)+h]$ Метрика Вудворда $Y(x)$ Метрика Мак-Клура $M(P) = fp * X(P) + gp * Y(P)$ Функциональная мера $f_1 = \sum c_1$ Метрика Кафура $I = length * (fan\_in * fan\_out)^2$
	ВЫБОР		Метрика Чена $M(G) = (n(G), N, Q_0)$ Метрика точек пересечения $\min(a,b) < \min(p,q) < \max(a,b) \& \max(p,q) > \max(a,b)$ $\min(a,b) < \max(p,q) < \max(a,b) \& \min(p,q) < \min(a,b)$ Метрика Пратта $M(\{F_1, F_2, ...F_n\}) = \sum_{i=1}^{n} M(F_i)$ Метрика Чепина $Q = P + 2M + 3C + 0,5T$
	ПРЕДПИСАНИЕ		Метрика Джилба $cl = CL / L,\ f = N_{cв} / L_{\text{mod}}$ Метрика Пивоварского $N(G) = V^*(G) + \sum P_i$ Метрика регулярных выражений $P(G) = N + L + \sum_{i} k$ Метрика спена $n, n-1$
СВОЙСТВА	ЭКВИВАЛЕНТНОСТЬ	ИНВАРИАНТ	Информационная энтропия $H(x) = -\sum_{i=1}^{n} p(i) \log_2 p(i)$
	ЧАСТИЧНОСТЬ		Информационное содержание $I = (\frac{\eta_1^*}{\eta_1} * \frac{\eta_2}{N_2}) * (\log_2 \eta * (\eta_1 \log_2 \eta_1 + \eta_2 \log_2 \eta_2))$
	ЗАВЕРШАЕМОСТЬ		Информационная мера Берлингера $I(R) = m(F^*(R) \times F^-(R))^2$
ДЕЙСТВИЯ	ЦИКЛ	ВЕРОЯТНОСТЬ	Время $\tau(\Phi_3) = (1 - P_a)\tau(a) \sum_{i=0}^{U} P_a^i + (1 - P_a)\left[\tau(a) + \tau(g)\right] \sum_{i=0}^{U} i P_a^i$ $\tau(\Phi_2) = P_a\left[\tau(a) + \tau(g) + (1 - P_a)\right]\left[\tau(a) + \tau(h)\right]$ $\tau(\Phi_1) = \tau(g) + \tau(g)$
	РАЗВЕТВЛЕНИЕ		Среднеквадратическое отклонение времени $\sigma_\tau(\Phi_2) = \sqrt{P_a\left[\sigma_\tau^2(a) + \sigma_\tau^2(g)\right] + (1 - P_a)\left[\sigma_\tau^2(a) + \sigma_\tau^2(g)\right]}$ $\sigma_{t\Gamma}(\Phi_1) = \sqrt{\sigma_\tau^2(g) + \sigma_\tau^2(h)}$ $\sigma_\tau^2(\Phi_3) = (1 - P_a) \sum_{i=0}^{U} P_a^i \left[\sigma_\tau^2(a) + i\sigma_\tau^2(a) + i\sigma_\tau^2(g)\right] + (1 - P_a)$ $\sum_{i=0}^{U} P_a^i \left[(1+i)\tau(a) + i\tau(g)\right]^2 - \left\{ \sum_{i=0}^{U} P_a^i (1 - P_a)\left[(1+i)\tau(a) + i\tau(g)\right]^2 - \right\}$
	ПОСЛЕДОВАТЕЛЬНОСТЬ		Вероятность наступления события P_a, P_g $P(A) = K_a / M_a$ $P(G) = K_g / M_g$

Рис. 3. Модель представления вычислительного процесса в базисе {<структура>, <свойства>, <действия>}

Все вышеперечисленные показатели позволяют нам контролировать целостность динамических объектов на основании выдвинутого базиса программ, который является неизменным на всем протяжении работы исполняемого кода. В дальнейшем нам предстоит только конкретизировать некоторые аспекты, предложенной частной структурированной модели динамического объекта (вычислительного процесса), а также подготовить для нее исходные данные.

В целях оптимального выбора метрик, лежащих в основе разработанной модели, предлагается ввести структурированный базис для конструкций языка ассемблер.

Базис конструкций охватывает все возможные типовые структуры, которые могут существовать в исполняемом коде программы. Наличие пересечений стандартных типовых конструкций («цикл-цикл» – «вложение», «разветвление-разветвление» – «ветвление», «последовательность-последовательность» – «составление») наиболее ярко отражают ключевые точки управляющего графа вычислительного процесса.

Простейшая конструкция «разветвление» самая распространенная из всех, а соответственно наиболее ярко отражает структуру процесса.

Анализ всех топологических метрик сложности для структурированного базиса конструкций сводится в метрическое пространство (рисунок 4), составляющее эталон.

Структуры процесса заданы набором показателей:

$$Q_1 = (q_{11}, q_{12}, q_{13}, ..., q_{19}), \quad (1)$$

где q_{1i} – один из метрических показателей, представленных на рисунке 3.

Метрический эталон свойств вычислимости динамических объектов (рисунок 5), содержит информационную энтропию q_{21}, информационное содержание q_{22} и информационную меру Берлингера процесса q_{23}.

$$Q_2 = (q_{21}, q_{22}, q_{23}). \quad (2)$$

Показатели, используемые для создания эталона устойчивости действий, представлены на рисунке 6.

Расчет метрических показателей динамического объекта производится как на этапе эталонирования, так и на этапе контроля целостности.

В качестве модели представления вычислительного процесса

выбрана частная метрическая модель $x_k\{Q_\gamma : \gamma = 1(1)3\}$ основу, которой составляют метрические показатели.

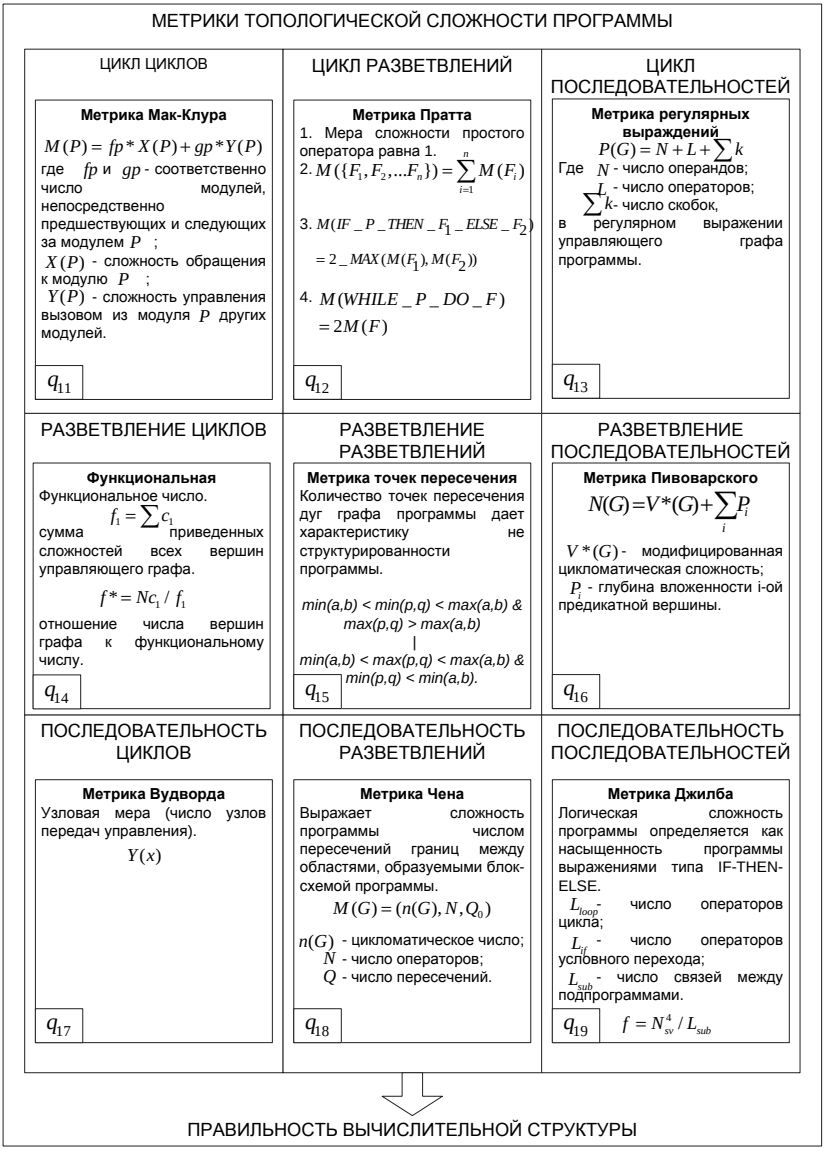


Рис. 4. Метрический эталон структуры вычислительного процесса

Метрические показатели, как уже было сказано выше, разделены на три категории:

1. Метрики структуры вычислительного процесса $Q = (q_{11}, q_{12}, ...q_{19})$.

2. Информационные показатели $Q_2 = (q_{21}, q_{22}, q_{23})$.

3. Критерии устойчивости выполнения вычислительного процесса $Q_3 = (q_{31}, q_{32}, ..., q_{39})$.

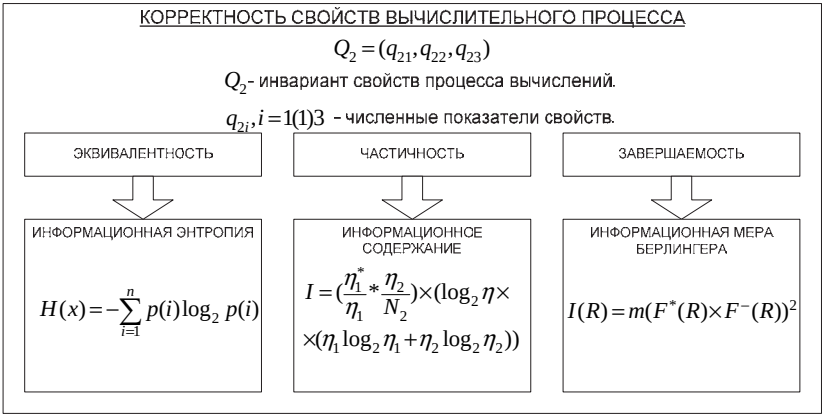
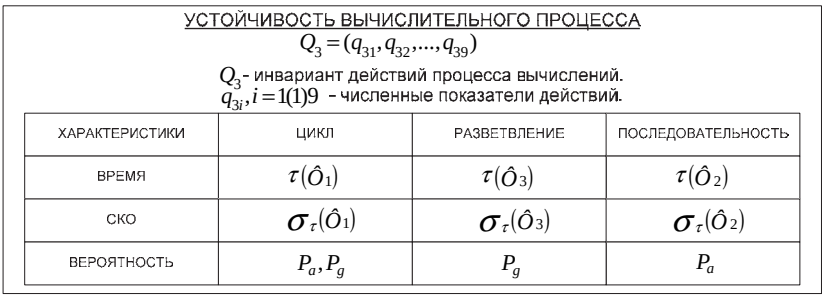


Рис. 5. Метрический эталон свойств вычислимости динамических объектов



ХАРАКТЕРИСТИКИ	ЦИКЛ	РАЗВЕТВЛЕНИЕ	ПОСЛЕДОВАТЕЛЬНОСТЬ
ВРЕМЯ	$\tau(\hat{O}_1)$	$\tau(\hat{O}_3)$	$\tau(\hat{O}_2)$
СКО	$\sigma_\tau(\hat{O}_1)$	$\sigma_\tau(\hat{O}_3)$	$\sigma_\tau(\hat{O}_2)$
ВЕРОЯТНОСТЬ	P_a, P_g	P_g	P_a

Рис. 6. Метрический эталон устойчивости действий динамических объектов

Представленные показатели, отражающие сущность динамического объекта, являются необходимым и достаточным условием для построения частной метрической модели.

После расчета всех метрических показателей на нескольких срезах (образах) эталонируемого динамического объекта можно приступать к создания векторов математического и среднеквадратического отклонения. В результате полученная модель

используется в качестве метрического эталона, который необходим для осуществления контроля целостности динамических объектов.

4. Выявление нарушений целостности динамического объекта. Выявление признаков нарушения целостности связано с задачей распознавания образов. Задача распознавания признаков нарушения целостности, а также существующие исходные данные нечетко определяют метод распознавания. Следовательно, необходимо заимствовать приемы статистических, структурно-лингвистических и кластерных методов. Это обусловлено набором статистических показателей $x_k = \{Q_\gamma : \gamma = 1(1)3\}$, срезов вычислительных процессов $X = (x_1, x_2, ..., x_k, ..., x_n)$ и наличием ситуаций неопределенности по соотнесению процесса вычислений к целостному ω_1 или нецелостному ω_4 классу. Решающим правилом (РП) является выражение 3, а решающей функцией 4.

В качестве ключевых (основных) элементов q_i выступают метрика точек пересечения, информационное содержание и среднее время выполнения конструкции «Разветвление».

$$d(x_k) = \begin{cases} \sum_{i=1}^{3} Q_i = 0 \rightarrow x_k \in \omega_1 \\ \sum_{i=1}^{3} Q_i = 1 \rightarrow x_k \in \omega_2 \\ \sum_{i=1}^{3} Q_i = 2 \rightarrow x_k \in \omega_3 \\ \sum_{i=1}^{3} Q_i = 3 \rightarrow x_k \in \omega_4 \end{cases} \quad (3)$$

$$IF(q_i \in [m_i \pm \sigma_i])THEN(Q_i = 0), \quad (4)$$

где q_i – ключевые показатели трех сущностей процесса вычислений;

m_i – математическое ожидание этих показателей;

σ_i – коэффициент строгости контроля целостности.

Коэффициент строгости позволяет гибко регулировать процесс контроля целостности в зависимости от назначения АС, и контролируемого динамического объекта, а также в зависимости от закона распределения метрического показателя.

Решающее правило определяет четыре класса целостности, которые представлены на рисунке 7.

Для решения дальнейшей задачи, и решение близости образа динамического объекта, относящегося ко второму (ω_2) или третьему (ω_3) классу, к целостному или нецелостному применяется аппарат нечетких распознавателей (кластерный анализ).

Специфика предлагаемого алгоритма нечеткой классификации состоит в том, что в отличие от существующих в данном алгоритме оценок параметра $q_k^* = (1, q_k)$ эта оценка может производиться нечетко и определяться функцией принадлежности (мерой близости) $\mu_0(q_k) = \max(\omega_i(q_k))$ для любых q_i .

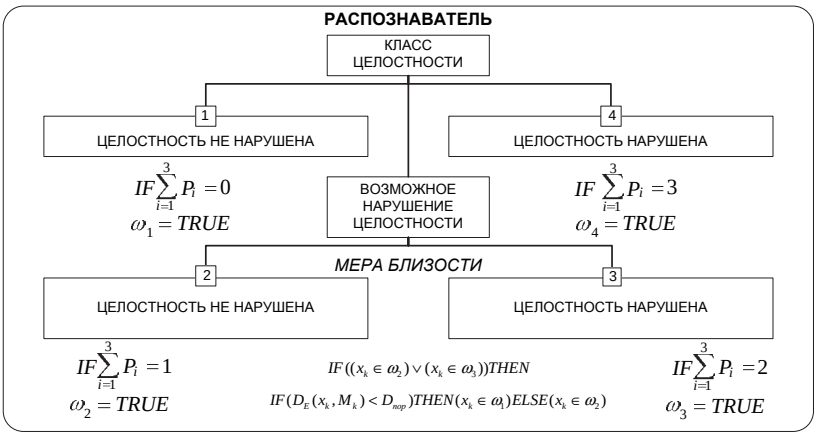


Рис. 7. Распознаватель классов состояний целостности динамических объектов

В качестве функции принадлежности (меры близости) было выбрано евклидово расстояние, которое вычисляется по формуле 5.

$$D_E(X, M_i) = \left\| X - M_i \right\|, \tag{5}$$

где M_i – вектор математического ожидания $M_i = (q_{11}, ..., q_{ki})$ его численных показателей.

В силу естественных рассуждений, очевидно, что предъявляемый для распознавания образ необходимо отнести к тому из классов, евклидово расстояние, до которого является наименьшим. Тогда соответствующее решающее правило может быть записано в представленном ниже виде (6).

$$X \in \omega_i = \arg\min D_E(X, M_i) . \tag{6}$$

Приведенный аппарат, а также в частности кластерной анализ, позволил построить распознаватель вредоносных воздействий на исполняемый код вычислительного процесса, который, помимо четкой классификации динамического объекта по признаку целостности, осуществляет процесс анализа при неопределенной конфигурации численных показателей.

5. Контроль целостности динамических объектов антивирусного средства Dr.Web 4.44. Сбор данных о динамических объектах Dr.Web, и последующий их анализ показал, что исходными данными для нашей технологии являются:

1. Процессы, протекающие в рамках функционирования антивирусного средства.
2. Важные характеристики этих процессов, которые необходимы для корректного снятия дампа памяти: страницы виртуальной памяти, регионы виртуальной памяти и их атрибуты.
3. Корректные дампы памяти протекающих процессов. Дамп имеет стартовый и конечный адреса, а также имеет различную форму представления (двоичную, шестнадцатеричную, ASCII-вид и т.п.).
4. Дизассемблированный листинг дампа памяти. Эта форма представления дампа в виде ассемблерных команд. Корректный переход от двоичного вида к дизассемблированному коду является нетривиальной задачей, и содержит ряд трудноразрешимых проблем.
5. Управляющий граф процесса. Он содержит различные уровни детализации, которые зависят от сложности самого исследуемого процесса и от применяемых функций свертки в процессе дизассемблирования и формализации листинга.

Перечисленные пять компонентов являются важнейшими составляющими исходных данных. От их корректной формы зависит правильность дальнейшего эталонирования процессов антивирусного продукта Dr.Web 4.44.

Формализация исходных данных. Этот этап технологии необходим для вычисления последовательности состояний и эквивалентных преобразований кода программы (управляющего графа), а также для моделирования функциональной структуры. Для осуществления этих действий требуется представить исходные данные в виде *автомата, продукции и грамматики.* Автомат позволит построить последовательность состояний (лексический разбор дампа), продукция поможет осуществить синтаксический разбор и эквивалентные преобразования (свертку графа) [8], а грамматика создаст функциональную модель структуры процесса (семантический разбор) [2]. Эквивалентные преобразования производятся только в

случае возникновения необходимости упростить код или уменьшить его объем, так как они могут в последующем привести к искажению функциональной структуры процесса [8]. Кроме того, продукционная модель дает возможность проверить корректность и завершаемость кода, но в целях решения поставленной задачи это не является необходимостью.

Пример формирования автомата на процессе spidernt.exe показан на рисунке 8.

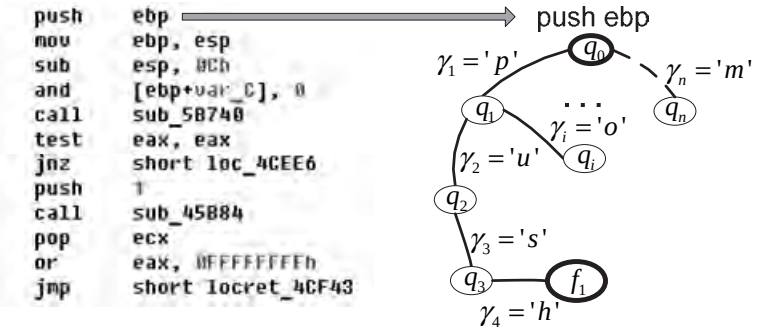


Рис. 8. Построение автомата переходов на графе состояний

На рисунке 8 представлены следующие обозначения:

q_0 – начальное состояние автомата;

$Q = \{q_1, q_2, ...q_n, ...q_i, ...q_{finish}\}$ – конечное множество состояний автомата;

$\Sigma = \{\gamma_1, \gamma_2, ...\gamma_n, ...\gamma_i, ...\gamma_{finish}\}$ – допустимый входной алфавит;

$\delta : Q \times \Sigma \to P(Q)$ – заданное отображение множества;

$F = \{f_1, f_2, ... f_n, ... f_i, ... f_{finish}\}$ - множество заключительных состояний.

Результатом работы автомата будет набор последовательных лексем, которые представляют собой конечные состояния автомата. Дальнейшие исследования потребуют объединение полученных лексем в более крупные синтаксические объединения – блоки. Для этого требуется построить продукционную систему вывода.

Результат работы с использованием продукционной формы представления процесса spidernt.exe показан на рисунке 9.

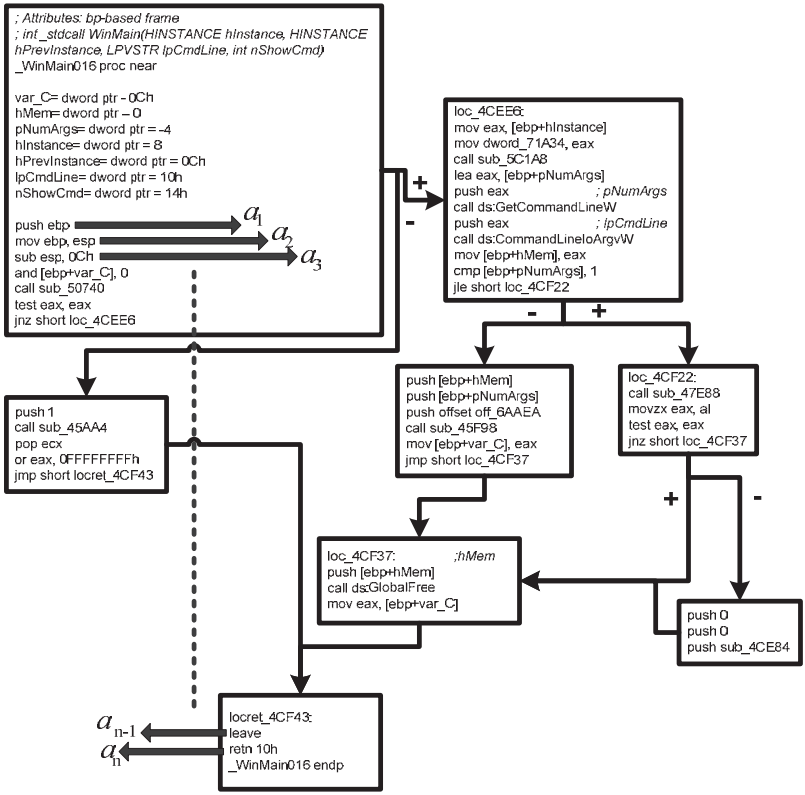


Рис. 9. Продукционная форма представления процесса spidernt.exe

На рисунке представлены следующие обозначения:

$A = \{a_1, a_2, ...a_n\}$ – множество входных символов (лексем) – алфавит;

F – множество формул в алфавите;

$F \subset A^* = a_1 \to a_2 \to a_3 \to ... \to a_n$

B – множество аксиом в алфавите;

$B \subset F$

R – множество правил вывода;

$R \subset F^{n+1}$

Аксиомы позволяют проверить корректность и завершаемость исследуемого кода (в данном случае это не требуется). Правила вывода помогают свернуть код (осуществить эквивалентные преобразования) в случае необходимости.

Третьим результатом процесса формализации исходных данных является модель функциональной структуры, основанная на грамматиках. Этот фрагмент отображает часть структуры, которая начинается с точки запуска процесса spidernt.exe – «StartPoint», и включает в себя все подпрограммы (функции), выполняющиеся с момента запуска.

Итогом процесса формализации являются три модели представления процесса вычислений, которые используются в дальнейшем.

Расчет метрик процесса spidernt.exe. На основе формального представления исходных данных производится расчет метрических показателей (структурных и информационных). Расчет временных метрик не осуществляется, так как он потребует создание дополнительного сложнейшего вычислительного стенда для оценки времени прохождения языковых конструкций процесса.

Для создания эталона требуется несколько временных срезов процессов антивирусного средства Dr.Web, то есть существуют несколько наборов входных данных разнесенных по времени. В качестве примера собрано 5 наборов исходных данных для процесса spidernt.exe.

Расчет полного набора метрических показателей требует существенных вычислительных и временных затрат, поэтому для осуществления эталонирования вычислительного процесса и последующего его контроля в некоторых случаях, когда требуется контролировать целостность процесса в режиме времени приближенном к реальному, допустимо использование меньшего количества метрических показателей. В качестве основных метрик, наиболее полно отражающих структуру вычислительного процесса, предлагается использовать:

1. Метрику точек пересечений. Механизм расчета этого показателя имеет следующий алгоритм:

a) из исходных данных считывается количество переходов условных и безусловных. Считывание производится в два массива (условный и безусловный), каждый переход характеризуется двумя значениями: стартовый и конечный адреса перехода (рисунок 10);

b) два массива сравниваются друг с другом поэлементно с целью поиска пересечений переходов по адресам. В результате находятся элементы и в том и в другом массиве, имеющие минимальное и максимальное количество пересечений. В «безусловном» массиве: $\min(a,b)=0$, $\max(c,d)=49$, где a,b – стартовый и конечный адреса безусловного перехода, имеющего минимально количество пересечений с другими переходами, c,d – стартовый и конечный адреса безусловного перехода, имеющего

максимальное количество пересечений с другими переходами. В «условном» массиве $\min(p,q)=0$, $\max(f,t)=9$, где p,q – стартовый и конечный адреса условного перехода, имеющего минимальное количество пересечений с другими переходами, f,t – стартовый и конечный адреса условного перехода, имеющего максимальное количество пересечений с другими переходами;

c) осуществляется расчет количественного показателя структурированности (метрики точек пересечения):

$$q_{15}=\frac{\max(c,d)}{\max(f,t)}=\frac{49}{9}=5,444 \qquad (7)$$

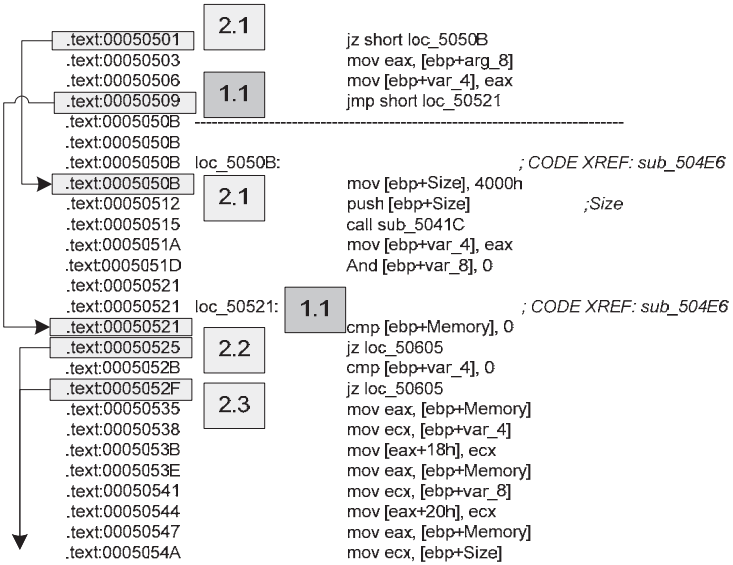


Рис. 10. Расчет метрики точек пересечения

2. Метрику Джилба. Она отражает насыщенность программы конструкциями циклов и переходов. Механизм расчета следующий:

a) считывается общее количество операторов цикла ($L_{loop}=567$), условия ($L_{jne}=26139$), безусловного перехода ($L_{jmp}=7147$). При считывании используются данные, полученные при расчете метрики точек пересечения, что сокращает время расчета;

b) производится подсчет количество модулей или подсистем (функций) $L_{sub}=607$ (рисунок 11);

c) вычисляется метрика Джилба:

$$q_{19} = \frac{N_{sv}}{L_{sub}} = \frac{33853}{607} = 55, \quad (8)$$

где $N_{sv} = L_{loop} + L_{jne} + L_{jmp} = 567 + 26139 + 7147 = 33853$

3. Метрику Вудворда. Она характеризует число узлов передачи управления и тесно связана с функциональным числом i-вершины. Представляет собой следующую тройку:

$$q_{17} = < F, U, P >, \quad (9)$$

где F - общее количество функциональных вершин всех узлов;
U - общее количество объединяющих вершин всех узлов;
P - общее количество предикатных вершин всех узлов.

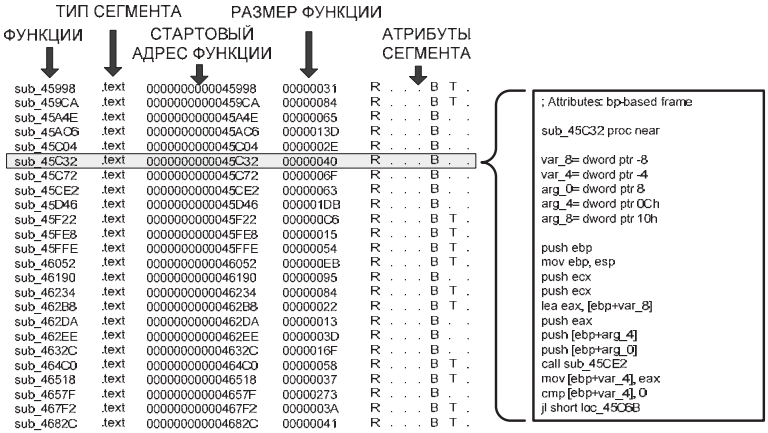


Рис. 11. Количество функций и их содержимое

Механизм расчета следующий:

a) процесс разбивается на узлы (функции) (рисунок 12). Количество узлов равно 607 ($i = \overline{1(1), 607}$);

b) в каждой функции подсчитывается количество функциональных вершин(f_i);

c) в каждой функции подсчитывается количество объединяющих вершин(u_i);

d) в каждой функции подсчитывается количество предикатных вершин(p_i);

e) рассчитывается полное количество функциональных

($F = \sum_{i=1}^{607} f_i = 25263$), объединяющих ($U = \sum_{i=1}^{607} u_i = 27103$) и предикатных вершин ($P = \sum_{i=1}^{607} p_i = 42658$);

f) в итоге получается метрика Вудворда:

$$q_{17} =< 25263, 27103, 42658 >$$

Сокращенный эталон, отражающий структуру вычислительного процесса, имеет следующий вид:

$$Etalon_{spidernt.exe} < q_{15}, q_{17}, q_{19} >$$
$$Etalon_{spidernt.exe} < 5,5(\pm 0,5); < 25400(\pm 900), \quad (10)$$
$$27300(\pm 700), 42500(\pm 600) >; 55,5(\pm 0,5) >$$

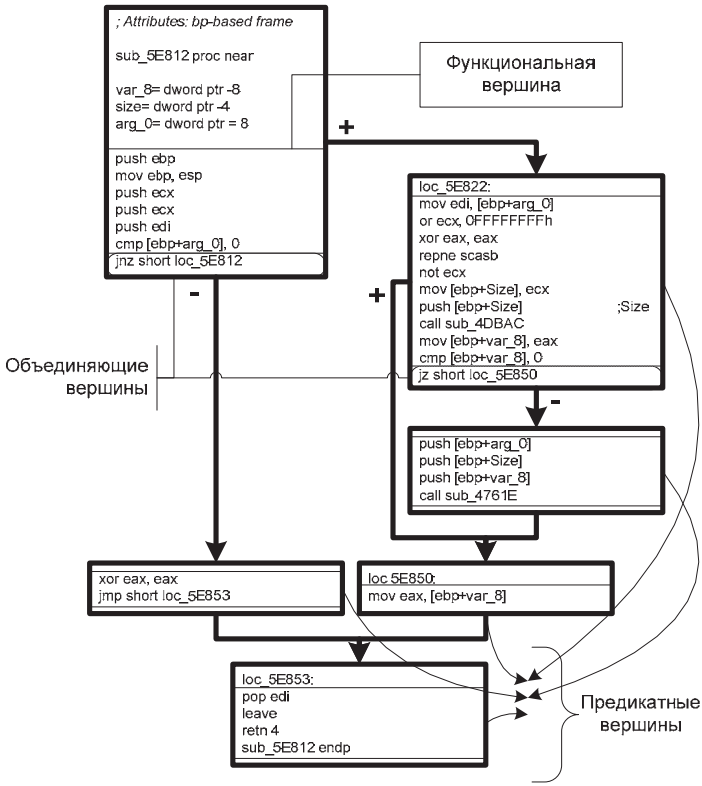


Рис. 12. Функциональные, объединяющие и предикатные вершины в узле

Все структурные метрики вычисляются разбором управляющего графа программы. Они отражены в таблице 1. В этой таблице приняты следующие обозначения: q_{11} – метрика Мак-Клура, q_{12} – метрика Пратта, q_{13} – метрика регулярных выражений, q_{14} – функциональная метрика, q_{15} – метрика точек пересечения, q_{16} – метрика Пивоварского, q_{17} – метрика Вудворда, q_{18} – метрика Чена, q_{19} – метрика Джилба.

Таблица 1. Структурные метрики процесса spidernt.exe

Метрика	Набор исходных данных				
	1	2	3	4	5
q_{11}	5	6	5	5	5
q_{12}	28	30	43	35	38
q_{13}	46 345	54 156	61 239	53 673	67 198
q_{14}	2,7	3,8	7,9	4,1	4,3
q_{15}	5,444	5,444	5,83	5,444	5,444
q_{16}	3,7	3,7	4,6	4,0	4,1
q_{17}	<25263, 27103, 42685>	<25145, 27512, 42698>	<25898, 27768, 43465>	<25345, 27128, 42491>	<25467, 27234, 42159>
q_{18}	1 892	1 543	2 567	1 897	1 954
q_{19}	55	55,9	56	55,3	55

Информационные метрики вычисляются путем синтаксического анализа дизассемблированного дампа памяти. Все информационные метрики, рассчитанные для 5 наборов исходных данных, показаны в таблице 2.

Таблица 2. Информационные метрики процесса spidernt.exe

Метрика	Набор исходных данных				
	1	2	3	4	5
q_{21}	0,32	0,45	0,42	0,7	0,52
q_{22}	5,73	7,67	8,9	5,9	6,23

В этой таблице приняты следующие обозначения: q_{21} – информационная энтропия, q_{22} – информационное содержание.

Полученные расчетные значения из пяти разных входных наборов данных позволяют построить эталонную метрическую модель процесса (spidernt.exe) антивирусного средства Dr.Web. Она состоит из

рассчитанных эталонных значений метрических показателей процесса, отражающих его структуру – структурные метрики (таблица 3), свойства – информационные метрики (таблица 4), а также доверительного интервала каждой метрики.

Полученный эталон позволяет контролировать целостность процесса функционирования spidernt.exe (одного из динамических компонентов антивирусного средства Dr.Web).

В качестве вредоносного воздействия на контролируемый динамический объект была осуществлена атака, связанная с изменением потока данных. Суть этой атаки заключалась в подмене потока сигнатур, считываемых из базы вирусных сигнатур. Это привело к снижению результативности обнаружения вирусов антивирусным средством Dr.Web. Системные мониторы, установленные в вычислительной системе, не зафиксировали искажений в действиях динамического объекта, следовательно, не смогли выявить деструктивное воздействие на этот объект. Предлагаемый распознаватель, позволил выявить существенные искажения в пространстве информационных метрик. Это отклонение является признаком нарушения целостности вычислительного процесса антивирусного средства.

Таблица 3. Структурный эталон процесса spidernt.exe

Метрика	Эталонное значение	Доверительный интервал
q_{11}	$5,2$	$\pm 1,2$
q_{12}	$34,8$	$\pm 16,25546$
q_{13}	$56522,2$	$\pm 21361,73381$
q_{14}	$4,56$	$\pm 5,27727$
q_{15}	$5,5212$	$\pm 0,4632$
q_{16}	$4,02$	$\pm 0,99318$
q_{17}	$< 25423,6;$ $27349;$ $42699,6 >$	$< \pm 778,29876;$ $\pm 764,51396;$ $\pm 1288,12552 >$
q_{18}	$1970,6$	$\pm 995,35389$
q_{19}	$55,44$	$\pm 1,29522$

Таблица 4. Информационный эталон процесса spidernt.exe

Метрика	Эталонное значение	Доверительный интервал
q_{21}	$0,482$	$\pm 0,37966$
q_{22}	$6,886$	$\pm 3,652$

Вредоносное воздействие, которое может осуществляться на вычислительный процесс путем добавления или уменьшения его функций, а также удаления или искажения данных, используемых в нем, моментально отражается в изменениях текущей метрической модели. Это позволяет выявить любое отклонение от эталона, и дает возможность утверждать о факте нарушения целостности функционирования этого процесса.

6. Заключение. Предлагаемый подход к контролю целостности вычислительных процессов с использованием метрического эталонирования, позволяет производить:

- расчёт метрических характеристик правильности структур, корректности свойств и устойчивости действий для эталонирования процесса вычислений;
- выбор ключевых параметров для первичного анализа процесса вычислений на основе построенных моделей представления процесса вычислений;
- распознавание признаков модификации процесса вычислений, на основании наличия которых выполняется классификация процесса вычислений к классам целостных и не целостных процессов, в том числе и с применением нечеткого классификатора;
- оценивать параметры контроля целостности с помощью корректирующих коэффициентов.

Этот подход в сочетании с другими средствами контроля целостности существенно повысит информационную безопасность АС, путем своевременного выявления преднамеренного или случайного искажения штатного состояния динамического объекта.

Литература

1. *Платонов А.А., Тимофеев В.И., Шаршаков В.Н., Ломако А.Г.* Модель угроз целостности вычислений в автоматизированных системах // Труды Института системного анализа Российской академии наук. 2013. №27. С. 321–337.
2. *Ахо А., Ульман Дж.* Теория синтаксического анализа, перевода и компиляции // М.: Мир. 1978. Т. 1. 614 с.
3. *Баранов С.Н., Тележкин А.М.* Метрическое обеспечение программных разработок // Труды СПИИРАН. 2014. №5(36). С. 5–27.
4. *Холстед М.Х.* Начала науки о программах // М.: Фин. и статистика. 1981. 128 с.
5. *Watson A.H., McCabe Th.J., Dolores R.* Structured Testing: a Testing Methodology Using the Cyclomatic Complexity Metric // National Institute of Standards and Technology Special Publication 500-235. 1996. 123 p.
6. *Neelamegam C., Punithavalli M.* Enhanced ensemble prediction algorithms for detecting faulty modules in object oriented systems using quality metrics // Journal of Computer Science. 2012. vol. 8. Issue 12. pp. 2075–2082.
7. *Карповский Е.Я., Чижов С.А.* Надежность программной продукции // Киев:

Техника. 1990. 171 с.
8. *Федорченко Л.Н.* Регуляризация контекстно-свободных грамматик на основе эквивалентных преобразований синтаксических граф-схем // Труды СПИИРАН. 2010. №4(15). С. 213–230.

References

1. Platonov A.A., Timofeev V.I., Sharshakov V.N., Lomako A.G. [Model of computation integrity threats in automated systems]. *Trudy Instituta sistemnogo analiza Rossijskoj akademii nauk – Proceedings of the Institute of systems analysis of Russian academy of sciences*. 2013. vol. 27. pp. 321–337. (In Russ.).
2. Aho A., Ulman Dzh. *Teoriya sintaksicheskogo analiza, perevoda i kompilyacii* [The theory of parsing, translation and compilation]. M.: Mir. 1978. vol .1. 614 p. (In Russ.)
3. Baranov S.N., Telezhkin A.M. [Metric for software development]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2014. vol. 5(36). pp. 5–27. (In Russ.).
4. Holsted M.H. *Nachala nauki o programmah* [Elements of Software Science]. M.: Finansy i statistika. 1981. 128 p. (In Russ.).
5. Watson A.H., McCabe Th.J., Dolores R. Structured Testing: a Testing Methodology Using the Cyclomatic Complexity Metric. National Institute of Standards and Technology Special Publication 500-235. 1996. 123 p.
6. Neelamegam C., Punithavalli M. Enhanced ensemble prediction algorithms for detecting faulty modules in object oriented systems using quality metrics. Journal of Computer Science. 2012. vol. 8. Issue 12. pp. 2075–2082.
7. Fedorchenko L.N. [Regularization of context free grammars on the base of equivalent transformations of syntax graph-schemes]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2010. vol. 4(15). pp. 213–230. (In Russ.).

Платонов Андрей Анатольевич — к-т техн. наук, старший преподаватель кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: технология программирования, формальные методы в разработке и анализе программного обеспечения. Число научных публикаций — 29. aplaton80@gmail.com; ул. Ждановская, д. 13, Санкт-Петербург, 197082; р.т.: 8-812-237-19-60.

Platonov Andrey Anatolievich — Ph.D., senior lecturer of systems for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: software engineering, the formal methods in development and the analysis of the software. The number of publications — 29. aplaton80@gmail.com; 13, Zhdanovskaya st., St. Petersburg, 197082, Russia; office phone: 8-812-237-19-60.

Тимофеев Владимир Ильич — преподаватель кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: организационно-правовое обеспечение защиты информации. Число научных публикаций — 11. tivlil@mail.ru; ул.Ждановская, д. 13, г.Санкт-Петербург, 197198; р.т.: +7-812-237-19-60.

Timofeev Vladimir Ilyich — lecturer of systems for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: organizational and legal protection of information. The number of publications — 11. tivlil@mail.ru; 13, Zhdanovskaya st., St. Petersburg, 197082, Russia; office phone: +7-812-237-19-60.

РЕФЕРАТ

Платонов А.А., Тимофеев В.И. **Контроль целостности динамических объектов вычислительных систем с использованием метрических эталонов.**

Рассмотренный в статье подход к контролю целостности динамических объектов развивает и дополняет методы контроля целостности информационных объектов в автоматизированных системах. Этот подход основывается на представлении вычислительного процесса в виде метрического эталона, включающего в себя метрики из полного базиса – правильности структуры, корректности свойств вычислимости и устойчивости действий. Каждая из составляющих этого базиса отражает наиболее значимые стороны вычислительного процесса, что позволяет отслеживать его искажения, вызванные преднамеренными или случайными внешними воздействиями.

Алгоритмы расчета метрик, составляющих эталон, приведены для динамических объектов антивирусного средства Dr.Web. Основной особенностью этих алгоритмов является, использование в качестве входных данных не исходных кодов программы, а дампа памяти, преобразованного к графу состояний. В алгоритме обработки дампа памяти используются приемы корректного дизассемблирования программ, а также методы эквивалентных преобразований на графах.

Процедура выявления изменений функциональных возможностей основана на решающем правиле и решающей функции, что позволяет отнести вычислительный процесс к классам целостных или не целостных динамических объектов автоматизированной системы. В случаях нечеткого распознавания используется мера близости и коэффициент строгости.

Результаты проведенного исследования позволяют сделать вывод об эффективности контроля динамических объектов с использованием метрических эталонов, но с большими затратами системных ресурсов. Эти затраты ориентируют использовать предлагаемый подход только для вычислительных процессов критически важных информационных объектов, например: средств защиты информации.

SUMMARY

Platonov A.A., Timofeev V.I. **Monitoring of Integrity of Dynamic Objects of Computing Systems with Use of Metric Standards.**

The approach to monitoring of integrity of dynamic objects considered in article develops and adds control methods of integrity of information objects in automated systems. This approach is based on representation of calculating process in the form of the metric standard including metrics from full base – correctness of structure, a correctness of properties of computability and stability of actions. Each of components of this base reflects the most significant sides of calculating process that allows to trace its distortions caused by premeditated or accidental external influences.

Algorithms of calculation of the metrics making a standard are given for dynamic objects of anti-virus means of Dr.Web. The main feature of these algorithms is, use as input data not of source codes of the program, but the memory dump transformed to a state graph. In algorithm of processing of a memory dump methods of incorrect disassembling of programs, and also methods of the equivalent conversions on graphs are used.

Procedure of detection of changes of the functional capabilities is based on the decisive rule and decision function that allows to refer calculating process to classes of integral or not integral dynamic objects of automated system. In cases of indistinct recognition the measure of closeness and coefficient of severity is used.

Results of the conducted research allow to draw a conclusion on efficiency of monitoring of dynamic objects with use of metric standards, but with big expenses of system resources. These expenses orient to use the offered approach only for calculating processes of crucial information objects, for example: information security features.

УДК 004.043

К.В. САЗОНОВ

ОЦЕНИВАНИЕ СЕМАНТИЧЕСКОГО СОДЕРЖАНИЯ СООБЩЕНИЙ НА ОСНОВЕ ПОТЕНЦИАЛЬНОЙ ИНФОРМАТИВНОСТИ

Сазонов К.В. **Оценивание семантического содержания сообщений на основе потенциальной информативности.**

Аннотация. В настоящей статье представлен анализ существующих подходов к оцениванию количества информации на различных уровнях ее представления. Введены и математически описаны понятия информационного потока и потенциальной информативности сообщения на синтактическом уровне представления. Сформулированы и доказаны теоремы, которые позволяют выполнить количественную оценку потенциальной информации. Предложен подход к оцениванию количества потенциальной информативности.

Ключевые слова: информация, неопределенность, прогнозирование, синтаксис, семантика, потенциальная информативность.

Sazonov K.V. **Evaluation of Semantic Content of Message based on Potential Informativeness.**

Abstract. This paper presents an analysis of the existing approaches to the estimation of the amount of information at different levels of its submission. The concepts of information flow and potential informative messages on the syntactic level of representation are described. Theorems that allow a quantitative estimation of the potential information are formulated and proved. An approach to the estimation of the number of potentially informative is proposed.

Keywords: information, uncertainty, forecasting, syntax, semantics, potential informativeness.

1. Введение. Одним из основных проблемных понятий в современной науке является понятие "информация". В настоящее время существует множество подходов к оцениванию количества информации:

– принцип неопределенности Гейзенберга [1];

– информация Фишера;

– информация и энтропия Шеннона [2].

В результате определить все подходы формально в универсальном смысле чрезвычайно сложно, что подчеркивает актуальность проблемы построения единой теории, призванной формализовать понятие информации и информационных процессов, а также описать превращения информации в процессах разной природы.

В теории передачи информации под формой представления информации подразумеваются сведения, являющиеся объектом некоторых операций, а именно: передачи, распределения, преобразования, хранения или непосредственного использования [2]. Особый интерес для систем обработки информации представляет процесс информационного взаимодействия, который состоит в передаче информации и

предполагает наличие источника (передатчика) S и ее получателя (интерпретанта) Pr.

Описание состояний источника S и получателя информации Pr осуществляется с помощью соответствующих им множеств параметров, мощности которых определяются числом возможных состояний, свойств и целей объектов информационного взаимодействия.

Процесс восприятия информации на уровне получателя связан с некоторым набором таких субъективных свойств информации, как важность, достоверность, своевременность, доступность, возможность ее измерения или количественного соотнесения и т.д. Свойства информации влияют на свойства сообщений и проявляются во взаимосвязях их элементов.

Под сообщением длиной m следует понимать совокупность $< s_j >_m$, $j = 0(1)m-1$ символов (знаков) источника (генеральной совокупности сообщений) S, определенных на множестве (алфавите) $S_{<N>}$, находящихся в определенных отношениях и связях друг с другом и образующих определенную целостность.

Таким образом, исходное сообщение в общем смысле есть форма представления информации в виде последовательности длиной m взаимосвязанных символов $s_j \in S_{<N>}$.

Анализируя количество, содержание и ценность информации в сообщениях, следует исходить из возможностей соответствующего анализа знаковых структур. Изучение связей между символами сообщения может быть реализовано путем измерения количества информации, содержащейся в сообщениях [3, 4].

При измерении количества информации ее свойства во внимание не принимаются. Кроме того, не вся информация имеет объективно измеряемое количество.

В результате многообразия и неоднозначности термина «информация» существует множество подходов к измерению количества информации. Однако, многообразие способов оценивания информации и неоднозначности субъективных оценок обуславливает необходимость разработки и внедрения новой концепции оценивания количества информации. При этом следует учитывать тот факт, что процесс информационного взаимодействия объектов с помощью телекоммуникационных систем предусматривает применение системы преобразований формы представления информации, отличающихся по сложности и структуре, а именно: кодирование источника, помехоустойчивое кодирование, модуляция и др., что обусловливает появление априорной неопределенности различных уровней относительно параметров этих преобразований.

2. Концептуальное описание понятия потенциальная информация. Обсуждения термина «информация» продолжаются до сих пор, однако часто носят не познавательный, а терминологический характер. Действительно, давно известно, что в реальном мире все материальное взаимодействует друг с другом (обменивается информацией), а проявлением этого взаимодействия является отражение, которое зачастую можно интерпретировать как сообщение, содержащее информацию об объекте. Отражение всякого материального объекта представляет собой некоторую упорядоченную вдоль оси времени структуру, которая характеризуется совокупностью связей между элементами, присутствующими в ней, распространяется в пространстве и изменяется во времени в том случае, когда объект является нестационарным.

Понятие «знаний» применимо не только к материальным, но и к идеальным объектам. В силу этого оно является более абстрактным, чем понятие информации, но понятие знаний представляется более конкретным, ориентирующим субъекта на совершение определенных действий. Понятие информации увязывается со знаниями конкретных предметов, их свойств, сторон и пр., что в философии называют предметом познания.

Предмет познания, по определению, является материальным, в силу чего информация действительно связана с отражением, которое проявляется как в физической, так и знаковой форме. Все знаковые и физические формы информации содержатся на каких-либо материальных предметах (носителях). Выявить смысл физической формы отражения без знаковой формы возможно, но описать без знаний нельзя. Указанное обстоятельство определяет более общий характер понятия знания по сравнению с понятием информации [5].

Таким образом, можно сформулировать такие важные понятия, как [6]:

– пространственный информационный поток – это конечное множество отражений материальных объектов, распространяющееся в пространстве, изменяющееся во времени и одновременно характеризующее его;

– сообщение информационного потока – это форма представления информации об окружающем пространстве, удобная для регистрирующей системы, выраженная в виде отражения материального объекта, содержащего данные о его структуре, свойствах и параметрах их изменения во времени;

– потенциальная информация как мера количественного описания воздействия сообщения информационного потока на рецепторы субъекта познания посредством отражений – количественная мера информации, которая содержится в сообщении информационного потока,

ограниченного на определенном временном интервале, и взаимосвязана с неопределенностью присутствующей в его структуре.

Опираясь на концептуальное понятие потенциальной информации можно сформулировать понятие потенциальной информативности сообщения.

Потенциальная информативность представляет собой среднее количество потенциальной информации, которая содержится в сообщении информационного потока, ограниченного на определенном временном интервале, и характеризует среднее значение неопределенности в связях между его элементами.

3. Концептуальное описание контента сообщения. Анализ и оценивание информации, содержащейся в различных типах сообщений семантических форматов (текстовых, звуковых, неподвижных и подвижных графических сообщениях), проводится на трех основных уровнях представления информации (рисунок 1), а именно: синтаксическом, семантическом и прагматическом [4].

Синтаксический уровень представления информации используется для описания комбинаторики символов (знаков) без учета значения и ценности, которую представляют эти символы и их сочетания как для субъекта или устройства, передающего информацию (передатчика), так и для потребителя информации (интерпретанта). Иными словами, на синтаксическом уровне описываются структурные свойства знаковых систем безотносительно к каким-либо их интерпретациям (составляющим предмет интересов семантики) и возможным интерпретаторам (рассматриваемым прагматикой).

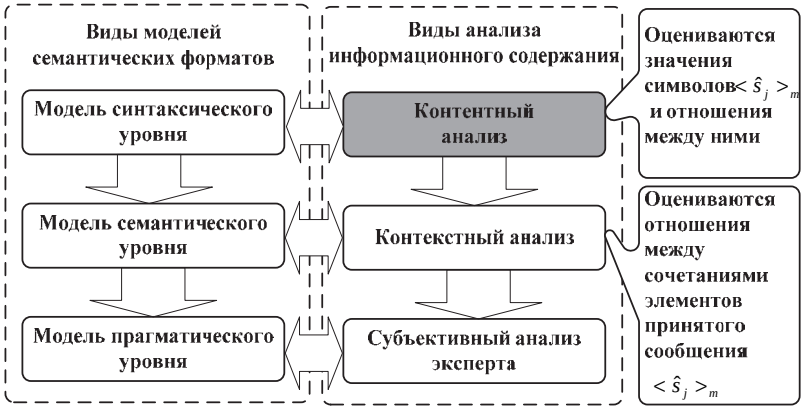


Рис. 1. Уровни представления информации

Исследование информационного содержания на синтаксическом уровне подразумевает оценивание значения символов $< s_j >_m$ и отношения между ними. Анализ такого типа позволяет выявить абсолютно любое информационно значимое либо содержательное наполнение сообщение, представленное в виде совокупности символов алфавита, а следовательно представляет собой ни что иное, как контентный анализ сообщения, а выявленное информационное содержание – контент сообщения. Таким образом, под содержанием сообщения подразумевается множество информационных символов, объединенных в единую структуру, с ярко выраженными особенностями в рамках одного сообщения (файла).

Исходя из выше сказанного, можно сделать вывод, что у сообщений с разным содержанием различная комбинаторика и различные отношения между символами, а следовательно можно предположить и различное количество информации на синтаксическом уровне, и данное количество информации может выступать в качестве информативного признака содержания сообщения.

Модель семантического уровня позволяет учитывать взаимосвязанность между символами с их содержанием (в терминах семиотики – между означающим и означаемым) без учета состояния как источника, так и приемника (интерпретанта) этих символов.

Предметом исследования и описания на этом уровне являются отношения между сочетаниями элементов принятого сообщения $S_{<m>}$ и понятиями, которые образуются в процессе обратной интерпретации сообщения $S_{<m>}$.

Анализ информационного содержания на семантическом уровне представления информации подразумевает оценивание отношений между сочетаниями элементов принятого сообщения. Представленный тип анализа позволяет оценить контекст сообщения (контекстный анализ) – относительно законченный по смыслу отрывок сообщения, в пределах которого наиболее точно и конкретно выявляется смысл и значение отдельного входящего символа или совокупности символов.

При исследовании и моделировании свойств сообщения на прагматическом уровне анализируется его смысловое содержание и отношение к источнику информации. При этом в качестве предмета анализа рассматриваются отношения между понятиями внутри некоторой системы или между понятиями, принадлежащими различным системам. Одна из таких систем образуется в процессе обратной интерпретации принятого сообщения $S_{<m>}$, вторая система отражает знания интерпретанта сообщения. В этом случае прагматика исследует

символы сообщения $S_{<m>}$ с точки зрения их ценности для интерпретанта, а иногда и для источника информации.

4. Математическая модель пространственного информационного потока. Пусть в некоторой области пространства присутствует множество процессов, доступных для наблюдения $\hat{S}^{*}_{<n>} \subseteq S_{<N>}$ и развивающихся во времени согласно законам теории вероятностей. Каждое сообщение $\hat{S}^{(i)}_{<m>} \in \hat{S}^{*}_{<n>}$ представляет собой набор данных:

$$\hat{S}^{*}_{<n>} = \{\hat{S}^{(i)}_{<m>}\}_n = \{<\hat{s}_j>^{(i)}_m\}_n = \{<\hat{s}_0, \hat{s}_1, ..., \hat{s}_j, ..., \hat{s}_{m-1}>^{(i)}\}_n, \; j = 0(1)m-1, \; i = 1(1)n, \quad (1)$$

где $i = 1(1)n$ – пространственная координата, определяющая положение сообщения в пространстве в фиксированный отсчет времени;

$j = 0(1)m-1$ – координата во временной области (последовательность дискретных отсчетов времени $t_j = j\Delta t$).

Данные (1) упорядочены вдоль оси аргумента – времени и пространственной координаты i, то есть представляют собой сообщение информационного потока, а множество $\hat{S}^{*}_{<n>}$ – непосредственно информационный поток.

Описанное множество сообщений имеет стохастическую природу и динамически изменяется с течением времени. Пусть $T = \{t_j \in T \mid t_0 \le t_j < t_0 + m\}$ – фрагмент оси времени, в пределах которого определяется наблюдаемый информационный поток $\hat{S}^{*}_{<n>}$. В этом случае каждое сообщение информационного потока может быть представлено как случайный процесс $\hat{S}^{(i)}_{<m>} \Leftrightarrow \hat{S}^{(i)}(t_j)$, а каждый элемент сообщения может быть описан в виде сечения случайного процесса в дискретные моменты времени как:

$$\hat{S}^{(i)}(t_j) = <\hat{s}^{(i)}_0, \hat{s}^{(i)}_1, ..., \hat{s}^{(i)}_{t_j}, ..., \hat{s}^{(i)}_{m\text{-}1}>, t_j \in T, \; j = 0(1)m-1, \; i = 1(1)n, \quad (2)$$

а в целом упорядоченная двумерная структура может быть представлена как множество временных рядов $\left\{\hat{S}^{(i)}(t_j)\right\}_n$, $j = 0(1)m-1$, $i = 1(1)n$.

Модель любого стохастического процесса может быть описана в следующем виде:

$$\hat{S}^{(i)}(t_j) = f^{(i)}(t_j) + \hat{a}^{(i)}(t_j), \; j = 0(1)m-1, \; i = 1(1)n, \quad (3)$$

где $\hat{a}^{(i)}(t_j)$ – случайная величина (шум, погрешность измерения), характеризуемая нормальным законом распределения с математическим ожиданием $M[\hat{a}]=0$ и дисперсией $D[\hat{a}]=const$;

$f^{(i)}(t_j)$ – функциональная зависимость, представляющая собой информационную составляющую сообщения;

$i=1(1)n$ – пространственная координата, определяющая пространственное положение стохастического процесса в фиксированный отсчет времени t_j, $j=0(1)m-1$.

Значения функций $f^{(i)}(t_j)$, $j=0(1)m-1$, $i=1(1)n$, соответствующие одному моменту времени и описывающие смежные векторы, могут быть связанны между собой в рамках плоскости, соответствующей сечению процесса во времени, и формируют единый образ, параметры которого изменяются во времени.

Таким образом, неопределенность, присутствующая в информационном потоке, может быть описана как множество функций времени $\{f^{(i)}(t_j)\}_n$, $j=0(1)m-1$, $i=1(1)n$, что эквивалентно множеству функций пространственных координат $\{f^{(i)}(j)\}_n$, $j=0(1)m-1$, $i=1(1)n$, в соответствии с описанием (1), где значения $i=1(1)n$ определяют положение вектора в плоскости сечения, а $j=0(1)m-1$ – положение символа в сообщении (векторе).

При этом множество всех функций времени $\{f^{(i)}(t_j)\}_n$, каждая из которых представляется в дискретные моменты времени t_j, образует собой информационный поток.

В свою очередь, информационный поток состоит из конечного множества элементов (символов алфавита) $\hat{s}_j^{(i)}$, $t_j \in T$, $j=0(1)m-1$, $i=1(1)n$. Наименьшим носителем неопределенности в структуре информационного потока являются значения двух соседних элементов, то есть элементом неопределенности предлагается считать пару смежных символов $\hat{s}_j^{(i)}$ и $\hat{s}_{j\pm1}^{(i\pm1)}$. В результате минимальный элемент неопределенности определяется как некоторая функция двух переменных $I(\hat{s}_j^{(i)}, \hat{s}_{j+1}^{(i+1)})$.

5. Математическое описание количественной меры потенциальной информации. В соответствии с основными постулатами

теории информации синтаксическую информацию сообщения можно выразить как неопределенность его структуры.

Впервые термин неопределенность был выдвинут Гейзенбергом, в соответствии с его принципом неопределенность пропорциональна произведению приращения импульса элементарной частицы Δp к приращению ее координаты Δx.

Применительно к информационному потоку $\left\{\hat{S}^{(i)}(t_j)\right\}_n$ неопределенность и информация, которая в нем содержится, пропорциональна функции $I(\hat{s}_j^{(i)}, \hat{s}_{j+1}^{(i+1)}) \sim h$, с той лишь разницей, что в качестве приращения импульса выступает приращение значения случайной величины $\Delta\hat{s}_{j+1}^{(i+1)}$, а в качестве приращения координаты Δx – приращение одной или нескольких координат $i \pm 1$ и $j \pm 1$ ($t_j \pm \Delta t$) пространственного информационного потока.

Каждая отдельно взятая реализация $s_j^{(i)}$ случайной величины $\hat{s}_j^{(i)}$ представляет собой численное значение, определяемое функцией $f^{(i)}(t_j)$. В соответствии с принципом неопределенности Гейзенберга в фиксированный момент времени можно наблюдать только одну реализацию $\hat{s}_j^{(i)}$, в результате чего возникает неопределенность значений $\hat{s}_{j+1}^{(i+1)}$, смещенных на один отсчет по координатам i или j:

$$h \sim \Delta x \Delta p \Rightarrow \Delta p \sim \Delta\hat{s}_{j+1}^{(i+1)}, \Delta x \sim \Delta t_j \Rightarrow h \sim \Delta\hat{s}_{j+1}^{(i+1)} \Delta t_{j+1} \sim I(\hat{s}_{j+1}^{(i+1)}, \hat{s}_j^{(i)}). \quad (4)$$

Указанную неопределенность можно устранить только в том случае, когда известна реализация случайной величины, характеризующей приращение $\Delta\hat{s}_{j+1}^{(i+1)}$ значения $\hat{s}_j^{(i)}$ по координатам i и j относительно $\hat{s}_{j+1}^{(i+1)}$, при условии, что значение $\hat{s}_{j+1}^{(i+1)}$ неизвестно.

Согласно теории Шеннона количество информации, содержащееся в сообщении, зависит от степени неопределенности этого сообщения, которая характеризуется вероятностью его появления. Количество информации тем больше, чем оно менее вероятно. В результате количество информации, содержащееся в одном символе сообщения $s_j^{(i)}$, целесообразно определить как функцию вероятности появления этого символа $P(s_j^{(i)})$.

Понятие неопределенности неотъемлемо связано с понятием субъекта, воспринимающего информационный поток, ибо с точки зрения различных субъектов в одном и том же потоке может присутствовать различное количество информации (неопределенности).

Оценивание контента сообщения информационного потока становится возможным только после восприятия данного сообщения некоторой регистрирующей системой.

Неопределенность, присутствующая в структуре информационного потока, не позволяет субъекту, воспринимающему данные, безошибочно предсказывать значение последующего элемента. Таким образом, процедуру восприятия сообщения субъектом можно описать в виде следующей структурной схемы (рисунок 2).

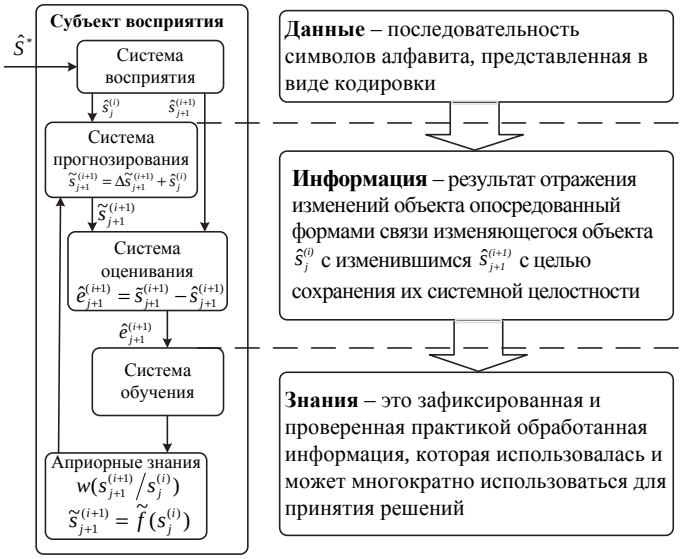


Рис. 2. Модель, поясняющая процесс восприятия сообщения субъектом

Пусть информационный поток $\left\{\hat{S}^{(i)}(t_j)\right\}_n$, $j = 0(1)m-1$, $i = 1(1)n$ доступен для наблюдения на интервале времени T ($t_j \in T$). Тогда субъекту в момент времени t_j становится доступно значение элемента $s_j^{(i)}$, принадлежащего сообщению $\hat{S}^{(i)}(t_j)$. На основе множества априорных данных о вероятностных характеристиках случайной величины $\hat{s}_{j+1}^{(i+1)}$, которые могут быть описаны в виде условного закона распреде-

ления $w(s_{j+1}^{(i+1)} / s_j^{(i)})$, либо на основе сформированного представления о функциональной зависимости $\tilde{s}_{j+1}^{(i+1)} = \tilde{f}(s_j^{(i)}) = \tilde{f}^{(i)}(t_j)$, субъект может осуществлять оценивание значения последующего элемента информационного потока.

Исходя из выше сказанного, в результате оценивания $s_j^{(i)}$ субъект прогнозирует наиболее вероятное, с его точки зрения, изменение элемента $s_j^{(i)}$, то есть $\Delta\tilde{s}_{j+1}^{(i+1)} = \tilde{s}_{j+1}^{(i+1)} - s_j^{(i)}$, в результате этого могут возникнуть следующие ситуации:

– для каждого элемента информационного потока $s_j^{(i)}$ соответствующее значение оценки $\Delta\tilde{s}_{j+1}^{(i+1)}$ совпадает с действительным значением $\Delta s_{j+1}^{(i+1)}$, в этом случае путем измерения любого $s_j^{(i)}$ можно вычислить значения всех элементов информационного потока. В таких условиях неопределенность в информационном потоке полностью отсутствует, в силу чего отсутствует и получаемая информация;

– субъект прогнозирует отличающееся значение элемента $\tilde{s}_{j+1}^{(i+1)} \neq s_{j+1}^{(i+1)}$, тогда после наблюдения реализации $\hat{s}_{j+1}^{(i+1)}$ определяется ошибка прогнозирования $\hat{e}_{j+1}^{(i+1)}$. Величина ошибки пропорциональна неопределенности значения элемента информационного потока $\hat{s}_{j+1}^{(i+1)}$ относительно значения элемента $\hat{s}_j^{(i)}$ и зависит от полноты описания условного закона распределения случайных величин $w(s_{j+1}^{(i+1)}/s_j^{(i)})$ для данного субъекта, либо от точности описания функциональной зависимости $\tilde{s}_{j+1}^{(i+1)} = \tilde{f}(s_j^{(i)})$. В том случае, когда между случайными величинами $\hat{s}_{j+1}^{(i+1)}$ и $\hat{s}_j^{(i)}$ прослеживается тесная взаимосвязь, у субъекта формируется более полное описание данной зависимости, что соответствует меньшим значениям ошибок прогнозирования $\hat{e}_{j+1}^{(i+1)}$;

– если априорные данные у субъекта относительно значения $\hat{s}_{j+1}^{(i+1)}$ полностью отсутствуют (совместное распределение $w(s_{j+1}^{(i+1)}/s_j^{(i)})$ и функция $\tilde{s}_{j+1}^{(i+1)} = \tilde{f}(s_j^{(i)})$ неизвестны, что соответствует полной неопределенности относительно структуры информационного потока) и реализация случайной величины $\hat{s}_j^{(i)}$ наблюдалась только один раз, то

в качестве наиболее ожидаемого значения предсказывается $\tilde{s}_{j+1}^{(i+1)} = s_j^{(i)}$, в силу чего значение $\Delta\tilde{s}_{j+1}^{(i+1)} = 0$, в этом случае возможны две ситуации:

а) все элементы сообщения действительно равны друг другу $s_{j+1}^{(i+1)} = s_j^{(i)} \Rightarrow \Delta s_{j+1}^{(i+1)} = 0$, прогноз окажется верным, и ошибки предсказания в этом случае отсутствуют, в силу чего информация так же отсутствует;

в) элементы информационного потока изменяются $s_{j+1}^{(i+1)} \neq s_j^{(i)} \Rightarrow \Delta s_{j+1}^{(i+1)} \neq 0$, ошибки предсказания принимают максимальные значения, что соответствует максимальной информативности потока.

После того, как субъектом определено значение $e_{j+1}^{(i+1)}$, он дополняет априорные данные об информационном потоке и тем самым корректирует совместное распределение случайных величин $w(s_{j+1}^{(i+1)}/s_j^{(i)})$ и параметры функциональной зависимости $\tilde{s}_{j+1}^{(i+1)} = \tilde{f}(s_j^{(i)})$ соседних элементов информационного потока (шаг оценивания). В результате после повторного наблюдения значение ошибки при оценивании $\Delta\tilde{s}_{j+1}^{(i+1)}$ становится меньше, в силу чего количество неопределенности в связях смежных случайных величин уменьшается.

В результате определенного числа L наблюдений субъект может полностью скорректировать свои априорные данные о связанности элементов информационного потока, в результате чего значения оценок будут соответствовать результатам наблюдений $\Delta\tilde{s}_{j+1}^{(i+1)} = \Delta s_{j+1}^{(i+1)}$, неопределенность в таком потоке устраняется.

Изложенный принцип составляет основу функционирования всех существующих систем распознавания. Число повторных наблюдений L интерпретируется как объем эталонных описаний, от которых зависит вероятность правильного распознавания.

Можно сделать вывод о том, что информативность потока принимает максимальные значения в том случае, когда поток воспринимается субъектом впервые. Воспринимая информационный поток как ранее не оцениваемый субъектом (распределение $w(s_{j+1}^{(i+1)}/s_j^{(i)})$ и $\tilde{s}_{j+1}^{(i+1)} = \tilde{f}(s_j^{(i)})$ неизвестны), можно определить количество информации, независимое от субъекта восприятия, то есть объективное количество информации – потенциальную (объективную) информативность.

Субъект оценивает информационный поток, полагаясь на свой априорные знания о данном информационном потоке и ошибку предсказания, на основании которой корректирует свою систему прогнозирования (посредством приобретения новых знаний), то есть обучается. В результате, посредством данной схемы возможно связать три основных понятия теории информации (рисунок 2).

Данные – последовательность символов алфавита, представленная в виде кодировки.

Информация – результат отражения изменений объекта опосредованный формами связи изменяющегося объекта $\hat{s}_{\mathrm{j}}^{(\mathrm{i})}$ с изменившимся $\hat{s}_{\mathrm{j+1}}^{(\mathrm{i+1})}$ с целью сохранения их системной целостности.

Знание – это зафиксированная и проверенная практикой обработанная информация, которая использовалась и может многократно использоваться для принятия решений.

Посредством получения из данных информации субъект пополняет свои знания.

6. Ошибка прогнозирования как количественная характеристика потенциальной информации. Взаимную связь двух смежных элементов информационного потока можно описать в виде некоторой функциональной зависимости двух случайных величин. Известный элемент в этом случае представляет собой объясняющую переменную $\hat{s}_{\mathrm{j}}^{(i)}$, а прогнозируемый – зависимую $\hat{s}_{\mathrm{j+1}}^{(\mathrm{i+1})}$. Такая односторонняя стохастическая зависимость называется простой регрессией (зависимость результата только от одной объясняющей переменной) $\tilde{s}_{\mathrm{j+1}}^{(\mathrm{i+1})} = f(s_{\mathrm{j}}^{(\mathrm{i})})$. Значение регрессии определяет оценку наиболее вероятного значения зависимой случайной величины $\hat{s}_{\mathrm{j+1}}^{(\mathrm{i+1})}$ при заданном значении реализации $s_j^{(i)}$ случайной величины $\hat{s}_j^{(i)}$. Разброс значений случайной величины $\hat{s}_{\mathrm{j+1}}^{(\mathrm{i+1})}$ вокруг $\tilde{s}_{\mathrm{j+1}}^{(\mathrm{i+1})}$ обусловлен влиянием неопределенности (энтропии), присутствующей в информационном потоке. Разность между эмпирическими значениями $s_{\mathrm{j+1}}^{(\mathrm{i+1})}$ и расчетным значением $\tilde{s}_{\mathrm{j+1}}^{(\mathrm{i+1})}$ позволяет получить количественную оценку неопределенности как ошибки предсказания:

$$\tilde{s}_{\mathrm{j+1}}^{(\mathrm{i+1})} - \hat{s}_{\mathrm{j+1}}^{(\mathrm{i+1})} = \hat{e}_{\mathrm{j+1}}^{(\mathrm{i+1})}. \qquad (5)$$

При отсутствии неопределенности в информационном потоке расчетные значения равны эмпирическим $\tilde{s}_{j+1}^{(i+1)} = s_{j+1}^{(i+1)}$, в силу чего между значениями $\hat{s}_j^{(i)}$ и $\hat{s}_{j+1}^{(i+1)}$ существует жесткая функциональная зависимость, неподверженная влиянию случайных факторов (зависимость полностью детерминирована). В том случае, когда какие-либо взаимные связи между случайными величинами $\hat{s}_j^{(i)}$ и $\hat{s}_{j+1}^{(i+1)}$ отсутствуют, определить их функциональную зависимость $\tilde{s}_{j+1}^{(i+1)} = f(s_j^{(i)})$ не представляется возможным, и разница между расчетным значением $\tilde{s}_{j+1}^{(i+1)}$ и эмпирическим максимальна. В этом случае и прогнозы и ошибки не зависят от субъекта, воспринимающего поток, в результате неопределенность при восприятии в таких условиях объективна и принимает значения, непосредственно зависящие только от структуры сообщения. Таким образом, в случае отсутствия знаний у оценивающего субъекта неопределенность в структуре потока максимальна и принимает значение, объективно характеризующее отношение между элементами информационного потока, а следовательно и синтаксическое содержание сообщения, то есть является информативным признаком содержания сообщения.

В целях обоснования потенциальной неопределенности в качестве информативного признака требуется описать количественную меру неопределенности, заключенной в смежных элементах потока.

Теорема 1. Пусть случайные величины $\hat{s}_{t_j}^{(i)}$ и $\hat{s}_{j+1}^{(i+1)}$ являются соседними элементами одного информационного потока. Тогда количественно величину, характеризующую их неопределенность, можно представить как меру разброса значений элементов потока вокруг некоторой функциональной зависимости их значений – регрессией.

Доказательство. В теории математической статистики разброс наблюдаемых значений случайной величины $\hat{s}_{j+1}^{(i+1)}$ около ее математического ожидания $M[\hat{s}_{j+1}^{(i+1)}]$ характеризуется оценкой дисперсии вида:

$$\tilde{D}[\hat{s}_{j+1}^{(i+1)}] = \frac{\sum_{\gamma=1}^{N} (s_{j+1,\gamma}^{(i+1)} - \tilde{M}[\hat{s}_{j+1}^{(i+1)}])^2}{N-1}. \qquad (6)$$

Оценка дисперсии (6) является общей, и ее значение обусловлено изменениями объясняющих переменных, в силу чего можно выпол-

нить разложение дисперсии. Отклонение γ-го результата наблюдения от общего среднего можно представить в следующем виде:

$$s_{j+1,\gamma}^{(i+1)} - \tilde{M}[\hat{s}_{j+1}^{(i+1)}] = (s_{j+1,\gamma}^{(i+1)} - \tilde{s}_{j+1,\gamma}^{(i+1)}) + (\tilde{s}_{j+1,\gamma}^{(i+1)} - \tilde{M}[\hat{s}_{j+1}^{(i+1)}]). \quad (7)$$

После возведения в квадрат обеих частей соотношения (7) и суммирования по γ имеет место следующее равенство:

$$\sum_{\gamma=1}^{N}(s_{j+1,\gamma}^{(i+1)} - \tilde{M}[\hat{s}_{j+1}^{(i+1)})^2 = \sum_{\gamma=1}^{N}(s_{j+1,\gamma}^{(i+1)} - \tilde{s}_{j+1,\gamma}^{(i+1)})^2 + \\ +2\sum_{\gamma=1}^{N}(s_{j+1,\gamma}^{(i+1)} - \tilde{s}_{j+1,\gamma}^{(i+1)})(\tilde{s}_{j+1,\gamma}^{(i+1)} - \tilde{M}[\hat{s}_{j+1}^{(i+1)}]) + \sum_{\gamma=1}^{N}(\tilde{s}_{j+1,\gamma}^{(i+1)} - \tilde{M}[\hat{s}_{j+1}^{(i+1)}])^2. \quad (8)$$

С учетом выражения (6) и $\sum_{\gamma=1}^{N}\tilde{s}_{j+1,\gamma}^{(i+1)}\hat{e}_{j+1,\gamma}^{(i+1)} = 0$ выражение (8) принимает вид:

$$\sum_{\gamma=1}^{N}(s_{j+1,\gamma}^{(i+1)} - \tilde{M}[\hat{s}_{j+1}^{(i+1)}])^2 = \sum_{\gamma=1}^{N}(s_{j+1,\gamma}^{(i+1)} - \tilde{s}_{j+1,\gamma}^{(i+1)})^2 + \sum_{\gamma=1}^{N}(\tilde{s}_{j+1,\gamma}^{(i+1)} - \tilde{M}[\hat{s}_{j+1}^{(i+1)}])^2. \quad (9)$$

Разделив соотношение (9) на $N-1$, получим:

$$\frac{\sum_{\gamma=1}^{N}(s_{j+1,\gamma}^{(i+1)} - \tilde{M}[\hat{s}_{j+1}^{(i+1)}])^2}{N-1} = \frac{\sum_{\gamma=1}^{N}(s_{j+1,\gamma}^{(i+1)} - \tilde{s}_{j+1,\gamma}^{(i+1)})^2}{N-1} + \frac{\sum_{\gamma=1}^{N}(\tilde{s}_{j+1,\gamma}^{(i+1)} - \tilde{M}[\hat{s}_{j+1}^{(i+1)}])^2}{N-1} = \\ = \frac{\sum_{\gamma=1}^{N}(e_{j+1,\gamma}^{(i+1)})^2}{N-1} + \frac{\sum_{\gamma=1}^{N}(\tilde{s}_{j+1,\gamma}^{(i+1)} - \tilde{M}[\hat{s}_{j+1}^{(i+1)}])^2}{N-1}. \quad (10)$$

Выражение (10) представляет собой разложение оценки общей дисперсии на две составляющие:

$$\tilde{D}[\hat{s}_{j+1}^{(i+1)}] = \tilde{D}[\hat{e}_{j+1}^{(i+1)}] + \tilde{D}[\hat{\tilde{s}}_{j+1}^{(i+1)}], \quad (11)$$

где $\tilde{D}[\hat{\tilde{s}}_{j+1}^{(i+1)}]$ – оценка дисперсии значений регрессии, представляющая собой ту часть общей дисперсии $\tilde{D}[\hat{s}_{j+1}^{(i+1)}]$, которая обусловлена влиянием случайной величины $\hat{s}_{j+1}^{(i+1)}$ («объясненная» дисперсия, или дисперсия, обусловленная регрессией); $\tilde{D}[\hat{e}_{j+1}^{(i+1)}]$ – оценка дисперсии зна-

чений ошибки прогнозирования, представляющая собой ту часть общей дисперсии $\tilde{D}[\hat{s}_{j+1}^{(i+1)}]$, которая не объясняется функцией регрессии («случайная», или остаточная дисперсия) и отражает независимость $\hat{s}_{j+1}^{(i+1)}$ от значения $\hat{s}_j^{(i)}$.

Из выражения (11) следует, что чем ближе оценка $\tilde{D}[\hat{e}_{j+1}^{(i+1)}]$ приближается к нулю, тем меньше эмпирические значения случайной величины $\hat{s}_{j+1}^{(i+1)}$ отклоняются от значения регрессии $\tilde{s}_{j+1}^{(i+1)}$. Иными словами, чем больше оценка дисперсии $\tilde{D}[\hat{s}_{j+1}^{(i+1)}]$ по сравнению с $\tilde{D}[\hat{e}_{j+1}^{(i+1)}]$, тем больше общая дисперсия формируется за счет объясняющей величины $\hat{s}_j^{(i)}$, в силу чего связь между значениями $\hat{s}_{j+1}^{(i+1)}$ и $\hat{s}_j^{(i)}$ более интенсивная.

Теорема доказана. ▲

Показателем интенсивности связи двух случайных величин является коэффициент детерминации, который с учетом разложения (11) представляет собой величину:

$$B(\hat{s}_j^{(i)}, \hat{s}_{j+1}^{(i+1)}) = \frac{\tilde{D}[\tilde{s}_{j+1}^{(i+1)}]}{\tilde{D}[\hat{s}_{j+1}^{(i+1)}]} = 1 - \frac{\tilde{D}[\hat{e}_{j+1}^{(i+1)}]}{\tilde{D}[\hat{s}_{j+1}^{(i+1)}]},\ j = 0(1)m-1,\ i = 1(1)n. \qquad (12)$$

В том случае, когда коэффициент детерминации $B(\hat{s}_j^{(i)}, \hat{s}_{j+1}^{(i+1)}) = 1$, все эмпирические значения $\hat{s}_j^{(i)}$ лежат на регрессионной прямой ($\tilde{D}[\hat{e}_{j+1}^{(i+1)}] = 0$). В свою очередь, при $B(\hat{s}_j^{(i)}, \hat{s}_{j+1}^{(i+1)}) = 0$ линия регрессии параллельна оси абсцисс, а коэффициенты регрессии при этом равны нулю.

Из выражения (12) следует, что отношение $\frac{\tilde{D}[\hat{e}_{j+1}^{(i+1)}]}{\tilde{D}[\hat{s}_{j+1}^{(i+1)}]}$ представляет собой показатель неопределенности связей и может быть использовано в качестве коэффициента неопределенности:

$$H(\hat{s}_j^{(i)}, \hat{s}_{j+1}^{(i+1)}) = 1 - B(\hat{s}_j^{(i)}, \hat{s}_{j+1}^{(i+1)}) = \frac{\tilde{D}[\hat{e}_{j+1}^{(i+1)}]}{\tilde{D}[\hat{s}_{j+1}^{(i+1)}]},\ j = 0(1)m-1,\ i = 1(1)n. \qquad (13)$$

Из выражения (13) следует, что большей связанности элементов соответствует меньшая энтропия и меньшее количество информации, заключенной в них, в силу чего коэффициент неопределенности и ко-

личество информации, содержащейся в близлежащих элементах сообщения, должны быть пропорциональны, т.е.:

$$\forall \hat{s}_j \exists \{\hat{I}_j\}_m, \hat{I}_j = I_j(\hat{s}_j^{(i)}, \hat{s}_{j+1}^{(i+1)}) \sim H_j(\hat{s}_j^{(i)}, \hat{s}_{j+1}^{(i+1)}), j = 0(1)m-1, i = 1(1)n, \quad (14)$$

где $I_j(\hat{s}_j^{(i)}, \hat{s}_{j+1}^{(i+1)})$ – количество информации, содержащейся в значениях двух соседних элементов сообщения информационного потока;

m – число элементов в сообщении $\hat{S}^{(i)}(t_j)$.

Информационный поток можно представить как множество временных рядов $\left\{\hat{S}^{(i)}(t_j)\right\}_n$, $j = 0(1)m-1$, $i = 1(1)n$. Для прогнозирования последующего элемента временного ряда $\hat{S}^{(i)}(t_j)$ при известном значении $\hat{s}_j^{(i)}$ принято использовать два подхода:

– в первом случае прогнозирование последующего значения ряда по одному или нескольким предыдущим значениям осуществляется с помощью известной функциональной зависимости (регрессии) $\tilde{s}_{j+1}^{(i+1)} = f(s_j^{(i)})$, в этом случае оценка элемента ряда называется регрессионной средней;

– во втором случае (вид регрессии неизвестен) в качестве оценки принимается наиболее вероятное значение случайной величины $\hat{s}_j^{(i)}$, то есть оценка моды $\tilde{s}_{j+1}^{(i+1)} = \tilde{Mo}[\hat{s}_{j+1}^{(i+1)}]$, в этом случае оценка элемента ряда называется вариационной средней и обозначается как $\dot{\tilde{s}}_{j+1}^{(i+1)}$.

Таким образом, процессы прогнозирования, используемые в теории анализа временных рядов, эквивалентны процедуре оценивания субъектом значения случайной величины $\hat{s}_{j+1}^{(i+1)}$.

Проведенный анализ позволяет сделать вывод, что по аналогии с описанием количества информации в информатике, величина ошибки прогнозирования одной случайной величины относительно другой характеризует количество информации совместно с условным распределением этих случайных величин. При этом количество информации $I_j(\hat{s}_j^{(i)}, \hat{s}_{j+1}^{(i+1)})$, присутствующее в реализации случайной величины $\hat{s}_{j+1}^{(i+1)}$ относительно $\hat{s}_j^{(i)}$, можно выразить через ошибку прогнозирования. Вместе с тем, в соответствии с выражением (14) количество информации зависит от коэффициента неопределенности $H_j(\hat{s}_j^{(i)}, \hat{s}_{j+1}^{(i+1)})$, в силу

чего можно утверждать, что величина коэффициента неопределенности $H_j(\hat{s}_{\text{j}}^{(\text{i})}, \hat{s}_{\text{j+1}}^{(\text{i+1})})$ и реализации ошибки $e_{\text{j+1}}^{(\text{i+1})}$ функционально зависимы.

В целях отыскания количественных характеристик коэффициента неопределенности требуется описать функциональную зависимость коэффициента неопределенности и ошибки оценивания элемента информационного потока.

Теорема 2. Пусть существует величина $H_j(\hat{s}_{\text{t}_\text{j}}^{(\text{i})}, \hat{s}_{\text{j+1}}^{(\text{i+1})})$, представляющая собой показатель неопределенности связей двух элементов информационного потока $\hat{s}_{\text{j+1}}^{(\text{i+1})}$ и $\hat{s}_{\text{j}}^{(\text{i})}$. Тогда значение неопределенности пропорционально величине ошибки прогнозирования значения $\tilde{s}_{\text{j+1}}^{(\text{i+1})}$ при известном значении $\hat{s}_{\text{j}}^{(\text{i})}$:

$$H_j(\hat{s}_{\text{j}}^{(\text{i})}, \hat{s}_{\text{j+1}}^{(\text{i+1})}) \sim \left| \tilde{s}_{\text{j+1}}^{(\text{i+1})} \mid \hat{s}_{\text{j}}^{(\text{i})} - \hat{s}_{\text{j+1}}^{(\text{i+1})} \right| \sim e_{\text{j+1}}^{(\text{i+1})} \ , \tag{15}$$

где $\tilde{s}_{\text{j+1}}^{(\text{i+1})} \mid \hat{s}_{\text{j}}^{(\text{i})}$ – оценка случайной величины $\hat{s}_{\text{j+1}}^{(\text{i+1})}$ при условии, что известно значение реализации величины $\hat{s}_{\text{j}}^{(\text{i})}$.

Доказательство. Пусть имеет место несмещенная оценка дисперсии ошибки прогнозирования величины $\hat{e}_{\text{j+1}}^{(\text{i+1})}$, математическое ожидание которой известно и с учетом ее аналитического описания равно $M[\hat{e}_{\text{j+1}}^{(\text{i+1})}] = 0$. При этом указанная оценка дисперсии может быть представлена в виде:

$$\tilde{D}[\hat{e}_{\text{j+1}}^{(\text{i+1})}] = \frac{1}{N} \sum_{\gamma=1}^{N} (e_{\text{j+1},\gamma}^{(\text{i+1})} - M[\hat{e}_{\text{j+1}}^{(\text{i+1})}])^2 = \frac{1}{N} \sum_{\gamma=1}^{N} (e_{\text{j+1},\gamma}^{(\text{i+1})})^2 \ . \tag{16}$$

Тогда коэффициент неопределенности (13) с учетом выражения (16) можно записать следующим образом:

$$H_j(\hat{s}_j^{(i)}, \hat{s}_{j+1}^{(i+1)}) = \frac{\tilde{D}[\hat{e}_{j+1}^{(i+1)}]}{\tilde{D}[\hat{s}_{j+1}^{(i+1)}]} = \frac{\sum_{\gamma=1}^{N} (e_{j+1,\gamma}^{(i+1)})^2}{N \cdot \tilde{D}[\hat{s}_{j+1}^{(i+1)}]} = \frac{\overline{(e_{j+1}^{(i+1)})^2}}{\tilde{D}[\hat{s}_{j+1}^{(i+1)}]}, \tag{17}$$

где $e_{\text{j+1},\gamma}^{(\text{i+1})}$ – ошибка при прогнозировании γ-го элемента алфавита.

Отношение (17) позволяет выявить, какая часть общего рассеяния значений случайной величины $\hat{s}_{\text{j+1}}^{(\text{i+1})}$ обусловлена факторами, не

зависящими от значения случайной величины $\hat{s}_{\mathrm{j}}^{(\mathrm{i})}$. При этом чем большую долю в общей дисперсии составляет оценка $\tilde{D}[\hat{e}_{\mathrm{j+1}}^{(\mathrm{i+1})}]$, тем меньшее влияние оказывает значение случайной величины $\hat{s}_{\mathrm{j}}^{(\mathrm{i})}$, то есть связь между $\hat{s}_{\mathrm{j}}^{(\mathrm{i})}$ и $\hat{s}_{\mathrm{j+1}}^{(\mathrm{i+1})}$ менее интенсивная.

Из выражения (17) следует пропорциональность значений коэффициента неопределенности $H_j(\hat{s}_{\mathrm{t\,j}}^{(\mathrm{i})}, \hat{s}_{\mathrm{j+1}}^{(\mathrm{i+1})})$ элемента сообщения $\hat{s}_{\mathrm{j+1}}^{(\mathrm{i+1})}$ относительно $\hat{s}_{\mathrm{j}}^{(\mathrm{i})}$ и среднего значения квадрата ошибки прогнозирования $\overline{(e_{\mathrm{j+1}}^{(\mathrm{i+1})})^2}$ (начального момента 2-го порядка $\nu_2[\hat{e}_{\mathrm{j+1},\gamma}^{(\mathrm{i+1})}]$), причем, чем большее значение принимает коэффициент неопределенности, тем ближе среднее значение квадрата ошибки прогнозирования $\overline{(e_{\mathrm{j+1}}^{(\mathrm{i+1})})^2}$ к значению оценки дисперсии $\tilde{D}[\hat{s}_{\mathrm{j+1}}^{(\mathrm{i+1})}]$. Коэффициент пропорциональности в соответствии с выражением (17) представляет собой величину $1/\tilde{D}[\hat{s}_{\mathrm{j+1}}^{(\mathrm{i+1})}]$. В том случае, когда неопределенность максимальна, справедливо равенство $\overline{(e_{\mathrm{j+1}}^{(\mathrm{i+1})})^2} = \tilde{D}[\hat{s}_{\mathrm{j+1}}^{(\mathrm{i+1})}]$, что полностью соответствует процессу с нулевым математическим ожиданием («белый шум»), который в классической теории информации принято воспринимать как максимально информативное сообщение.

Теорема доказана. ▲

Основываясь на выводах, полученных в соответствии с теоремой 2, можно предложить альтернативный вариант вычисления среднего значения квадрата ошибки прогнозирования:

$$\overline{(e_{\mathrm{j+1}}^{(\mathrm{i+1})})^2} = H_{\mathrm{j}}^{(\mathrm{i})}(\hat{s}_{\mathrm{j+1}}^{(\mathrm{i+1})}, \hat{s}_{\mathrm{j}}^{(\mathrm{i})})\tilde{D}[\hat{s}_{\mathrm{j+1}}^{(\mathrm{i+1})}] \ . \qquad (18)$$

Подставляя в выражение (18) выражение для коэффициента детерминации (13) можно представить выражения для вычисления среднего значения квадрата ошибки оценивания смежных случайных величин по их реализациям:

$$\overline{(e_{j+1}^{(i+1)})^2} = \frac{1}{N(N-1)}\left(N\sum_{\gamma=1}^{N}(s_{j+1,\gamma}^{(i+1)})^2 - \left(\sum_{\gamma=1}^{N}s_{j+1,\gamma}^{(i+1)}\right)^2\right) - \frac{\left(N\sum_{\gamma=1}^{N}s_{j,\gamma}^{(i)}s_{j+1,\gamma}^{(i+1)} - \left(\sum_{\gamma=1}^{N}s_{j,\gamma}^{(i)}\right)\left(\sum_{\gamma=1}^{N}s_{j+1,\gamma}^{(i+1)}\right)\right)^2}{N(N-1)\left(N\sum_{\gamma=1}^{N}(s_{j,\gamma}^{(i)})^2 - \left(\sum_{\gamma=1}^{N}s_{j,\gamma}^{(i)}\right)^2\right)} \cdot \qquad (19)$$

Выражение (19) позволяет отойти от процедур прогнозирования элементов сообщения и использовать для вычисления квадрата среднего значения ошибки предсказания непосредственно значения элементов сообщения.

Таким образом, если для каждого элемента информационного потока $\hat{s}_{\mathrm{j}}^{(\mathrm{i})}$ определены все ошибки прогнозирования связанных с ним элементов $\hat{s}_{\mathrm{j+1}}^{(\mathrm{i+1})}$, то можно представить неопределенность всего потока в виде множества ошибок прогнозирования:

$$\left\{\sqrt{\overline{(e_{\mathrm{j+1}}^{(\mathrm{i+1})})^2}}\right\}_{\mathrm{mn}}, i = 1(1)n,\ j = 0(1)m-1. \qquad (20)$$

Вследствие чего значение потенциальной информативности, которая присутствует в информационном потоке, можно представить в следующем виде:

$$I = \sum_{i=1}^{n}\sum_{j=0}^{m-1}\sqrt{\overline{(e_{\mathrm{j+1}}^{(\mathrm{i+1})})^2}},\ i = 1(1)n,\ j = 0(1)m-1. \qquad (21)$$

7. Заключение. В итоге можно сделать вывод, что вся потенциальная информативность, которая содержится в потоке, может быть представлена в виде множества ошибок оценивания смежных случайных величин. Величина I зависит от интенсивности связей между элементами информационного потока и характеризует количество информации сообщения на семантическом уровне. Иными словами, выражение (21) представляет объективно существующую информацию сообщения, которая не зависит от субъекта при условии, что до восприятия первых элементов потока $\hat{s}_{t_1}^{(i)}$ любые априорные знания у субъекта отсутствовали.

Количество информации, определяемое выражением (21), соответствует концептуальному понятию потенциальной информации [7]. В результате можно сделать вывод, что величина I является количественной мерой потенциальной информации.

Полученные аналитические выражения, позволяют описать информативные признаки распознавания семантического содержания сообщений информационного потока, в целях обеспечения поиска как потенциально ценной информации, так и вредоносного контента.

Для практического использования аналитических моделей требуется сопоставление различных типов семантических сообщений соответствующим аналитическим моделям и информативным признакам.

Литература

1. *Гейзенберг В.* Избранные философские работы // С.-Пб.: Наука. 2006. 576 с.
2. *Левин В.И.* К.Э. Шеннон и современная наука // Вестник ТГТУ. 2008. Том 14. №3. С. 703–724.
3. *Астахов М.А., Ростовцев Ю.Г., Яфраков М.Ф.* Информационная борьба и знаковые системы // М.: Издательство «ТОМ». 2007. 334 с.
4. *Ростовцев Ю.Г.* Основы построения автоматизированных систем сбора и обработки информации // СПб.: ВИКИ. 1992. 216 с.
5. *Данилин С.Н.* О современном понятии информации // Информационные технологии. 2003. № 11. С. 53–57.
6. *Присяжнюк С.П., Сазонов К.В.* Потенциальная информативность как новая характеристика отражения материального объекта // Информация и космос. 2006. №2. С. 100–105.
7. *Сазонов К.В.* Модели оценивания потенциальной информативности потоков сообщений // Наукоемкие технологии. 2009. Т. 10. № 12. С. 63–69.

References

1. Gejzenberg V. *Izbrannye filosofskie raboty* [Selected philosophical works]. M.: Nauka, 2006. 576 p. (In Russ.)
2. Levin V.I. [C.E. Shannon and modern science]. *Vestnik TGTU – Bulletin of the TGTU*. 2008. vol. 14. no. 3. pp. 703–724 (In Russ.)
3. Astakhov M.A., Rostovtcev Y.G., Yafrakov M.F. *Informacionaia borba i znakovie sistemy* [Information warfare and sign systems]. M .: Publisher “TOM”. 2007. 334 p. (In Russ.)
4. Rostovtcev Y.G. *Osnovy postroeniya avtomatizirovannyh sistem sbora i obrabotki informacii* [Fundamentals of automated systems for the collection and processing of information]. SPb .: Vicki. 1992. 216 p. (In Russ.)
5. Danilin S.N. [On the current concept of information]. *Informacionnye tekhnologii – Information Technology*. 2003. vol. 11. pp. 53–57. (In Russ.)
6. Prysiazhnyuk S.P., Sazonov K.V. [Potential as a new informative reflection characteristics of the material object]. *Informaciya i kosmos – Information and Space*. 2006. vol. 2. pp. 100–105.
7. Sazonov K.V. [Models estimating potential information content of message flows]. *Naukoemkie tekhnologii – High Tech.* 2009. vol. 10. no. 12, pp. 63–69.

Сазонов Константин Викторович — д-р техн. наук, начальник кафедры инженерного анализа, Военно-космическая академия имени А. Ф. Можайского. Область научных интересов: системы сбора и обработки информации, обратное проектирование современных телекоммуникационных систем. Число научных публикаций — 65. Staffa78@mail.ru; ул. Ждановская д. 13, г. Санкт-Петербург, 199178, РФ; р.т.: (812) 230-28-15, Факс: (812)237-12-49.

Sazonov Konstantin Viktorovich — Ph.D., Dr. Sci., head of engineering analysis department, Mozhaisky Military Space Academy. Research interests: the system of data collection and processing, reverse engineering of modern telecommunication systems. The number of publications — 65. Staffa78@mail.ru; st. Zhdanovskaya d. 13, St. Petersburg, 199178, Russian Federation; office phone: (812) 230-28-15, Fax: (812)237-12-49.

РЕФЕРАТ

Сазонов К.В. **Оценивание семантического содержания сообщения на основе потенциальной информативности.**

Любое сообщение информационного потока может быть представлено в виде некоторой упорядоченной структуры элементов и связей между ними. В том случае, когда для определенной интеллектуальной системы, воспринимающей сообщение, структура и связи между элементами известны, для данной системы такое сообщение полностью детерминировано, и неопределенность в его структуре полностью отсутствует. Если предсказание элемента выполняется с ошибкой, система оценивает ее значение для адаптации и корректировки процедуры прогнозирования, в результате чего на следующем шаге ошибка прогнозирования снижается. Иными словами интеллектуальная система получает некоторый объем информации, которая содержится в смежных элементах, на основании этого происходит самообучение системы с целью минимизации ошибки следующих прогнозов.

При условии отсутствия у системы, воспринимающей сообщение, априорных данных о сообщении, процедура обучения выполняется впервые, и как следствие, образуются максимальные ошибки прогнозирования. Эффективное значение ошибок прогнозирования представляет собой объективную оценку количества информации, не зависящую от воспринимающей системы и получившую название потенциальной информации сообщения.

Содержание сообщения на семантическом уровне зависит от структурных особенностей сообщения, а также от плотности (скачков связанности) неопределенности в структуре сообщения. Таким образом, для различных классов контента величина потенциальной информации принимает различные значения, а эффективное значение ошибки прогнозирования предлагается использовать в качестве информативного признака распознавания семантического содержания сообщений.

SUMMARY

Sazonov K.V. **Evaluation of Semantic Content of Message based on Potential Informativeness.**

Any message of information flow can be represented in the form of an ordered structure of the elements and the relationships between them. In that case, when for a certain intelligent system that receives a message, the structure and relationships between elements are known to the system a message is completely determined, and uncertainty in its structure completely absent. If the prediction element fails, the system evaluates its importance for adapting and correcting the prediction procedure, whereby in the next step the prediction error decreases. An intelligent system receives a certain amount of information that is contained in the adjacent cell. Then the system is self-learned in order to minimize errors following forecasts.

In the absence of a system that receives the message, a priori data about the message the process of learning for the first time, and as a result, the maximum prediction error is formed. The effective value of prediction errors is an objective assessment of the amount of information that is independent of the receiving system and received the name of the potential of information messages.

The content of posts on the semantic level depends on the structural features of messages, and the density (jumps connectivity) uncertainty in the structure of the message. Thus, for various classes of potential information content value takes different values, and the effective value of the prediction error is proposed as an informative feature recognition semantic content of messages.

УДК 004.853

В.И. Городецкий, О.Н. Тушканова

АССОЦИАТИВНАЯ КЛАССИФИКАЦИЯ: АНАЛИТИЧЕСКИЙ ОБЗОР. ЧАСТЬ 1

Городецкий В.И., Тушканова О.Н. **Ассоциативная классификация: аналитический обзор. Часть 1.**

Аннотация. В работе описаны основные результаты, модели и методы, разработанные в области ассоциативной классификации, ориентированные на обработку данных большого объема. В работе дается постановка задачи ассоциативной классификации, вводится необходимая терминология и формальные обозначения, используемые в ассоциативной классификации. Приводится описание и сравнительный анализ ранних подходов, методов и конкретных алгоритмов ассоциативной классификации. Дается оценка вклада первых работ, посвящённых ассоциативной классификации, в развитие этого направления.

Ключевые слова: большие данные, ассоциативное правило, ассоциативная классификация.

Gorodetsky V., Tushkanova O. **Associative classification: analytical overview. Part 1.**

Abstract. The paper topic is associative classification intended for processing of big data. It formulates corresponding problem statement and introduces basic concepts and formal notation used in associative classification. An extended overview and comparative analysis of the early approaches, models and algorithms for associative classification form the main paper contents. The paper assesses the contribution of the first papers devoted to associative classification to the development of this area and formulates goals of the further research.

Keywords: associative classification, emerging pattern, big data.

1. Введение. Среди множества современных моделей анализа данных особое место занимают модели, связанные с решением наиболее представительного класса задач принятия решений, а именно задач классификации. История исследований моделей классификации насчитывает уже несколько десятилетий, однако их актуальность не снижается ввиду регулярного появления новых классов задач и конкретных приложений, специфических типов данных, описывающих объекты классификации, новых требований к качеству решения задач и т.п. Современные приложения во многом не похожи на те, для которых развивались классические модели, методы и алгоритмы решения задач классификации. Типичными примерами приложений нового типа являются задачи интеллектуального управления бизнесом (англ. *business intelligence*), анализ социальных сетей и принятие решений по тем или иным аспектам их функционирования, приложения в области прогнозирования спроса и персонификации предложений в интернет–торговле, в области продвижения веб-сайтов и многие другие. Изменился также и характер самих задач классификации. Например, важ-

нейшую роль приобретают задачи типа *Что, …, если?*, в которых нужно определять атрибуты, факторы, явления, процессы и т.п., которые связаны с наблюдаемыми на практике нежелательными отклонениями свойств тех или иных процессов от номинальных или от желаемых значений, чтобы затем управлять ими для изменения свойств процессов в нужном направлении. Эти и другие причины требуют разработки новых и новых моделей, методов и алгоритмов в области, которую принято называть интеллектуальным анализом данных, в частности, в области обучения классификации и синтеза классификаторов.

Специфика приложений, примеры которых приведены выше, проявляется, прежде всего, в особенностях данных, которые доступны в них для принятия решений. Новый класс задач подобного рода и новые непростые проблемы появились в последнее время в связи развитием концепции *больших данных*. Хотя понятие больших данных (англ. *Big Data*) было введено совсем недавно (2008 г.) [1], оно быстро вошло в обиход специалистов, и в настоящее время является общепринятым.

Естественно, что точного определения понятия больших данных не существует, и оно дается описательно. К большим данным относят не просто данные большого объема и/или высокой размерности. Большие данные обычно обладают сложной структурой. Как правило, они описываются разнородными атрибутами (числовыми, булевыми, ординальными, номинальными), содержат в себе тексты на естественном языке, изображения, а также данные некоторых специальных форматов. К ним относятся, например, веб–ссылки, адреса электронной почты, номера телефонов, адреса и имена организаций и людей, даты и т.п. Нередко такие данные имеют характер потоков во времени. Поэтому часто они представляются множеством транзакций и первично записываются в транзакционных базах данных. Такие данные могут иметь объемы, измеряемые терабайтами, петабайтами и более, и размерности, исчисляемые сотнями и тысячами атрибутов, каждый их которых, в свою очередь, может иметь сложную структуру или быть неструктурированным, например, может быть текстом на естественном языке. Как принято сейчас говорить, эти данные характеризуются "*тремя V*": *Volume*, *Velocity*, *Variety*, т.е. *объемом*, *скоростью* прироста и *разнообразием* шкал и структур представления [1, 2]. Типичными примерами больших данных являются распределенные потоки текстовых сообщений из социальных сетей, метеорологические, экологические и другие пространственно–временные данные исследований окружающей среды. Сюда же относятся потоки данных о соединениях абонентов сотовой связи и их местонахождениях, серверные данные

интернет–торговли, содержащие информацию о покупателях, товарах, динамике и структуре покупок, данные о финансовых потоках банков с офисами, распределенными глобально, потоки данных о дорожном движении в мегаполисах и т.п.

Появление таких данных потребовало не только новых методов и средств их хранения (NoSQL, Hadoop и др.), но также и создания специальных технологий их обработки и представления, в частности, визуализации. Отметим, что в литературе иногда к понятию *большие данные* относят не только сами данные с описанными выше свойствами, но также и все специфические методы, средства и технологии их хранения, обработки и представления результатов. Иначе говоря, этот термин иногда используется также и как название соответствующего научного направления.

В настоящее время для работы с большими данными, в частности, в интересах решения задач классификации, развиваются новые методы, модели и алгоритмы интеллектуальной обработки больших данных. Одним из таких новых направлений является *ассоциативная классификация*. Следует отметить, что хотя в большинстве исследований аспект, непосредственно связанный с особенностями ассоциативной классификации применительно к большим данным явно не обсуждается, тем не менее, все исследования в этой области акцентируют внимание на эффективной работе именно с данными большого объема и размерности.

В данной работе дается обзор алгоритмов, моделей и методов, разработанных в области ассоциативной классификации применительно к обработке данных большого объема на начальном этапе развития этого направления интеллектуального анализа данных. Задача ассоциативной классификации была впервые сформулирована в работе [3], так что данное направление активно развивается уже в течение более чем 15 лет. В разделе 2 дается постановка задачи ассоциативной классификации, вводится необходимая терминология и формальные обозначения, используемые в последующей части обзора. Раздел 3 представляет основное содержание данной работы. В нем приводится описание и сравнительный анализ первых результатов, полученных в области ассоциативного анализа. В заключении по работе дается оценка вклада работ, посвящённых ассоциативной классификации, в развитие этого направления на его начальном этапе, а также формулируются цели дальнейшего исследования.

2. Ассоциативная классификация: термины, обозначения и модели ассоциаций. В данном обзоре рассматриваются методы поиска ассоциативных правил, которые ориентированы на решение задач

классификации. При поиске ассоциативных правил конкретное приложение и задача, в которой далее предполагается использовать полученные правила, не конкретизируется. В отличие от этого, в ассоциативной классификации такая задача указывается явно, и потому в ней отыскиваются ассоциативные правила специального вида. Поэтому если задача поиска ассоциативных правил в общем случае относится к задачам поиска анализа связей в данных (англ. *data mining*), то задача поиска ассоциативных связей относится к области машинного обучения (англ. *machine lrarning*). В правой части этих правил может присутствовать только целевая переменная, а именно *метка класса*, что существенно сужает множество искомых правил и, следовательно, снижает сложность поиска. Такие правила принято называть *ассоциативными правилами класса* (*class associative rules, CARs*).

Задачи ассоциативной классификации обладают и рядом других особенностей, поэтому поиск классифицирующих ассоциативных правил имеет свою специфику. В отличие от классических постановок задач поиска ассоциативных правил, обучающие данные для синтеза ассоциативных классификаторов могут не являться транзакциями, что на практике может привести к значительному увеличению числа потенциальных правил. Например, обучающие данные могут быть гетерогенными, иметь сложную структуру и даже являться текстами. Это усложняет задачу предобработки данных, используемых для обучения. Существуют и другие особенности задач ассоциативной классификации, которые требуют введения некоторых специальных понятий, используемых авторами работ по данной тематике.

Рассмотрим формальную постановку задачи ассоциативной классификации, введем некоторые базовые термины и формализмы, используемые в существующей литературе по данной проблематике, в частности, авторами работ, анализируемых далее.

Пусть $\boldsymbol{D}$ – транзакционная база данных (множество данных), $D_i \in \boldsymbol{D}$ – произвольная транзакция, $\boldsymbol{X}$ – множество всех символов, которые используются для обозначения объектов (признаков, атрибутов) в транзакциях множества $\boldsymbol{D}$, $\boldsymbol{A}$ – подмножество символов из множества $\boldsymbol{X}$ и $\boldsymbol{D(A)}$ – подмножество множества транзакций из множества $\boldsymbol{D}$, каждая из которых содержит подмножество символов $\boldsymbol{A} \in \boldsymbol{X}$ в качестве подмножества. Для характеристики статистических свойств подмножества $\boldsymbol{A}$ в базе данных $\boldsymbol{D}$ используют отношение мощности n_A множества $\boldsymbol{D(A)}$ к мощности n всего множества транзакций $\boldsymbol{D}$. Эту величину принято называть *поддержкой* (*support*) подмножества $\boldsymbol{A}$ во множестве транзакций $\boldsymbol{D}$:

$$supp(\boldsymbol{A}) = n_A / n . \quad (1)$$

Пусть даны два набора символов (объектов) $\boldsymbol{A}\in\boldsymbol{X}$ и $\boldsymbol{B}\in\boldsymbol{X}$, причем $\boldsymbol{A}$ и $\boldsymbol{B}$ не имеют общих элементов, и пусть σ и γ – вещественные числа из интервала [*0, 1*]. Говорят [4, 5], что выражение вида $\boldsymbol{A}\rightarrow\boldsymbol{B}$ есть *ассоциативное правило* с *порогом уверенности* $conf(\boldsymbol{A}\rightarrow\boldsymbol{B})=\gamma$ и *порогом поддержки* $supp(\boldsymbol{A})=\sigma$ (σ, γ – ассоциативное правило), если справедливы следующие неравенства:

$$n_{AB}/n\geq\sigma, \tag{2}$$

$$n_{AB}/n_A\geq\gamma, \tag{3}$$

где n_{AB} – количество транзакций во множестве $\boldsymbol{D}$, которые содержат объединение множества символов подмножеств $\boldsymbol{A}$ и $\boldsymbol{B}$. Модель ассоциативного правила, заданную условиями (2), (3), принято называть моделью типа *поддержка–уверенность*.

Подмножество (последовательность) элементов $\boldsymbol{A}$ принято называть посылкой ассоциативного правила $\boldsymbol{A}\rightarrow\boldsymbol{B}$, а подмножество (последовательность) $\boldsymbol{B}$ – его следствием. Обычно эти последовательности называют паттернами (*patterns*). В задачах ассоциативной классификации заключение правила может содержать только однолитерный паттерн, который является именем одного из классов. Поэтому в общем случае основная подзадача задачи ассоциативной классификации сводится к поиску множества (σ, γ)–ассоциативных правил для каждого класса. Эта подзадача называется обычно задачей *обучения* классификатора. Другая подзадача – это синтез классификатора на множестве найденных ассоциативных правил.

Сделаем два важных замечания, касающихся понятия *ассоциативное правило*. Первое замечание касается задания линейного порядка на множестве символов $\boldsymbol{X}$. Множества $\boldsymbol{D(A)}$ и $\boldsymbol{D(B)}$– это множества транзакций, в которых каждая транзакция содержит подмножества $\boldsymbol{A}$ и $\boldsymbol{B}$, соответственно, в качестве подмножеств. В них конкретные символы могут следовать в любом порядке. Если наборы этих символов интерпретировать как компоненты векторов (это часто создает большие удобства с формальной точки зрения), то их следует рассматривать как упорядоченные последовательности (цепочки) символов. Зададим линейный порядок на множестве всех символов $\boldsymbol{X}$ и будем, где это удобно, рассматривать любое его подмножество как последовательность символов, упорядоченную в соответствии с введенным порядком на множестве $\boldsymbol{X}$.

Второе замечание касается интерпретации ассоциативного правила как некоторой статистической зависимости. Можно видеть, что ассоциативное правило задает *статистическую зависимость* между

посылкой правила $\boldsymbol{A}$ и его следствием $\boldsymbol{B}$, а числа σ, γ являются статистическими оценками двух вероятностей. Величина σ является оценкой вероятности $\boldsymbol{p(A)}$ появления последовательности $\boldsymbol{A}$ в транзакциях базы данных $\boldsymbol{D}$, а величина γ является оценкой вероятности появления последовательности $\boldsymbol{B}$ в транзакциях этой базы, в которых появилась последовательность $\boldsymbol{A}$, т.е. γ является оценкой условной вероятности $\boldsymbol{p(B/A)}$. Даже в серьезной литературе часто можно встретить высказывания о том, что ассоциативное правило задает отношение импликации. Однако это серьезное заблуждение. Чтобы избежать в дальнейшем путаницы, подчеркнем, что семантика отношения, задаваемого ассоциативным правилом, является совершенно иной, чем семантика отношения, задаваемого импликацией в вероятностной пропозициональной логике или отношением выводимости, задаваемым в аналогичном пропозициональном исчислении. В этом контексте термин *ассоциативное правило* применительно к отношению $\boldsymbol{A \rightarrow B}$ вряд ли является удачным, поскольку он может ввести в заблуждение относительно его семантики. Однако этот термин является общепринятым, а потому для этого отношения далее, несмотря на его неудачность, будет использоваться именно он.

Классические методы поиска ассоциативных правил используют модель, известную под названием *Apriori* [6]. Эта модель является переборной с механизмом отсечения, использующим свойство антимонотонности вероятности появления паттерна (его поддержки) по мере увеличения его длины. Существенно более эффективным методом является группа алгоритмов, известная под названием *FP-growth* [7], однако он пользуется меньшей популярностью у прикладников ввиду его большей сложности. Заметим, что если база данных не является транзакционной, то для использования названных алгоритмов потребуется некоторое преобразование данных.

Понятие ассоциативного правила, введенное условиями (2) и (3), обладает большим недостатком, а именно, оно не учитывает возможную вероятностную независимость, которая может существовать между паттернами $\boldsymbol{A}$ и $\boldsymbol{B}$, когда говорить о существовании ассоциации не имеет смысла. Действительно, можно столкнуться с ситуацией, в которой меры поддержки и уверенности будут достаточно большими просто за счет больших значений вероятностей компонент паттернов, и тогда может быть сделано ошибочное заключение о существовании ассоциативной связи между этими паттернами.

Попытка ослабить действие отмеченного недостатка модели ассоциативного правила вида *поддержка–уверенность* (2), (3) была

предпринята в модели Г.Пятецкого–Шапиро, предложенной в [8]. Дополнительно к мерам поддержки и уверенности, в ней вводится еще один параметр для выбора или отклонения правила. Этот параметр использует известную точечную статистическую меру зависимости между случайными величинами, представленную нижеследующей формулой:

$$I = (n \times n_{AB}) / (n_A \times n_B), \tag{4}$$

которая является статистической оценкой величины

$$I = \frac{P(\boldsymbol{A}, \boldsymbol{B})}{P(\boldsymbol{A})P(\boldsymbol{B})}. \tag{5}$$

В формуле (5) величина $\boldsymbol{P(A,B)}$ есть вероятность совместного появления паттернов $\boldsymbol{A}$ и $\boldsymbol{B}$, а величины $\boldsymbol{P(A)}$ и $\boldsymbol{P(B)}$ – это вероятности появления паттернов $\boldsymbol{A}$ и $\boldsymbol{B}$ в этой же выборке. Близость этой величины к единице свидетельствует о слабой статистической зависимости между паттернами $\boldsymbol{A}$ и $\boldsymbol{B}$. Эта величина в модели Г. Пятецкого–Шапиро используется для задания пороговой характеристики

$$\left| \frac{P(\boldsymbol{A}, \boldsymbol{B})}{P(\boldsymbol{A})P(\boldsymbol{B})} - 1 \right| \geq \delta_{\min}, \tag{6}$$

при этом величина δ_{min} названа автором *минимальным интересом*.

Соответственно, в данной модели определение ассоциативного правила, дополнительно к требованиям (2) и (3), расширено требованием (6), которое позволяет отличить зависимые паттерны $\boldsymbol{A}$ и $\boldsymbol{B}$ от независимых. Эту модель называют моделью *поддержка–уверенность–зависимость*. Параметрами алгоритмов для поиска ассоциативных правил в этом случае являются значения минимальной поддержки $\sigma_{\min}$, минимальной уверенности $\gamma_{\min}$ и минимального интереса δ_{min}. С помощью выбора их значений можно управлять числом ассоциативных правил, которые будут генерироваться соответствующей программой, а также их качеством.

Более строго эта же модель оценки зависимости между компонентами паттерна введена в работе [5]. В ней для проверки зависимости паттернов $\boldsymbol{A}$ и $\boldsymbol{B}$ используется классический χ^2–тест математической статистики, проверяющий значимость гипотезы о равенстве слу-

чайных величин (точечных оценок вероятностей), присутствующих в числителе и знаменателе метрики Г. Пятецкого–Шапиро (5):

$$H_0 : P(\boldsymbol{A},\boldsymbol{B}) - P(\boldsymbol{A})\,\boldsymbol{P}(\boldsymbol{B}) = 0. \qquad (7)$$

Как обычно, алгоритм проверки этой гипотезы состоит в том, чтобы сосчитать оценки вероятностей отдельных паттернов по выборке, сосчитать оценку вероятности их совместного появления в выборке и оценить по критерию χ^2 значимость различия между этими величинами для заданного объема выборки и заданного порога отсечки. Напомним, что значение порога отсечки задает уровень значимости этого различия. Обычно уровень значимости должен быть не меньше, чем 0,95. Заметим, что в работе [8] какая-либо оценка разброса случайной величины (7) не рассматривается.

Обратим внимание на следующее свойство описанной здесь модели ассоциативного правила. Ассоциативная связь, отвечающая модели *поддержка–уверенность–зависимость*, является симметричной относительно посылки и заключения. Другими словами, она не дает информации о направлении этой связи, утверждая только, что или $\boldsymbol{A} \to \boldsymbol{B}$, или $\boldsymbol{A} \leftarrow \boldsymbol{B}$, или эта связь двухсторонняя, т.е. $\boldsymbol{A} \leftrightarrow \boldsymbol{B}$. Естественно, что отсутствие информации о направлении ассоциативной связи в рассматриваемой здесь модели ассоциативного правила является ее недостатком. Этот недостаток преодолевается в моделях ассоциаций причинного типа, в которых рассматривается направленная статистическая связь вида $\boldsymbol{A} \to \boldsymbol{B}$. Построение формальной модели причинной связи, методы поиска и использования ассоциаций причинного типа в задачах принятия решений – это достаточно актуальная и практически важная тема, которая активно исследуется уже в течение почти трех десятилетий. Она развивалась сначала в рамках модели байесовских и причинных сетей доверия, в которых напрямую понятие ассоциативной связи не используется. Однако в последнее десятилетие намечается достаточно сильная конвергенция идей причинных сетей доверия и ассоциативных правил классификации в рамках направления, которое называется ассоциативно–причинная классификация [9, 10]. Однако это уже специальная тема, которая требует отдельного рассмотрения.

В последующем материале данной работы описываются основные результаты, модели, методы, и алгоритмы, разработанные в области ассоциативной классификации, а также приводится их сравнительный анализ применительно к работе с данными большого объема.

3. Ассоциативная классификация: Начальные модели и методы. Работа [3] была первой работой, в которой сформулирована за-

дача ассоциативной классификации. Во многом эта работа выполнена по аналогии с другими моделями поиска правил классификации, которые были разработаны ко времени ее публикации.

В этой работе в постановке задачи рассматриваются обучающие данные, заданные в форме обычной таблицы *объект–признак* с N примерами (строками), l атрибутами и q классами. Полагается, что атрибуты данных являются либо категориальными, либо целочисленными, либо числовыми. Категориальные атрибуты просто нумеруются (точнее–заменяются последовательными целочисленными значениям, однако это не вполне корректно, т.к. при этом на значениях атрибутов искусственно вводится некоторый порядок, реально несуществующий), непрерывные атрибуты заменяются набором дискретных значений и также заменяются нумерованными атрибутами. Таким способом каждый пример выборки трансформируются во множество пар <*атрибут, целочисленное значение*>, которому ставится в соответствие метка класса. В работе рассматривается модель ассоциативного правила в стандартной форме *поддержка–уверенность* вида $\boldsymbol{A_i} \rightarrow \boldsymbol{B_k}$, где посылка $\boldsymbol{A_i} \in \boldsymbol{X}$ есть последовательность пар <*атрибут, целочисленное значение*>, а $\boldsymbol{B_k}$ есть метка класса, $k \in \{1,\ldots,q\}$. Заметим, что авторы ошибочно называют такое правило импликацией (см. по этому поводу замечание в разделе 2).

Предложенный в работе алгоритм поиска ассоциативных правил назван *CBA* (*Classification Based on Associations*). Он состоит из трех шагов, среди которых *первым* является уже описанный алгоритм приведения данных к квази–целочисленной форме. На *втором* шаге поочередно для каждой метки класса генерируется все множество ассоциативных правил, удовлетворяющих заданным ограничениям на минимальные значения мер поддержки и уверенности. Этот шаг реализуется с использованием стандартного алгоритма *Apriori* [6]. Поиск правил для ассоциативной классификации применительно к конкретному классу реализуется с помощью эвристической процедуры на третьем шаге. Для этого используются слегка модифицированные идеи бустинга [11]. Сначала на множестве всех правил класса определяется линейный (тотальный) порядок таким образом:

Правило $r_i \succ r_j$ (первое правило предшествует второму), если

1. Мера уверенности *conf* правила r_i больше, чем правила r_j.

2. Меры уверенности обоих правил одинаковы, но правило r_i имеет большее значение меры поддержки.

3. Обе меры имеют одинаковые значения для обоих правил, но первое правило сгенерировано раньше второго.

Опишем общую идею *третьего* шага предложенного алгоритма для поиска множества правил классификации для конкретного класса, например, для класса $\boldsymbol{B_k}$. Сначала из множества правил, упорядоченного по отношению $\succ$ и имеющего в качестве заключениях имя класса $\boldsymbol{B_k}$, выбирается правило с наименьшим номером. Далее для этого правила находятся все примеры, которые этим правилом *покрываются*. Из обучающей выборки все примеры, найденные таким образом, удаляются, и далее они в процессе выбора правил для класса $\boldsymbol{B_k}$ участия не принимают. Далее аналогичные действия выполняются для следующего (по порядку) правила и т.д. Если очередное правило покрывает хотя бы один новый пример, то оно рассматривается как потенциальное правило классификации и помечается соответствующим образом. После каждого шага вычисляется относительное число ошибок классификации, достигаемое при использовании сформированного множества правил. Если эта величина превышает заданный порог, то процесс формирования итогового множества правил классификации продолжается до тех пор, пока на текущем шаге остаются примеры, которые еще не покрыты ни одним из выбранных правил. Заметим, что примерно так же строится обычная процедура обучения на основе бустинга [11]. После останова процедуры отбора правил классификации из итогового множества удаляются те правила, которые не улучшают точность классификации.

Описанный алгоритм выбора правил удовлетворяет следующим двум условиям:

1. Каждый пример в данных, используемых для обучения, будет покрыт хотя бы одним правилом, и это правило имеет наименьший номер в построенной последовательности правил.

2. Каждое правило в выбранном множестве покрывает хотя бы один пример данных, который не покрывается другим правилом.

Очевидно, что такой алгоритм не является эффективным. Авторы это понимают и предлагают его эвристическую модификацию. Суть этой модификации алгоритма состоит в том, что в нем наилучшее правило отыскивается поочередно для каждого примера. Поэтому эвристический вариант алгоритма является многопроходным по множеству данных. Алгоритм состоит из трех этапов.

На первом этапе для каждого примера $d \in \boldsymbol{D}$ класса $\boldsymbol{B_k}$ находятся два правила, одно из которых правильно классифицирует этот пример и имеет наименьший номер в последовательности правил для этого класса (оно обозначается *cRule*). Второе, аналогичное первому, имеет наименьший номер, но классифицирует этот пример неверно (*wRule*). Если $cRule \succ wRule$, то *cRule* включается во множество потен-

циальных правил классификации для класса $\boldsymbol{B_k}$. В противном случае ситуация обрабатывается несколько более сложным образом. Это связано с тем, что на текущем этапе пока неясно, как правило *cRule* ведет себя по отношению к примерам других классов, и следует ли его включать в потенциальное множество правил для класса $\boldsymbol{B_k}$. Для каждого *cRule* определяется также (и хранится в некоторой структуре данных) то множество примеров, которое этим правилом покрывается.

На втором этапе для тех примеров, для которых выбор правила на этапе 1 сделан не был, выполняется повторный проход по данным. На этом проходе отыскиваются все те *wRule*–правила, которые предшествуют *cRule*, построенному для соответствующего примера. Далее каждое *wRule*– правило, найденное для примера, анализируется, и если оно помечено как *cRule*–правило для некоторого другого примера данного класса, то оно оставляется в найденном множестве, в противном случае – удаляется.

На третьем этапе выполняется финальный выбор правил для класса B_k. Он реализуется в два шага. На первом шаге найденное множество правил упорядочивается и далее вычисляется ошибка классификации по мере увеличения числа правил в соответствии с установленным их порядком. При этом может оказаться, что некоторые правила не покрывают новых примеров (не увеличивают точность классификации). Тогда такие правила удаляются. На втором шаге удаляются правила, которые вносят наибольшие ошибки. В работе [3] приведен псевдокод этого алгоритма, который дополняет его деталями, опущенными здесь.

Авторы сравнивают свой алгоритм с классическим алгоритмом *C4.5* на основе вычислительных экспериментов с 26 наборами данных из *UCI ML Repository* [12] и делают вывод о том, что предложенный ими алгоритм ассоциативного поиска правил классификации демонстрирует более высокую точность.

Ценность этой работы состоит, по-видимому, в том, что она сформулировала проблему ассоциативной классификации, очертила ее особенности и предложила эвристический алгоритм классификации *CBA*. Этот алгоритм аналогичен обычному алгоритму поиска ассоциативных правил с добавлением идей бустинга, разработанного ранее для машинного обучения. Однако более поздние работы показали, что задача поиска ассоциативных правил для решения задач классификации значительно своеобразнее и намного сложнее, чем это может показаться на основании работы [3].

Развитием алгоритма *CBA* является алгоритм *CMAR* (***C**lassification based on **M**ultiple **A**ssociation **R**ules*), предложенный в работе [13].

В этой работе задача классификации формулируется аналогично тому, как она сформулирована в [3]. Ее принципиальное отличие от последней работы состоит в том, что в ней делается акцент на повышение эффективности, причем как процессов генерации ассоциативных правил, так и самих алгоритмов классификации. Заметим, что обеспечение вычислительной эффективности ассоциативной классификации – это ключевая проблема, которая плохо решается большинством методов, предложенных для этих целей. Эта проблема особенно остро проявляется при работе с большими данными.

Для обеспечения высокой эффективности авторы вводят в алгоритм *CBA* два новшества. Первое состоит в том, что они отказываются от использования переборных алгоритмов типа *Apriori* для поиска ассоциативных правил. Вместо него они используют свой метод, разработанный ими двумя годами раньше, который хорошо известен в литературе под названием *метод возрастающих паттернов* (англ. *Frequent Pattern growth, FP-growth*) [7]. Основное новшество этого алгоритма, которое и является источником его эффективности, состоит в том, что все последовательности–кандидаты на включение в искомое множество часто встречающихся паттернов, формирующих посылки правил, представляются в виде *префиксного дерева последовательностей* (*FP-tree*). В этом дереве каждый узел соответствует некоторому символу множества $\boldsymbol{X}$, а последовательности символов с общим префиксом представляются общей последовательностью узлов дерева с началом в его корне. После генерации множества часто встречающихся паттернов дерево типа *FP-tree* оказывается очень удобной структурой их представления. После некоторой модификации оно используется как для реализации процедур отсечения “плохих” правил, так и для просмотра и поиска правил в процессе классификации новых примеров, когда требуется выполнять мэтчинг (сравнение с образцом, от англ. *matching*) тестируемого примера с большим числом ассоциативных правил. Получаемая в итоге структура для представления ассоциативных правил называется авторами *CR-tree*.

Дадим описание этого алгоритма и дерева *CR-tree* более детально, поскольку генерация ассоциативных правил в алгоритме *CMAR* несколько отличается от аналогичного процесса в общем случае алгоритма *FP-growth*. По сравнению с алгоритмом *FP-growth* алгоритм поиска часто встречающихся паттернов в *CMAR* имеет два основных отличия. Если алгоритм *FP-growth* выполняется в два шага, на которых сначала строится дерево часто встречающихся последовательностей, которые имеют значение поддержки больше заданного порогового значения, а затем генерируются ассоциативные правила с требуе-

мым значением меры уверенности, то в алгоритме *CMAR* часто встречающиеся паттерны и правила генерируются за один шаг. Второе отличие состоит в том, что алгоритм *CMAR* для каждого правила запоминает распределение значений поддержки на множестве всех классов, для которых данное правило имеет ненулевое ее значение. Последнее не требует дополнительных вычислений, поскольку значения поддержки для классов в *CMAR* вычисляются в любом случае.

Множество сгенерированных ассоциативных правил, каждое из которых имеет три атрибута – метка класса, значение поддержки и меры уверенности, хранится в структуре дерева *CR-tree*. Пример такого дерева представлен на рисунке 1 (рисунок заимствован из работы [13]). Можно видеть, что *CR-tree* является достаточно компактной структурой. Оно уже хранит индексы для доступа к правилам. Очевидно, что просмотр правил при таком их представлении является эффективной процедурой.

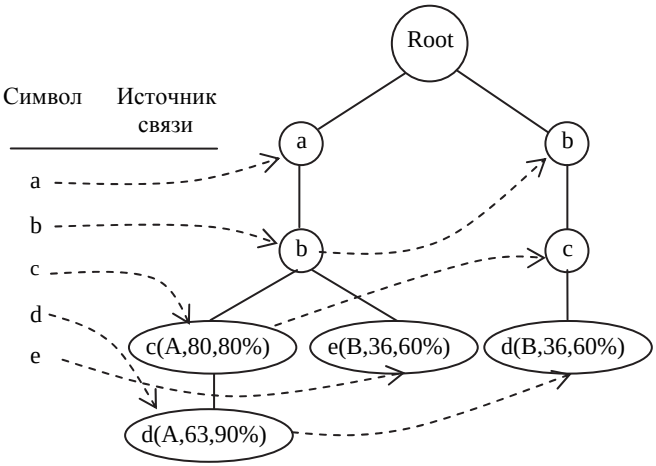


Рис. 1. Пример *CR-tree*. A, B–метка класса, 80–поддержка (число примеров класса, содержащих паттерн), 80%–значение уверенности

Однако не все правила построенного таким способом дерева используются в алгоритме классификации. Наименее эффективные правила удаляются на этапе отсечения. Можно видеть, что и процедура отсечения может быть эффективно реализована с помощью того же дерева *CR-tree* следующим образом. Сначала на множестве правил задается глобальный порядок, в соответствии с которым далее упоря-

дочиваются все правила класса. Порядок этот строится следующим образом.

Говорят, что из двух правил r_1 и r_2 правило r_1 имеет больший ранг, чем правило r_2, иначе, $r_1 \succ r_2$, если и только если (1) $conf(r_1)>conf(r_2)$; или (2) если $conf(r_1)=conf(r_2)$, но $supp(r_1)>supp(r_2)$; или (3) если $conf(r_1)=conf(r_2)$ и $supp(r_1)=supp(r_2)$, но правило r_1 в левой части имеет меньшее число символов, чем правило r_2. Говорят также, что правило r_1: $\boldsymbol{P}\rightarrow\boldsymbol{C}$ является более общим по отношению к правилу r_2: $\boldsymbol{P}'\rightarrow\boldsymbol{C}'$ тогда и только тогда, когда посылка $\boldsymbol{P}$ первого правила $\boldsymbol{P}$ является подмножеством посылки $\boldsymbol{P}'$ второго правила. Введенный порядок используется алгоритмом *CMAR* для отсечения правил из дерева *CR-tree*.

Процедура отсечения выполняется за три шага:

Шаг 1. Отсекаются менее общие правила с низким значением меры уверенности. Это отсечение выполняется каждый раз, когда правило вставляется в *CR-tree* в процессе генерации правил.

Шаг 2. После построения дерева *CR-tree* из него удаляются правила, в которых посылка и заключение имеют отрицательную корреляцию. Этот факт определяется применением χ^2–теста. Заметим, что с необходимостью удаления таких правил нельзя согласиться безоговорочно, поскольку правила с отрицательной корреляцией в некоторых случаях несут очень полезную информацию для классификации, в особенности, если связь имеет причинный характер. Например, если некоторый паттерн имеет значение коэффициента корреляции с заключением близкое к величине *–1*, то такое правило является *запретом* для данного класса. А запрет представляет собой очень сильную закономерность. Его удаление из множества классификационных правил вряд ли оправдано.

Шаг 3. Отсекаются правила, имеющие значение фактора покрытия примеров класса в обучающей выборке меньшее, чем заданный порог.

Что касается алгоритма классификации, то он строится на основе полученного множества классификационных правил аналогично тому, как это делается в алгоритме *CBA* с некоторым отличием в модели объединения решений, выдаваемых различными правилами. В алгоритме *CMAR* сначала все правила, оставленные в дереве *CR-tree* после отсечения разбиваются на группы, каждая их которых в заключении содержит метку одного и того же класса. При тестировании примера для каждой такой группы правил в *CMAR* вычисляется значение веса. Этот вес является некоторой эвристически выбранной функцией, которую авторы называют *взвешенной χ^2–статистикой* [13]. Заметим,

что эта мера имеет достаточно сложное выражение. Авторы признают, что она не имеет никакого теоретического обоснования или содержательной интерпретации. Мотивацией для ее использования в алгоритме *CMAR* являются только результаты экспериментальных исследований. Решение принимается в пользу того класса, для которого взвешенная χ^2–статистика принимает наибольшее значение.

Свойства алгоритма *CMAR* исследованы на 26 наборах тестовых данных из UCI репозитория [12]. На основании экспериментальных результатов, приведенных в работе, авторы делают вывод о том, что алгоритм *CMAR* обладает существенно лучшими характеристиками по вычислительной эффективности по сравнению с методами *CBA* и *C4.5* [14]. Он обладает также лучшими показателями по точности решения задач классификации, однако в этом отношении его преимущества не столь существенны.

Для генерации правил ассоциативной классификации в работе [15] предлагается использовать идеи метода ID3 [16]. Этот метод был очень популярен в период с 1980 по 2000 г.г. Хотя предложенный метод, для которого авторы используют название *CPAR (**C**lassification based on **P**redictive **A**ssociation **R**ules)*, эксплуатирует довольно старую идею, он имеет некоторые новые свойства, заслуживающие упоминания.

В основу метода положен алгоритм *FOIL* [17]. Этот алгоритм рекурсивно отыскивает атрибут (признак), добавляемый к последовательности–потенциальной посылке формируемого правила, который максимизирует метрику, называемую *информационным выигрышем* (*information gain*). Максимизация этой метрики ведет к наилучшему покрытию текущего множества обучающих данных. Данные выборки, покрытые найденным правилом, удаляются из обучающего множества, и далее поиск атрибутов, обеспечивающих максимизацию информационного выигрыша, ведется по отношению к новому, сокращенному множеству обучающих данных. Как хорошо известно, этот метод работает с парой классов. Если классов много, то метод *FOIL* использует хорошо известную схему “выбранный класс” – “все другие классы” для сведения задачи с множеством классов к последовательности задач бинарной классификации. Алгоритм CWAC [18], по сути, аналогичен алгоритму FOIL. Отличие состоит только в том, что авторы [18], кроме *информационного выигрыша*, используют для оценки правил *взвешенную поддержку* и *взвешенную уверенность*.

Модификация же метода CPAR применительно к задаче ассоциативной классификации состоит в следующем. В отличие от *FOIL*, который на каждом шаге рекурсивного формирования посылки прави-

ла допускает только одно ее продолжение за счет добавления нового атрибута, алгоритм *CPAR* рассматривает несколько таких продолжений. В качестве вариантов продолжений он рассматривает все те атрибуты, которые имеют одинаковые или близкие значения *информационного выигрыша*. Эту часть алгоритма *CPAR* авторы называют *PRM*–алгоритмом, *Predictive Rule Mining.* Далее, в отличие от того, как это делается в некоторых вариантах алгоритмов генерации правил классификации с использованием идей бустинга [11], пример обучающих данных, покрытый вновь сгенерированным правилом, не удаляется из процесса обучения. Он используется и на последующих шагах поиска, но с меньшим весом. Каждое сгенерированное правило оценивается по некоторой метрике, значение которой используется в дальнейшем для принятия решения о том, использовать ли то или иное правило в алгоритме классификации или нет. Для каждого класса оставляется k наилучших (по упомянутой метрике) правил, на базе которых и строится алгоритм классификации новых примеров. Заметим, что механизм классификации на основе множества построенных правил не отличается оригинальностью. В нем для классифицируемого примера оценивается среднее значение вероятности его принадлежности к каждому классу по множеству всех правил. Предпочтение отдается тому из классов, для которого эта точность наибольшая. Детали алгоритма, как и доказательства корректности различных его шагов применительно к задачам ассоциативной классификации, могут быть найдены в работе [15].

Метод *CPAR* был исследован экспериментально на 26 наборах данных их UCI–репозитория [12]. По утверждению авторов, он превзошел по точности предсказания класса другие методы, которые на момент публикации работы [15] рассматривались как наилучшие. К ним относятся, в частности, такие методы, как *C4.5* [16], *RIPPER* [19], *CBA* [3], *CMAR* [13] и ACAC [14, 20].

Заметим, что в число алгоритмов, с которыми авторы сравнивали метод *CPAR*, не вошли алгоритмы, основанные на использовании понятия эмерджентных паттернов, хотя эти алгоритмы были опубликованы за несколько лет до публикации алгоритма *CPAR*.

4. Заключение. Модели ассоциативной классификации, получившие основное развитие в течение последних пятнадцати лет, предлагают подход, который пытается интегрировать в себе некоторые базовые результаты теории и практики классического индуктивного обучения и механизмы поиска ассоциативных правил. Целью такой интеграции является повышение вычислительной эффективности и точности решения традиционных задач классификации с ориентацией на

использование полученных моделей для анализа больших данных. Первые модели ассоциативной классификации рассматривали задачу ассоциативной классификации просто как частный случай задачи поиска ассоциативных правил, в котором правая часть правила может принимать значения из фиксированного множества меток (идентификаторов классов). Рассмотренные в работе алгоритмы *CBA* [3], *CMAR* [13] и *CPAR* [15], являются примерами такого прямолинейного подхода. Однако именно в этих работах была явно сформулирована проблема ассоциативной классификации, очерчены ее особенности. Эти работы задали исходный уровень эффективности алгоритмов ассоциативной классификации и выявили главные проблемы, которые возникают при обучении и использовании моделей ассоциативной классификации, определив тем самым направления дальнейшего развития этих моделей.

Отметим, что более поздние работы показали, что задача поиска ассоциативных правил для решения задач классификации значительно своеобразнее и намного сложнее, чем это может показаться на основании работ [3, 13, 15].

Во второй части текущей работы будет более подробно рассмотрена группа методов и алгоритмов, предназначенных для поиска ассоциативных правил классификации с помощью эмерджентных паттернов. Этот подход, по существу, определил новое направление в области ассоциативной классификации. Это направление активно развивается вплоть до настоящего времени. Его результаты позволяют устранить некоторые недостатки начальных моделей и алгоритмов ассоциативной классификации, описанных в данной работе. Работы в этом направлении [21-24] во многом способствовали более глубокому пониманию специфики задач ассоциативной классификации и путей ее эффективной алгоритмизации.

Литература

1. Wikipedia.org: the free encyclopedia // URL: http://en.wikipedia.org/w/index.php?title=Big_data&oldid=556537897 (дата обращения 20.06.2014 г.).
2. *Douglas L.* 3D Data Management: Controlling Data Volume, Velocity and Variety // URL: http://blogs. gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf (дата обращения 20.06.2014 г.).
3. *Liu B., Hsu W., Ma Y.* Integrating classification and association rule mining // Proceedings of the KDD'98, New York, NY, Aug. 1998. pp. 80–86.
4. *Городецкий В.И., Самойлов В.В.* Ассоциативный и причинный анализ и ассоциативные байесовские сети // Труды СПИИРАН. 2009. №9. С. 13-65.
5. *Brin S., Motwani R., Silverstein C.* Beyond market baskets: generalizing association rules to correlations // Proceedings of the ACM SIGMOD Intern. Conf. on Management of Data. 1997. pp. 255–264.

6. *Agrawal R., Sricant R.* Fast Algorithm for Mining Association rules // Proceedings of the 20th Intern. Conference on Very Large Databases, Santiago, Chile. 1994. pp. 68-77.
7. *Han J., Pei J., Yin Y.* Mining frequent patterns without candidate generation // Proceedings of the ACM SIGMOD Intern. Conf. on Management of Data. 2000. pp. 1–12.
8. *Piatetsky–Shapiro G.* Discover, analysis, and presentation of strong rules // Knowledge discovery from Databases. G. Piatetsky–Shapiro and W.Frawley (Eds.). AAAI Press/MIT Press. 1991. pp. 229-248.
9. *Aliferis C.F., Statnikov A., et al.* Local Causal and Markov Blanket Induction for Causal Discovery and Feature Selection for Classification Part I: Algorithms and Empirical Evaluation // Journal of Machine Learning Research. 2010. no. 11. pp. 171-234.
10. *Aliferis C.F., Statnikov A.*, et al. Local Causal and Markov Blanket Induction for Causal Discovery and Feature Selection for Classification Part II: Analysis and Extensions // Journal of Machine Learning Research. 2010. No. 11. pp. 235 – 299.
11. *Schapire R.E.* The Boosting Approach to Machine Learning. An Overview Nonlinear Estimation and Classification. Springer. Lecture Notes in Statistics. vol. 171. Denison D.D., Hansen M.H, Holmes C.C., Mallick B., Yu B. (Eds). 2003. pp. 149–172.
12. *Blake C.L., Murphy P.M.* UCI Repository of machine learning database. University of California, Department of Information and Computer Science. Irvine, CA. 1998 // URL: http://www.cs.uci.edu/ mleam/mlrepository.html (дата обращения 20.06.2014).
13. *Li W., Han J., Pei J.* CMAR: Accurate and efficient classification based on multiple class-association rules // Proceedings of the ICDM'01, San Jose, CA, Nov. 2001. pp. 369–376.
14. *Wedyan S.* Review and Comparison of Associative Classification Data Mining Approaches // International Journal of Computer, Information, Systems and Control Engineering. 2014. vol. 8 no.1. pp. 34–45.
15. *Yin X., Han J.* CPAR: Classification Based on Predictive Association Rule // Proceedings of the SDM'03. 2003. pp. 369–376.
16. *Quinlan J.R.* C4.5: Programs for Machine Learning. Morgan Kaufmann, 1993.
17. *Quinlan J.R., Cameron-Jones R.M.* FOIL: A midterm report // Proceedings of the European Conference on Machine Learning. Vienna, Austria. 1993. pp. 3–20.
18. *Ibrahim S., Chandran K.R.* Compact Weighted Class Association Rule Mining using Information Gain // International Journal of Data Mining & Knowledge Management Process (IJDKP). 2011. vol.1, no.6. pp. 1–13.
19. *Cohen W.* Fast effective rule induction // Proceedings of the ICML'95. Tahoe City, CA. 1995. pp. 115–123.
20. *Huang Z., Zhou Z., He T., Wang X.* ACAC: Associative Classification based on All-Confidence // Proceedings of IEEE International Conference on Granular Computing (GrC). 2011. pp. 289-293.
21. *Dong G., Li J.* Efficient Mining of Emerging Patterns: Discovering Trends and Differences // Proceedings of the KDD'99. 1999. pp. 43–52.
22. *Dong G., Zhang X., Wong L., Li J.* CAEP: Classification by Aggregating Emerging Patterns // Proceedings of the DS'99, .1999. pp. 30–42.
23. *Fan H., Ramamohanarao K.* Fast Discovery and the Generalization of Strong Jumping Emerging Patterns for Building Compact and Accurate Classifiers // IEEE Trans. Knowl. Data Eng. 2006. vol. 18(6). pp. 721-737.
24. *Li J., Dong G, Ramamohanarao K.* Making use of the most expressive jumping emerging patterns for classification // Proceedings of the Fourth Pacific-Asia Conference on Knowledge Discovery and Data Mining. Kyoto, Japan. 2000. pp. 220-230.

References

1. Wikipedia.org: the free encyclopedia. Available at: http://en.wikipedia.org/w/index.php?title=Big_data&oldid=556537897 (Accessed: 20.06.2014 г.).
2. Douglas L. 3D Data Management: Controlling Data Volume, Velocity and Variety. Available at: http://blogs. gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf (Accessed: 20.06.2014 г.).
3. Liu B., Hsu W., Ma Y. Integrating classification and association rule mining. Proceedings of the KDD'98, New York, NY, Aug. 1998. pp. 80–86.
4. Gorodetsky V., Samoylov V. [Associative and causal analysis and associative Bayesian networks]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2009. vol.9. pp. 13-65. (In Russ.).
5. Brin S., Motwani R., Silverstein C. Beyond market baskets: generalizing association rules to correlations. Proceedings of the ACM SIGMOD Intern. Conf. on Management of Data. 1997. pp. 255–264.
6. Agrawal R., Sricant R. Fast Algorithm for Mining Association rules. Proceedings of the 20th Intern. Conference on Very Large Databases, Santiago, Chile. 1994. pp. 68-77.
7. Han J., Pei J., Yin Y. Mining frequent patterns without candidate generation. Proceedings of the ACM SIGMOD Intern. Conf. on Management of Data. 2000. pp. 1–12.
8. Piatetsky–Shapiro G. Discover, analysis, and presentation of strong rules. Knowledge discovery from Databases. G. Piatetsky–Shapiro and W.Frawley (Eds.). AAAI Press/MIT Press. 1991. pp. 229-248.
9. Aliferis C.F., Statnikov A., et al. Local Causal and Markov Blanket Induction for Causal Discovery and Feature Selection for Classification Part I: Algorithms and Empirical Evaluation. Journal of Machine Learning Research. 2010. no. 11. pp. 171-234.
10. Aliferis C.F., Statnikov A., et al. Local Causal and Markov Blanket Induction for Causal Discovery and Feature Selection for Classification Part II: Analysis and Extensions. Journal of Machine Learning Research. 2010. no. 11. pp. 235 – 299.
11. Schapire R.E. The Boosting Approach to Machine Learning. An Overview Nonlinear Estimation and Classification. Springer. Lecture Notes in Statistics. Vol. 171. Denison D.D., Hansen M.H, Holmes C.C., Mallick B., Yu B. (Eds). 2003. pp. 149–172.
12. Blake C.L., Murphy P.M. UCI Repository of machine learning database / University of California, Department of Information and Computer Science. Irvine, CA. 1998. Available at: http://www.cs.uci.edu/ mleam/mlrepository.html (Accessed:20.06.2014).
13. Li W., Han J., Pei J. CMAR: Accurate and efficient classification based on multiple class-association rules. Proceedings of the ICDM'01, San Jose, CA, Nov. 2001. pp. 369–376.
14. Wedyan S. Review and Comparison of Associative Classification Data Mining Approaches. International Journal of Computer, Information, Systems and Control Engineering. 2014. vol. 8 no.1. pp. 34–45.
15. Yin X., Han J. CPAR: Classification Based on Predictive Association Rule. Proceedings of the SDM'03. 2003. pp. 369–376.
16. Quinlan J.R. C4.5: Programs for Machine Learning. Morgan Kaufmann, 1993.
17. Quinlan J.R., Cameron-Jones R.M. FOIL: A midterm report. Proceedings of the European Conference on Machine Learning. Vienna, Austria. 1993. pp. 3–20.
18. Ibrahim S., Chandran K.R. Compact Weighted Class Association Rule Mining using Information Gain. International Journal of Data Mining & Knowledge Management Process (IJDKP). 2011. vol.1, no.6. pp. 1–13.
19. Cohen W. Fast effective rule induction. Proceedings of the ICML'95. Tahoe City, CA. 1995. pp. 115–123.

20. Huang Z., Zhou Z., He T., Wang X. ACAC: Associative Classification based on All-Confidence. Proceedings of IEEE International Conference on Granular Computing (GrC). 2011. pp. 289-293.
21. Dong G., Li J. Efficient Mining of Emerging Patterns: Discovering Trends and Differences. Proceedings of the KDD'99. 1999. pp. 43–52.
22. Dong G., Zhang X., Wong L., Li J. CAEP: Classification by Aggregating Emerging Patterns. Proceedings of the DS'99, .1999. pp. 30–42.
23. Fan H., Ramamohanarao K. Fast Discovery and the Generalization of Strong Jumping Emerging Patterns for Building Compact and Accurate Classifiers. IEEE Trans. Knowl. Data Eng. 2006. vol. 18(6). pp. 721-737.
24. Li J., Dong G, Ramamohanarao K. Making use of the most expressive jumping emerging patterns for classification. Proceedings of the Fourth Pacific-Asia Conference on Knowledge Discovery and Data Mining. Kyoto, Japan. 2000. pp. 220-230.

Тушканова Ольга Николаевна — аспирант, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук. Область научных интересов: машинное обучение, интеллектуальный анализ данных, извлечение знаний, многоагентные системы, рекомендующие системы, облачные технологии, онтологии. Число научных публикаций — 12. tushkanova.on@gmail.com; 199178, Санкт-Петербург, 14 линия, д. 39; р.т.: +79817343119.

Tushkanova Olga Nikolaevna — Ph.D. student, St.Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences. Research interests: data mining, multi-agent systems, recommender systems, cloud computing, ontologies, knowledge extraction technologies. The number of publications — 12. tushkanova.on@gmail.com; 39, 14-th Line, St. Petersburg, 199178, Russia; office phone: +79817343119.

Городецкий Владимир Иванович — д-р техн. наук, профессор, заведующий лабораторией интеллектуальных систем, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук. Область научных интересов: искусственный интеллект, технология многоагентных систем, распределенное обучение, извлечение знаний из баз данных, анализ и объединение данных различных источников, P2P сети принятия решений и P2P методы извлечения знаний из данных, обработка больших данных, планирование и составление расписаний, алгоритмы улучшения изображений, рекомендующие системы. Число научных публикаций — 200. gor@mail.iias.spb.su; 199178, Санкт-Петербург, 14 линия, д. 39; р.т.: +7-812-328-3311.

Gorodetsky Vladimir Ivanovich — Ph.D., professor, head of laboratory of intelligent systems, St.Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences. Research interests: intelligent data analysis, information fusion, P2P data mining and machine learning, multi-agent systems technology and software tools, agent-based applications, recommender systems, mobile image enhancement. The number of publications — 200. gor@mail.iias.spb.su; 39, 14-th Line, St. Petersburg, 199178, Russia; office phone: +7-812-328-3311.

РЕФЕРАТ

Городецкий В.И., Тушканова О.Н. **Ассоциативная классификация: аналитический обзор. Часть 1.**

В настоящее время в области работы с большими данными, в частности, в интересах решения задач классификации, развиваются новые методы, модели и алгоритмы интеллектуальной обработки. Одним из таких относительно новых направлений является *ассоциативная классификация*. В данной работе описываются, анализируются и сравниваются начальные результаты, модели и методы, разработанные в области ассоциативной классификации, применительно к работе с данными большого объема и устанавливается их связь с классическими результатами в области индуктивного обучения и методами поиска часто встречающихся паттернов для генерации ассоциативных правил. В работе дается постановка задачи ассоциативной классификации, вводится необходимая терминология и формальные обозначения, используемые в ассоциативной классификации. Приводится описание и сравнительный анализ начальных алгоритмов в области ассоциативной классификации. Дается оценка вклада первых работ, посвящённых ассоциативной классификации, в развитие этого направления, а также и формулируются цели дальнейшего исследования.

SUMMARY

Gorodetsky V., Tushkanova O. **Associative Classification: Analytical Overview. Part 1.**

Currently new methods, models and algorithms for intelligent processing of big data (in particular for solving classification problems) are rapidly developing. One of these areas - associative classification - is relatively new. The paper topic is early methods of associative classification intended for processing of big data. It formulates corresponding problem statement and introduces basic concepts and formal notation used in associative classification. An extended overview and comparative analysis of the basic approaches, models and algorithms developed for associative classification form the main paper contents. The paper assesses the contribution of the first papers devoted to associative classification to the development of this area and formulates goals of the further research.

УДК 004.82; 004.94

П.А. Глыбовский, С.В.Пилькевич, Р.Б. Жолус, Ю.А.Пономарев

МНОГОУРОВНЕВОЕ ПРЕДСТАВЛЕНИЕ РАЗНОРОДНЫХ НЕЧЕТКИХ ПАРАМЕТРОВ ДЛЯ ИДЕНТИФИКАЦИИ СОСТОЯНИЙ ОБЪЕКТА КОНТРОЛЯ

Глыбовский П.А., Пилькевич С.В., Жолус Р.Б., Пономарев Ю.А. **Многоуровневое представление разнородных нечетких параметров для идентификации состояний объекта контроля.**

Аннотация. Для принятия решения о степени принадлежности объекта контроля классу идентифицируемых состояний необходимо произвести агрегирование его известных характеристик, в результате которого массив разнородных параметров может быть сведен к небольшому числу обобщенных классов, функционально связанных с исходными данными. Данная задача решается с помощью алгоритмов нечеткой классификации.

Ключевые слова: агрегирование, функция принадлежности, информационные НЕ-факторы, нечеткое представление разнородных параметров.

Glybovsky P.A., Pilkevich S.V., Zholus R.B., Ponomarev Y.A. **Multilevel Representation of Heterogeneous Fuzzy Parameters for Identification of Object Control States**.

Abstract. For a decision about the degree of membership of the test object to class of identified conditions it is necessary to produce the aggregation of its known characteristics, as the result diverse array of parameters can be reduced to a small number of generic classes that are functionally associated with the source data. This problem can be solved using algorithms for fuzzy classification.

Keywords: aggregation, membership function, information non-factors, the fuzzy representation of the heterogeneous parameters.

1. Введение. В области инженерии знаний к настоящему моменту разработано достаточно большое число методов, стратегий и процедур работы с экспертами, предложены различные способы обработки полученных в результате взаимодействия с экспертами результатов, а также создан целый ряд программных средств, автоматизирующих процессы извлечения знаний из экспертов, специальных текстов на естественном или структурированном языке и баз данных [1].

Неотъемлемой частью Системы знаний являются систематизированные знания, образующие целостное описание некоторой проблемной области с доступной и достаточной для решения прикладных задач степенью точности. При этом общие базовые свойства традиционных математических аппаратов, которые по умолчанию привыкли считать необходимыми для любой формальной системы (*точность*, *полнота*, *определенность*, *корректность* и др.), являются в знаниях о реальном мире редкими исключениями, представляя лишь искусственные частные случаи таких НЕ-факторов, как *недоопределенность*, *неточность*, *неполнота*, *некорректность* и др.

НЕ-фактором называется некоторое понятие, которое лексически, синтаксически и семантически отрицает какое-либо свойство или аспект знания, как, например, противоречивость (отрицает непротиворечивость знания), неточность (отрицает точность знания) и т. д. [2, 3].

НЕ-факторы "встроены" в нашу Картину мира, как основная составляющая знаний, являясь их материей и строительным материалом [4]. Обращает на себя внимание, тот факт, что НЕ-факторы присущи не только знаниям экспертов о соответствующих предметных областях, но и абсолютно объективным источникам данных и знаний – например, детектирующей аппаратуре, сенсорам, измерительным приборам и т.д.

Причем речь не идет только о роли НЕ-факторов в формальном описании Системы знаний в рамках тематики искусственного интеллекта. Это касается всех наших знаний о знаниях, т.е. всего известного пространства функционирования знаний во всех областях человеческой деятельности.

Современные объекты экономики и инфраструктуры, военно-технических и сложных социотехнических систем, а также природно-территориальные комплексы требуют применения эффективных подсистем управления, функционирующих на базе экспертных систем и систем поддержки принятия решений, в основе которых должны быть базы знаний, учитывающих разнообразные информационные НЕ-факторы.

2. Терминология и классификация. В виду разнородности знаний о мире как таковых и нашем представлении о комплексе НЕ-факторов, присущих современной картине мира, полная классификация НЕ-факторов отсутствует. Тем не менее, систематизации могут быть подвергнуты наиболее проработанные к настоящему времени НЕ-факторы. Классификационная схема, объединяющая основные информационные НЕ-факторы, составленная по [2] представлена на рисунке 1.

Здесь приведен комплекс НЕ-факторов, отражающих различные аспекты Системы знаний и объединенных в группы:

– *базовые НЕ-факторы*, являющиеся неотъемлемым элементом любой Системы знаний;

– *системные НЕ-факторы*, относимые к тем данным и знаниям, которые оцениваются как адекватные, но не достигшие уровня, достаточного для того, чтобы считать их в текущем контексте *однозначными* и/или *четкими*;

– *НЕ-факторы*, играющие роль *классификаторов* и связанных с понятием *некорректности*, определяемом как комплекс нарушений в данных, знаниях и методах их обработки, приводящих к возникновению ошибок, искажений и противоречий;

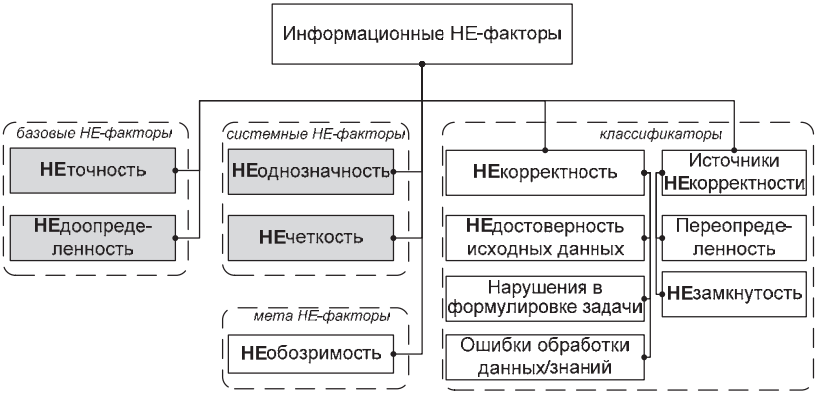


Рис. 1. Классификация информационных НЕ-факторов

– *мета НЕ-факторы*, характеризующие необозримость компонент Системы знаний, т.е. недостаточность текущих знаний, не позволяющую эффективно использовать их для решения практических задач.

Для практики построения методов и алгоритмов, реализуемых в рамках экспертных систем и систем поддержки принятия решений, наибольшую значимость имеет учет базовых и системных НЕ-факторов.

Неточность – один из наиболее часто встречающихся НЕ–факторов [5], так как он проявляется в знаниях из-за погрешности измерения.

Неточность определяется как наличие некоторого множества *X*, такого что $X \cap F \not\in \varnothing$, где $x \in F$, F – нечеткое множество, и при этом значение параметра *x* определено с точностью до *X*-оценка погрешности измерений [6].

Недоопределенность - это частичное отсутствие знаний о значении какого-либо параметра [3]. Как правило, Недоопределенность значения переменной выражается в её интервальном характере. Например, в физиологии и медицине значения параметров организма человека варьируются в широких диапазонах: частота сердечных сокращений (ЧСС) при брадикардии от 40 до 60 ударов в минуту. В норме для взрослого человека ЧСС от 60 до 80 ударов в минуту. При умеренной физической и психоэмоциональной нагрузке увеличивается до 90-120 в минуту, а при больших нагрузках – до 100-150 в минуту. У спортсменов во время максимальной нагрузки ЧСС может достигать 190-200 ударов в минуту. Таким образом, $x^{ЧСС} \in [40;200]$.

В случае измеримых параметров недоопределенность и неточность можно приводить друг к другу, однако существует четкое разгра-

ничение. При недоопределенности частичное отсутствие знаний можно восполнять, постепенно доопределяя параметр, а неточные измеренные параметры самодостаточны сами по себе, так как зачастую повышать точность измерения для решения конкретной задачи не имеет смысла.

Возвращаясь к примеру отметим, что если имеется дополнительная информация о возрасте (65 лет), поле (мужской), физическом и психологическом состоянии индвида (тахикардия), то это доопределит параметр до более уточненного диапазона значений - $x^{ЧСС} \in [120;140]$.

Как отмечалось во введении, определенные и точные значения в реальных задачах являются исключением, поскольку и *Неточность* и *Недоопределенность* – факторы, присущие всем параметрам реальных объектов. Каждая переменная адекватной математической модели в общем случае должна быть одновременно и неточной, и недоопределенной, т.е. обладать способностью уточняться, но до предела, заданного уровнем точности ее области значений [1].

Неоднозначное значение параметра X включает текущее значение H, представляющее альтернативы возможных вариантов X, т.е. $H \subseteq X$, и заданное на нем распределение оценки каждой из этих альтернатив $\hat{f}(H)$. Таким образом, формально неоднозначное значение представляется следующим образом:

$$X = \langle \{H\}; \hat{f}(H) \rangle.$$

При этом распределение и Н-значение тесно связаны между собой: стягивание Н-значения приводит к корректировке распределения и, наоборот, если распределение принимает значение ноль на какой-то из альтернатив, то она исключается из Н-значения и оно сокращается (уточняется) [7].

Физиологические параметры организма человека, как отмечалось выше, носят интервальный характер, причем распределение значений на этих интервалах (например, $x^{ЧСС} \in [40;200]$) является нормальным, т.е. неоднозначное значение ЧСС представимо в виде:

$$X = \left\langle \{x\}; \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-m)^2}{2\sigma^2}} \right\rangle,$$

где m – математическое ожидание, а величина σ – среднее квадратическое отклонение величины x (ЧСС). При этом отмечается, что нормальное распределение значений того или иного параметра соответствует большой репрезентативной выборке. В том случае, если выборка

представлена иной целевой аудиторией, например лицами мужского пола возрастом от 18 до 22 лет, то исследуемый параметр $\left(x^{ЧСС} \in [55;120]\right)$ подчиняется распределению Фишера-Типпета и Н-значение X будет иметь следующий вид:

$$X = \left\langle \{x\}; \frac{1}{\sigma}\left[1+\frac{1}{2}\left(\frac{x-m}{\sigma}\right)\right]^{-3} e^{-\left(1+\frac{x-m}{2\sigma}\right)^{-2}} \right\rangle.$$

Наиболее популярным НЕ-фактором является *Нечеткость*. Нечеткая переменная характеризуется тройкой [8]:

$$FV = \langle \alpha, X, A \rangle,$$

где α – наименование переменной, X - универсальное множество (область определения α), A - нечеткое множество на X, описывающее ограничения $\mu_A(x)$ на значение нечеткой переменной α.

Пусть $X = \{1,2,3,...,100\}$ соответствует понятию «возраст», тогда нечеткое множество «молодой», можно определить с помощью функции принадлежности вида:

$$\mu_{молодой}(x) = \begin{cases} 1, 1 \le x < 25 \\ \dfrac{1}{1+\left(\dfrac{x-25}{5}\right)^2}, x \ge 25 \end{cases}.$$

Нечеткое множество «молодой» на универсальном множестве $X' = \{\text{Иванов,Петров,Сидоров,...}\}$ задается с помощью функции принадлежности $\mu_{молодой}(x)$ на $X = \{1,2,3,...,100\}$ (возраст), что называется относительно X' функцией совместимости, при этом:

$$\mu_{молодой}(\text{Сидоров}) = \mu_{молодой}(18),$$

где 18 – возраст Сидорова.

Применение нечетких переменных при описании проблемной ситуации позволяет абстрагироваться от уяснения различий в прагматике тех или иных реальных НЕ-факторов, к которым она применяет-

ся, а также связи этой прагматики с конкретной коммуникативной и (или) когнитивной ситуацией.

Подводя промежуточный итог, отметим, что наличие информационных НЕ-факторов, характерно не только для данных и знаний из области физиологии и медицины. Более того, приведенный в качестве примеров интервальный характер Н-значений является частным случаем при котором элементы нечеткого множества строго упорядочены. Н-значения параметров объектов контроля и(или) их экспертные оценки, свойственны как гуманитарным (социология, экономика, психология, лингвистика и др.), так и техническим (кибернетика, робототехника, информатика и др.) наукам.

3. Иерархическая структура показателей объекта контроля. В рамках рассматриваемой проблематики наибольший интерес вызывает исследование показателей, отражающих данные и (или) знания о предметной области и составляющих строгие иерархии.

Данный факт, а также то, что разнородные параметры объектов контроля имеют ярко выраженный нечеткий характер, позволяет получать обобщенные агрегированные показатели, которые объединяют только те параметры, которые характеризуют вполне конкретные свойства объекта контроля [9].

Для сложных социотехнических систем особую актуальность приобретает мониторинг функционального состояния операторов дежурных смен ухудшение психофизиологического состояния которых, снижение эффективности работы, а также скрытое изменение поведения может привести к значительному ущербу, вплоть до техногенной катастрофы.

Одним из агрегирующих параметров организма, изменение которого может сигнализировать о выходе состояния оператора за «границы нормы» является индекс стресса, также известный как индекс напряжения регуляторных систем или индекс Баевского. Исходными данными для получения индекса Баевского являются измерения частоты пульса, уровня артериального давления, роста и массы тела [10].

Рассматривая более высокие уровни иерархии показателей можно перейти от индивида к характеристикам социальной группы, членом которой он является. Так, например, эмоциональная напряженность в коллективе представляет собой агрегирование таких показателей как потребность в информации, необходимая и имеющаяся информация, представленных как значения на безразмерной шкале, полученные в результате опроса или анкетирования членов исследуемого коллектива.

В ряде случаев окончательный вывод может быть сделан лишь после многократной свертки частных показателей объекта или его отдельных компонентов. Поэтому задача оценивания, не поддающегося непосредственному измерению интегрального показателя по заданным значениям частных критериальных характеристик может рассматриваться как задача снижения размерности исследуемого признакового пространства [11].

Целевой функцией исследуемого обобщенного показателя, определяемого значениями $x^{(1)},...,x^{(p)}$ ее частных критериальных характеристик, будем называть любое преобразование $f(x^{(1)},...,x^{(p)})$, сохраняющее заданное соотношение порядка между анализируемыми параметрами, характеристики которых относительно хорошо известны экспертам, и обладающее тем свойством, что из $W_1>...>W_i>...>W_n$ (W_i - параметр, соответствующий i-му состоянию объекта контроля) с необходимостью следует $f(x_1) > f(x_2) > \ldots > f(x_n)$ и наоборот.

Известные методы агрегирования исходных параметров, развитые к настоящему времени, многочисленны и разнообразны [11].

Наиболее простым способом решения этой задачи является применение экспериментальных методов удельных весов агрегируемых параметров. Несмотря на их ограниченность, они широко используются вследствие своей простоты и доступности.

Вместе с тем, разнообразные параметры, обладают рядом особенностей, не позволяющих в большинстве случаев использовать традиционные процедуры оценивания интегрального показателя, реализуемые в рамках многомерного шкалирования, кластерного, дискриминантного и других методов анализа. К этим особенностям, прежде всего, следует отнести:

а) нечеткость оценок как самих исходных параметров объекта контроля, особенно для долгосрочного прогнозирования, так и характера их влияния на эффективность системы;

б) многомерный, разнородный характер агрегируемых параметров, выражаемых в общем виде множествами количественных и качественных оценок, строковыми образами, логическими конструкциями, предложениями естественного языка и т.п.;

в) иерархический или матричный характер взаимосвязи агрегируемых параметров. Прямым следствием указанных особенностей является нечеткость сравнительных оценок по анализируемому интегральному свойству.

Будем полагать, что агрегирование частных показателей объекта контроля имеет иерархическую структуру (см. рисунок 2), а составляющие ее компоненты образуют критериальное пространство.

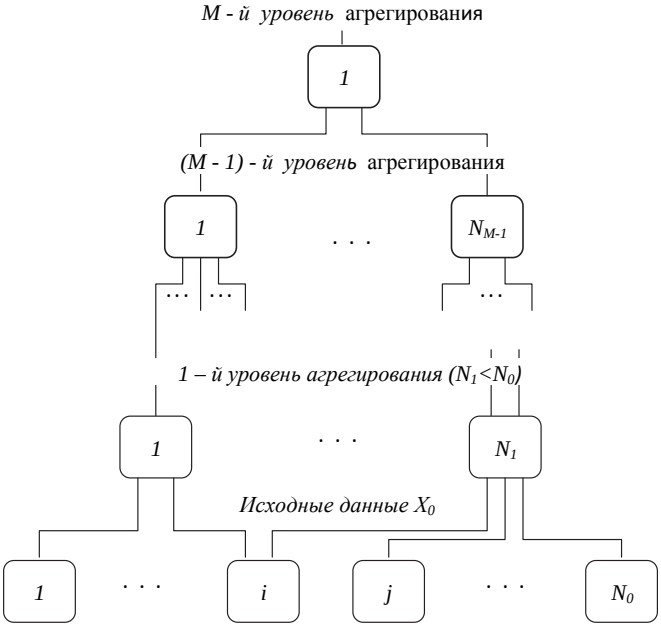


Рис. 2. Иерархическая структура показателей объекта контроля

Таким образом, возникает задача согласования отношений предпочтения при агрегировании показателей на множестве частных оценок их интегральных показателей.

4. Формальная постановка задачи агрегирования частных показателей и классификация показателей объекта контроля. Пусть результаты измерения некоторых показателей $x_{j,}\{\ j=\overline{1,n}\ \}$ в различных условиях обстановки $E=\{l_r,\ r=\overline{1,m}\ \}$ сведены в матрицу данных $X = ||x_{rj}||_{[m,n]}$, где n - количество групп показателей в матрице данных, m - количество измерений исследуемых показателей. Будем считать множество E выборкой статистических данных ограниченного объема из генеральной совокупности частных показателей, для которых известна степень выраженности показателей в целом, обладающая некоторыми вероятностными свойствами. Назовем множество E обучающей выборкой (ОВ). Практические исследования показывают, что однозначно утверждение о принадлежности ОВ к генеральной совокупности в виду ее малого объема оказывается не всегда корректным. Поэтому будем считать, что показатели x_{rj} из ОВ в общем случае измеряются нечетко и, следовательно, каждому показателю x_{rj} можно по-

ставить в соответствие функцию принадлежности $\mu_{rj}(x_{rj})$. Обозначим $\mu=||\mu_{rj}(x_{rj})||$.

Таким образом, результатам оценки частных показателей в конкретных условиях обстановки, представляемых вектор-строкой x_r матрицы X, ставится в соответствие вектор-строка μ_r матрицы μ. При этом $x_r \in k$, где k- n-мерное векторное пространство координат, координатные оси которого соответствуют исходным (частным) показателям x_j ($j = \overline{1,n}$).

Требуется синтезировать алгоритм, позволяющий на основании анализа и обработки данных, сформированной ОВ получать аналитическую модель обобщенного агрегированного показателя вида $W=f(x)$ ($f(x)\in F$, где F - заданное множество функций).

Показатель W называется шкалой. Шкала W определяет соотношение между интегральными показателями в конкретных условиях обстановки из множества E. Предполагается, что эти отношения оцениваются при помощи числовой функции, отражающей совокупность всех пар взаимных оценок из ОВ в матрицу коэффициентов связи между ними. Далее эта матрица определяется как матрица парных отношений Q.

Обозначим через $W = (W_1,...,W_m)$ вектор значений шкалы оценок из множества E и определим функцию $G(W_r, W_k)$ двух переменных, порождающую на любой допустимой шкале $f(x)\in F$ аппроксимирующее парное отношение вида: $d_{rk}(f)=G(f(x_r), f(x_k))$, $x_r, x_k \in k$.

Введем матрицу $D=||d_{rk}(f)||_{[m,n]}$. Кроме того, предположим, что на E определено аппроксимируемое парное отношение $Q_э = ||q_{rk}||_{[m,n]}$ и задан функционал $J(Q, D)$, оценивающий близость Q и D.

Проведенный анализ показал, что в качестве такого функционала наиболее целесообразно использовать выражение вида [9]:

$$J(Q,D) = \sum_{r,\,k} \left(q_{rk} - d_{rk}(f)\right)^2.$$

В этом случае задача синтеза алгоритма агрегирования частных показателей $A(X,\mu)$ состоит в том, чтобы среди допустимых шкал W измерения интегральной оценки $f(x)\in F$ найти такую, которая бы обращала в минимум функционал $J(Q,D)$:

$$W^* = \min_W J(Q,D),$$

позволяла бы классифицировать и оценивать показатели по совокупности частных показателей, не входящих в обучающую выборку.

При этом синтезируемый алгоритм должен удовлетворять ограничению:

$$P\left\{J(Q,D) \to \min;\ A\left(X,\mu\right)\right\} \le P_{доп},$$

где P – функционал потерь на идентификацию, т.е. на решение задачи $J(Q,D) \to \min$ с помощью алгоритма $A\left(X,\mu\right)$; $P_{доп}$ – задаваемые допустимые потери на идентификацию.

В качестве задаваемых потерь на идентификацию может использоваться время решения задачи идентификации, сложность формирования достоверной обучающей выборки и т.д. В конкретном случае под потерями на идентификацию будем понимать совокупное время, затрачиваемое на формирование достоверной обучающей выборки и построение с помощью алгоритма $A\left(X,\mu\right)$ модели обобщенного агрегированного показателя вида $W = f(x)$.

В общем виде задача классификации объектов, описываемых разнородными количественно-качественными признаками, состоит в том, чтобы качественные или порядковые отношения объектов ОВ преобразовать с достаточной определенностью в количественную метрическую пространственную структуру, отражающую в некотором приближении классификационные отношения.

При этом данные об объекте в виде случайной последовательности многомерных наблюдений, носящих в общем случае нечеткий и неоднородный характер. Известные статистические методы анализа в этом случае оказываются неприменимы по двум причинам: во-первых, из-за высокой вычислительной сложности алгоритмов при обработке больших объемов статистической информации; во-вторых, из-за недостаточной эффективности методов в условиях априорной неопределенности нестатистического порядка, когда нарушаются аксиомы классической вероятностной схемы и приходится искать новые постановки задач классификации. Особые возможности в этом плане открываются с использованием теории нечетких множеств. Нечеткие модели являются более гибкими по сравнению с четкими, поскольку в большей степени позволяют учитывать опыт и интуицию человека-специалиста в конкретных областях деятельности.

Задача классификации нечетко заданных образов объектов обычно рассматривается как задача формирования в конечном пространстве признаков эталонных образов обобщенных ситуаций. Отправной точкой при этом служит либо экспертная, либо статистическая информация в тех или иных условиях обстановки [12]. Для пред-

ставления разнородных параметров используется система решающих правил, полученных от экспертов и обучающая выборка, представляющие собой декларативные и процедурные знания. Формирование эталонных классов осуществляется либо на основе построения и решения системы предикатных уравнений, либо на основе определения системы функциональных отображений множества лингвистических значений признаков на соответствующие количественные шкалы.

6. Заключение. Задачи в вышеуказанной постановке (при наличии многомерной разнородной структуры нечетких исходных данных) не имеют строгого аксиоматического обоснования в рамках теории нечетких множеств. Сложность решения подобных задач связана в первую очередь не только с нечеткостью исходных данных, но и с не метрическим характером описания в обучающей выборке. Поэтому применение для этих целей алгоритма многомерной размытой классификации при наличии разнородных исходных данных оказывается также невозможным. Учитывая указанные особенности, синтез алгоритма и методики решения задачи агрегирования и классификации показателей целесообразно выполнить на основе совместного использования не метрических методов многомерного шкалирования и размытой нечеткой классификации.

Таким образом, для решения задачи идентификации состояний объекта контроля необходимо выполнить следующие шаги:

– ввод и подготовка исходных данных предварительной классификации;

– структуризация объектов обучающей выборки;

– расчет параметров классификационной шкалы;

– контроль достоверности непротиворечивости обучающей выборки;

– принятие решения о классификации объекта по значению функции принадлежности к одному из классов.

Литература

1. *Душкин Р.В.* Методы получения, представления и обработки знаний с НЕ – факторами // Библиотека оценщика LABRATE.RU. 2011. URL: http://www.labrate.ru/discus/messages/33870/dushkin_ne-factors_2011-36925.pdf (дата обращения: 13.11.2014).
2. *Нариньяни А.С.* Инженерия знаний и НЕ-факторы: краткий обзор-08 // Вопросы искусственного интеллекта. Вестник НСМИИ РАН. 2008. №1. С. 61–77.
3. *Нариньяни А.С.* Недоопределенность в системах представления и обработки знаний // Изв. АН СССР. Техн. кибернетика. 1986. № 5. С.42–54.
4. *Нариньяни А.С.* НЕ-факторы и инженерия знаний: от наивной формализации к естественной прагматике // Сборник трудов IV национальной конференции по Искусственному Интеллекту (КИИ-94). Рыбинск. 1994. Т. 1 С. 9–18.
5. *Душкин Р.В., Рыбина Г.В.* Об одном подходе к автоматизированному извлечению, представлению и обработке знаний с НЕ-факторами // Известия РАН. Теория и системы управления. 1999. № 5. С. 34–44.

6. *Шапот М.Д.* Вывод решений в условиях неопределенности в системе ЭКО // Экспертные системы на персональных компьютерах. Материалы семинара. М.: МДНТМ. 1989. С. 65–78.
7. *Нариньяни А.С.* НЕ-факторы: неоднозначность (до-формальное исследование) // Новости искусственного интеллекта. 2003. №№ 5–6. С. 123–130.
8. *Круглов В.В., Дли М.И., Голунов Р.Ю.* Нечеткая логика и искусственные нейронные сети: учебное пособие // М.: Издательство Физико-математической литературы. 2001. 256 с.
9. *Багрецов С.А., Львов В.М., Наумов В.В. и др.* Диагностика социально-психологических характеристик малых групп с внешним статусом // СПб.: Лань. Издательство Санкт-Петербургского Университета МВД России. 1999. 640 с.
10. *Берг Т.Н.* Нервно-психическая неустойчивость и способы ее выявления // Владивосток.: Мор. гос. ун-т им. адмирала Г.И. Невельского. 2005. 63 с.
11. *Брюхомицкий Ю.А.* Нейросетевые модели для систем информационной безопасности // Таганрог: ТГРТУ. 2005. 160 с.
12. *Горелик А.Л., Скрипкин В.А.* Методы распознавания // М.: Высшая школа. 1989. 232 с.

References

1. Dushkin R.V. [Methods for the preparation , submission and processing of knowledge NOT – factors]. *Biblioteka ocenshhika LABRATE.RU – Library of appraiser LABRATE.RU*. 2001. Available at: http://www.labrate.ru/discus/messages/33870/dushkin_ne-factors_2011-36925.pdf (accessed: 13.11.2014). (In Russ.).
2. Narinyani A.S. [Knowledge engineering and non- factors]. *Voprosy iskusstvennogo intellekta. Vestnik NSMII RAN – Questions of artificial intelligence. Vestnik NSMII RAN*. Moscow: *LENAND*. 2008. vol. 1. pp. 61–77. (In Russ.).
3. Narinyani A.S. [Underdetermined in systems of knowledge representation and processing]. *Izv. AN SSSR. Tehn. kibernetika – Proceedings of the Academy of Sciences of the USSR*. 1986. vol. 5. pp. 42–54. (In Russ.).
4. Narinyani A.S. [NON- factors and knowledge engineering: from the naive to the formalization of natural pragmatics]. *Sbornik trudov IV nacional'noj konferencii po Iskusstvennomu Intellektu* [Proceedings of the IV National Conference on Artificial Intelligence]. Rybinsk. 1994. vol. 1. pp. 9–18. (In Russ.).
5. Dushkin R.V., Rybin G.V. [An approach to automated extract, knowledge representation and processing with non- factors]. *Izvestija RAN. Teorija i sistemy upravlenija – Proceedings of the Academy of Sciences. Theory and control systems*. 1999. vol. 5. pp. 34–44. (In Russ.).
6. Shapot M.D. [Conclusion making under uncertainty in the IVF]. *Jekspertnye sistemy na personal'nyh komp'juterah. Materialy seminara – Expert systems on personal computers*. Moscow. 1989. pp. 65–78. (In Russ.).
7. Narinyani A.S. [NOT-factors: the ambiguity of (pre- formal study)]. *Novosti iskusstvennogo intellekta – News of artificial intelligence*. Moscow. 2003. no. 5–6. pp. 123–130. (In Russ.).
8. Kruglov V.V., Syntax M.I., Golunov R.Y. *Nechetkaja logika i iskusstvennye nejronnye seti: uchebnoe posobie* [Fuzzy logic and artificial neural network: textbook]. Moscow: Publisher Physical and mathematical literatury. 2001. 256 p. (In Russ.).
9. Bagrets S.A. Bagrecov S.A., L'vov V.M., Naumov V.V., et al. *Diagnostika social'no-psihologicheskih harakteristik malyh grupp s vneshnim statusom.* [Diagnosis of socio-psychological characteristics of small groups with an external status]. SPb.: Lan'. Izdatel'stvo Sankt-Peterburgskogo Universiteta MVD Rossii. 1999. 640 p. (In Russ.).
10. Berg T.N. *Nervno-psihicheskaja neustojchivost' i sposoby ee vyjavlenija* [Neuro-psychological instability and how to identify]. Vladivostok.: Mor. gos. un-t im. admirala G.I. Nevel'skogo. 2005. 63 p. (In Russ.).

11. Bryuhomitsky Y.A. *Nejrosetevye modeli dlja sistem informacionnoj bezopasnosti* [Neural network model for information security systems]. Taganrog: TGRTU. 2005. 160 p. (In Russ.).
12. Gorelik A.L., Skripkin V.A. *Metody raspoznavanija* [Recognition methods]. M.: Vysshaja shkola 1989. 232 p. (In Russ.).

Глыбовский Павел Анатольевич — к-т техн. наук, доцент кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: теория распознавания образов, теория информации. Число научных публикаций — 45. p_glybovsky@mail.ru; ул. Ждановская, д. 13, Санкт-Петербург, 197198; р.т.: +7(812) 237-19-60.

Glybovsky Pavel Anatolievich — Ph.D., associate professor of system for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: theory of pattern recognition; information theory. The number of publications — 45. p_glybovsky@mail.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812) 237-19-60.

Пилькевич Сергей Владимирович — к-т техн. наук, докторант кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: информационная безопасность, криптография, моделирование социальных систем. Число научных публикаций — 60. ambers@list.ru; ул. Ждановская, д. 13, Санкт-Петербург, 197198; р.т.: +7(812) 237-19-60.

Pilkevich Sergey Vladimirovich — Ph.D., doctoral student of system for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: information security, cryptography, modeling social systems. The number of publications — 60. ambers@list.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198; office phone: +7(812) 237-19-60.

Жолус Роман Борисович — к-т биол. наук, соискатель кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: информационная безопасность; моделирование социальных систем. Число научных публикаций — 10. p.glybovsky@yandex.ru; ул. Ждановская, д. 13, Санкт-Петербург, 197198; р.т.: +7(812) 237-19-60

Zholus Roman Borisovich — Ph.D., applicant of system for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: information security, modeling social systems. The number of publications — 10. p.glybovsky@yandex.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812) 237-19-60.

Пономарев Юрий Александрович — к-т техн. наук, доцент, заместитель начальника кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: методы анализа социально-психологических характеристик, теория нечетких множеств. Число научных публикаций — 35. yurij_1969_2011@mail.ru; ул. Ждановская, д. 13, Санкт-Петербург, 197198; р.т.: +7(812) 237-19-60.

Ponomarev Yuri Aleksandrovich — Ph.D., associate professor, deputy head of system for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: methods of analysis of the socio-psychological characteristics, fuzzy set theory. The number of publications — 35. yurij_1969_2011@mail.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812) 237-19-60.

РЕФЕРАТ

Глыбовский П.А., Пилькевич С.В., Жолус Р.Б., Пономарев Ю.А. **Многоуровневое представление разнородных нечетких параметров для идентификации состояний объекта контроля.**

Материальной и технологической базой информационного общества являются разнородные автоматизированные системы, на базе компьютерной техники, систем и сетей передачи данных. К числу важнейших систем подобного рода относятся современные объекты экономики и инфраструктуры, военно-технических и сложных социотехнических систем. Автоматизация повышает требования к квалификации персонала, а также увеличивает его ответственность. При этом ошибочные или намеренно деструктивные действия персонала способны привести к резко негативным, а порой и трагическим последствиям.

Для разрешения данных проблем целесообразно применять методы идентификации функционального состояния человека-оператора.

Статья посвящена вопросу разработки многоуровневого представления разнородных нечетких параметров. Показано место нечетких параметров в общей системе информационных НЕ-факторов, приведены примеры из области физиологии и медицины, иллюстрирующие иерархический характер структуры разнородных нечетких параметров. Рассматриваемый авторами подход требует формальной постановки задачи агрегирования частных показателей. В работе обосновано применение теории нечетких множеств для решения задачи классификации объектов, описываемых разнородными количественно-качественными признаками.

SUMMARY

Glybovsky P.A., Pilkevich S.V., Zholus R.B., Ponomarev Y.A. **Multilevel Representation of Heterogeneous Fuzzy Parameters for Identification of Object Control States.**

The material and technological base of the information society are heterogeneous automated systems based on computer technology, systems and data networks. The most important of such systems include modern economic facilities and infrastructure, military-technical and complex sociotechnical systems. Automation increases the requirements for staff qualification and responsibility. Erroneous or deliberately destructive actions of personnel can lead to negative and sometimes tragic consequences.

To resolve these problems, it is advisable to apply the identification methods of the operator's state.

The paper is devoted to development of multi-level representation of heterogeneous fuzzy parameters. The position of the fuzzy parameters in the system of information-factors, examples from physiology and medicine, illustrating the hierarchical nature of the structure of heterogeneous fuzzy parameters are presented. Considered by the authors approach requires a formal statement of the problem of aggregation of partial indices. In the work the use of fuzzy set theory for solving the problem of classification of objects described heterogeneous quantitative and qualitative traits is justified.

УДК 681.142

В. П. Бубнов, А. С. Еремин, С. А. Сергеев

ОСОБЕННОСТИ ПРОГРАММНОЙ РЕАЛИЗАЦИИ ЧИСЛЕННО-АНАЛИТИЧЕСКОГО МЕТОДА РАСЧЕТА МОДЕЛЕЙ НЕСТАЦИОНАРНЫХ СИСТЕМ ОБСЛУЖИВАНИЯ

Бубнов В.П., Еремин А.С., Сергеев С.А. **Особенности программной реализации численно-аналитического метода расчета моделей нестационарных систем обслуживания.**

Аннотация. В статье описывается численно-аналитический метод расчета моделей нестационарных систем обслуживания. Находится решение системы уравнений Чепмена — Колмогорова в аналитическом виде. Приводится алгоритм построения решения и особенности его программной реализации на языке Java. Также приводятся результаты сравнения времени работы и точности выходных данных метода со временем работы и точностью выходных данных численного метода типа Рунге — Кутты, который используется в Matlab для решения аналогичных задач.

Ключевые слова: нестационарные системы обслуживания, уравнения Чепмена — Колмогорова, численно-аналитический метод.

Bubnov V.P., Eremin A.S., Sergeev S.A. **Program Implementation of the Numerical-Analytical Method for Computation of Non-Stationary Service System Models.**

Abstract. A numerical-analytical method for non-stationary queueing systems models computation is presented. The solution of Chapman—Kolmogorov equations is found in the analytical form. The algorithm and its practical implementation with Java language are discussed. Computation time and results precision for the presented method and the Runge—Kutta type method used in Matlab are compared.

Keywords: non-stationary queueing systems, Chapman—Kolmogorov equations, numerical-analytical method

1. Введение. Отличительной чертой современных аппаратно-программных комплексов (АПК) является то, что при создании они, прежде всего, должны быть ориентированы на функционирование не только в нормальных, но и в критических (кризисных) условиях. Это обусловлено с одной стороны возрастанием угроз, вызванных техногенными, природными и человеческими факторами, а с другой — желанием использовать уже существующие АПК для решения новых более сложных задач. В рассматриваемых ситуациях мониторинг и прогнозирование должны сопровождаться целенаправленными процедурами реконфигурации структур (в общем случае, управления структурами) как самих АПК, так и систем управления (СУ) ими для обеспечения максимально допустимого уровня их работоспособности и пропускной способности. Для определения возможности реализации всех операций, связанных с технологическим циклом управления, на заданном временном интервале применяют математическое моделирование. Математической базой является теория массового обслужива-

ния (ТМО), позволяющая решать разнообразные задачи анализа и синтеза АПК путем определения технико-экономических показателей эффективности функционирования комплексов в целом при известных технических параметрах их элементов и рабочей нагрузке. Большинство авторов используют модели ТМО в предположении, что очередь заявок бесконечна, существует стационарный режим, а коэффициент загрузки не превышает единицы [1, 2]. Однако наибольший практический и теоретический интерес представляют модели нестационарных систем обслуживания, учитывающие поведение АПК в контуре управления технологическими процессами и объектами, функционирующими в условиях перегрузок на заданном (директивном) временном интервале. Этим объясняется появление в последнее время публикаций, связанных с исследованием поведения моделей ТМО в переходных режимах [3–7].

На основе результатов работ [8–11] разработан комплекс программ [12] расчета надежности и планирования испытаний программных средств, в котором системы обыкновенных дифференциальных уравнений (ОДУ) для различных моделей нестационарных систем обслуживания решаются с помощью численных методов. Популярным программным инструментом, например, является Matlab, предлагающий несколько процедур для решения систем ОДУ. Основными недостатками традиционных численных методов являются накапливаемая на каждом шаге интегрирования погрешность и время работы алгоритма. Причем, вычислительная погрешность может привести и к отсутствию физического смысла получаемого решения.

В частности, мы использовали для решения систем, которые будут описаны в следующем разделе, процедуру ode45 из пакета Matlab (при настройках по умолчанию), основанную на паре вложенных методов Рунге — Кутты порядков 4 и 5, разработанных Э. Фельбергом [13]. Глобальная погрешность этой процедуры имеет порядок $O(h^5)$, где h — максимальная величина шага, в данном случае, по времени. Положив число заявок на обслуживание равным 100 (что дает 5151 дифференциальное уравнение в системе Чепмена — Колмогорова), выбрав интенсивность поступления всех заявок 1, а интенсивность обработки 2, мы получили, что многие состояния имели отрицательную вероятность, в частности, вероятность состояния номер 5087 стала $-9{,}27196448052287 0 \cdot 10^{-9}$. Повышение же точности расчетов значительно увеличивает время работы программы.

В то же время, желание учета большего числа факторов реальных процессов, подлежащих моделированию, приводит к увеличению числа уравнений Чепмена — Колмогорова относительно вероятностей

состояний. Время численного решения такого рода систем уравнений, как показывают эксперименты, экспоненциально зависит от общего числа состояний систем обслуживания. Это накладывает серьезные ограничения на разрабатываемые модели нестационарных систем обслуживания.

Высказанные соображения свидетельствуют об актуальности разработки альтернативных методов расчета вероятностей состояний нестационарных систем обслуживания с конечным источником (НСО), рассматриваемых в настоящей работе.

Нами был разработан численно-аналитический подход к решению возникающих в НСО дифференциальных уравнений, пресдтавленный в данной статье.

2. Суть численно-аналитического метода решения систем дифференциальных уравнений. Суть численно-аналитического метода представлена на модели НСО. На вход последовательно поступает N запросов на обработку. Распределения временных интервалов между моментами поступления запросов описываются экспоненциальными законами с интенсивностями $\{\lambda_1, \lambda_2, \dots, \lambda_N\}$, где λ_i соответствует i-й поступающей заявке. Считаем, что система не имеет потерь. Закон распределения времен обслуживания тоже экспоненциальный с интенсивностями $\{\mu_1, \mu_2, \dots, \mu_N\}$, где μ_j соответствует j-й обслуживаемой заявке.

Состояния системы в каждый момент времени характеризуются числом находящихся в системе запросов $i = \overline{0, N}$ и числом уже получивших обслуживание запросов $j = \overline{0, N-i}$. Вероятности пребывания системы в этих состояниях обозначается через $P_{i,j}(t)$. Их общее число $K = (N+1)(N+2)/2$. На рис. 1 представлена диаграмма переходов между состояниями системы.

Для определения распределения вероятностей нахождения системы обслуживания в состояниях (i, j) необходимо решить относительно $P_{i,j}(t)$ систему ОДУ, каждое из которых выглядит как

$$\begin{aligned}\dot{P}_{i,j}(t) = u(i)\left(\lambda_{i+j}P_{i-1,j}(t) - \mu_{j+1}P_{i,j}(t)\right) + \\ + u(j)\mu_j P_{i+1,j-1}(t) - u(N-i-j)\lambda_{i+j+1}P_{i,j}(t).\end{aligned} \quad (1)$$

Здесь $u(t)$ — функция Хевисайда, заданная как

$$u(t) = \begin{cases}1, & t > 0,\\ 0, & t \le 0.\end{cases} \quad (2)$$

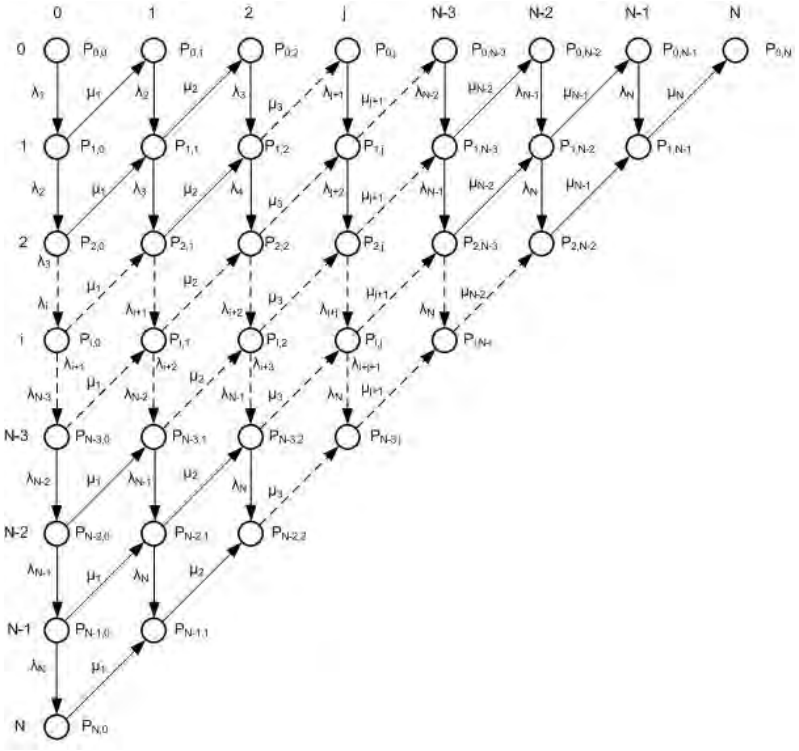


Рис. 1. Диаграмма переходов между состояниями НСО

В качестве начальных условий выбирают обычно нахождение в состоянии $(0, 0)$, то есть

$$P_{i,j}(0) = 1 - u(i + j). \tag{3}$$

Получаемое решение позволяет затем найти вероятности нахождения в системе i запросов, ожидаемое число запросов, вероятность обслуживания всех или не менее некоторого числа поступивших запросов и другие интересующие управленца характеристики.

Алгоритм нумерации состояний НСО. Рассмотренная выше система ОДУ (1) является линейной однородной системой уравнений. Она может быть представлена в матричной форме:

$$\dot{x}(t) = \mathbf{A}x(t), \tag{4}$$

где $x(t)$ — вектор неизвестных функций размерности K, а $\mathbf{A}$ — квадратная матрица.

Для указанной системы существует явное аналитическое решение, если только известны собственные числа матрицы **A**. Очевидным является тот факт, что в случае треугольного вида матрицы **A** (для определенности будем считать ее нижнетреугольной) ее собственные числа выписаны в явном виде на диагонали. Таким образом, аналитическое решение системы вида (4) можно легко найти, если только матрица **A** — треугольная.

Если пронумеровать состояния по возрастанию числа обработанных запросов, а внутри этих групп по возрастанию числа поступивших запросов:

(i,j)	$(0,0)$	$(1,0)$	...	$(N,0)$	$(0,1)$	...	$(N-1,1)$	...	$(0,N)$
k	1	2	...	$N+1$	$N+2$	...	$2N+1$	...	$(N+1)(N+2)/2$

то ни одно из состояний полученного списка не будет иметь зависимости от последующих. На графе это будет выглядеть как нумерация сверху вниз с перемещением по столбцам слева направо. Соответственно, полученная матрица **A** системы (4) будет нижнетреугольной.

Перепишем систему (4), учитывая треугольность матрицы **A**:

$$\begin{cases} \dfrac{dx_1}{dt} = a_{11}x_1, \\ \dfrac{dx_2}{dt} = a_{21}x_1 + a_{22}x_2, \\ \cdots \\ \dfrac{dx_i}{dt} = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{ii}x_i, \\ \cdots \\ \dfrac{dx_K}{dt} = a_{K1}x_1 + a_{K2}x_2 + \cdots + a_{KK}x_K. \end{cases}, \tag{5}$$

где a_{ij} — интенсивность перехода из состояния с номером j в состояние с номером i (в векторе $x(t)$).

Решение системы ОДУ. Решение системы (5) разбивается на последовательное решение скалярных уравнений, первое из которых будет однородным, а все последующие будут включать в себя решения предыдущих уравнений в качестве неоднородности. Это позволяет сформулировать следующий алгоритм нахождения решения.

Решением первого уравнения (5) очевидно является

$$x_1(t) = x_1(0)e^{a_{11}t}, \tag{6}$$

и ему соответствует фундаментальное решение $\tilde{x}_1(t) = e^{a_{11}t}$.

Предположим, что решения первых $i-1$ уравнений найдены в форме:

$$x_j(t) = \sum_{w=1}^{j} k_{jw}\tilde{x}_w(t), \quad j = \overline{1, \iota - 1}, \tag{7}$$

причем $\tilde{x}_j(t) = t^{v_j-1}e^{a_{jj}t}$, где v_j — кратность собственного числа a_{jj} в системе первых j уравнений. Тогда, после подстановки (7) в i-е уравнение системы (5), последнее можно записать в виде:

$$\frac{dx_i}{dt}(t) = a_{ii}x_i(t) + \sum_{j=1}^{i-1} b_{ij}\tilde{x}_j(t), \tag{8}$$

где $b_{ij} = \sum_{w=j}^{i-1} a_{iw}k_{wj}$. Решение (8) будет иметь вид

$$x_i(t) = \sum_{j=1}^{i} k_{ij}\tilde{x}_j(t), \quad x_i(t) = t^{v_j-1}e^{a_{ii}t}. \tag{9}$$

Пусть a_{ii} — собственное число, кратность которого в системе первых i уравнений равна v_i. Собственные числа $a_{i_1i_1} = a_{i_2i_2} = \cdots = a_{i_{v_i}i_{v_i}}$, $i_{v_i} = i$, пронумерованы в порядке нахождения на диагонали матрицы A. Тогда

$$k_{ii_{v_i}} = \frac{b_{ii_{v_i-1}}}{v_i}, \qquad v_i > 1. \tag{10}$$

Коэффициенты k_{ij} при тех $\tilde{x}_j(t)$, для которых $a_{ii} \neq a_{jj}$:

$$k_{ij} = \begin{cases} \frac{b_{ij} - k_{iw}(v_j - 1)}{a_{jj} - a_{ii}}, & v_j > 1, \\ \frac{b_{ij}}{a_{jj} - a_{ii}}, & v_j = 1. \end{cases} \tag{11}$$

где w такая, что $a_{ww} = a_{jj}$ и $v_w = v_j - 1$.

После нахождения всех коэффициентов (10) и (11), через начальные данные найдем оставшиеся:

$$k_{ii_1} = x_i(0) - \sum_{\substack{j=1 \\ v_j=0}}^{i-1} k_{ij}. \tag{12}$$

Следует отметить, что нахождение решения системы ОДУ в данном случае, в отличие от численного метода, дающего конечный набор точек, представляет собой построение процедуры, позволяющей определить вероятности состояний НСО в произвольный момент времени. Это, во-первых, дает возможность вывести решение ОДУ с произвольной степенью детальности, а во-вторых, скорость нахождения решения в любой сколь угодно удаленный момент времени одинакова и не требует расчета многих предыдущих временных состояний, как это потребовалось бы численному методу, имеющему к тому же и методическую погрешность, оценка которой дополнительно увеличивает сложность решения.

3. Особенности программной реализации метода. Описанный в разделе 2 метод был реализован на объектно-ориентированном языке программирования Java. Первая версия реализации данного метода значительно выигрывала в скорости у Matlab. В таблице 1 приведено сравнение времени работы методов. Для всех заявок были установлены интенсивности поступления $\lambda = 1$ и обработки $\mu = 2$. Рассчитывались вероятности состояний при $t = 100$.

Таблица 1. Сравнение времени работы методов

Количество заявок (N)	Время расчета на Java, мс	Время расчета в Matlab, мс
3	1	24
5	3	29
10	21	49
15	22	60

Тестирование метода при больших N показало, что используемая реализация непригодна к практическому применению, в связи с появляющейся погрешностью. Это объясняется особенностями хранения чисел с плавающей точкой чисел в памяти ЭВМ. Стандартный тип хранения таких данных в Java — тип double, размерность которого равна 64 бита. На всех этапах алгоритма происходит округление переменных, вследствие чего происходит накопление погрешности и при больших N итоговая погрешность становится неприемлемо высокой.

Способ борьбы с погрешностью вычислений. Для решения данной проблемы было принято решение использовать числа с практически неограниченной разрядностью, реализованные в классе BigDecimal [14]. Эти числа представляют собой сочетание двух значений. Первое — неограниченное значение строкового типа (String, s), для хранения мантиссы числа, второе — 32-битное целое число (Integer, I), в котором хранится десятичный показатель. Таким образом, значение числа типа BigDecimal представляется в виде: $s \cdot 10^I$.

Для контроля погрешности в программу была добавлена возможность задания точности чисел, т. е. определения числа разрядов в мантиссе. Необходимо учитывать тот факт, что повышение точность хранения чисел приводит к увеличению времени на совершение арифметических операций над ними, и, соответственно, к увеличению времени, требуемого для нахождения решения системы.

В классе BigDecimal реализованы все необходимые в аналитическом методе арифметические операции кроме вычисления экспоненты. Данная функциональность была реализована в ходе разработки; в ее основе лежит ряд Тейлора

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}. \quad (13)$$

После реализации алгоритма с числами типа BigDecimal, его точность, но, к сожалению, и время работы значительно возросли. Так, например, при $N = 100$, $\lambda = 1$, $\mu = 2$ с использованием точности чисел в 1000 знаков расчет вероятностей состояний занимал около полутора часов до проведения оптимизация программной реализации.

Оптимизация реализации численно-аналитического метода. В ходе анализа времени работы алгоритма было выяснено, что основное время занимает расчет коэффициентов k по формулам (10)–(12). Для ускорения этой части программы было сделано несколько изменений в коде.

1) Изначально при вычислении коэффициентов по (11) выполнялся цикл от $j = 0$ до $j = i$. При такой реализации, при очередном j, таком, что $\nu_j > 1$, приходилось пересчитывать все предыдущие k_{iw}, для которых $a_{ww} = a_{jj}$. Это приводило к многократному пересчету одних и тех же значений и значительно увеличивало время работы программы. После оптимизации цикл стал выполняться от $j = i$ к $j = 0$. Таким образом, каждое значение k вычисляется только один раз.

2) Было установлено, что большинство элементов матрицы **A** равны 0, поэтому в (8) было добавлено условие:

$$b_{ij} = \sum_{w=j}^{i-1} a_{iw} k_{wj}\,, a_{iw} \neq 0, \quad (14)$$

что позволило значительно сократить время работы алгоритма, за счет отбрасывания операций, не влияющих на результат.

3) Изначально в программе выделалась оперативная память для хранения всех значений b, но было замечено, что при вычислении значений k_{ij}, используются только значения b_{is}, с тем же первым индексом i. Было принято решение выделять память только для хранения набора коэффициентов b_{ij} при фиксированном i, а при переходе к вычислению значений при новом i освобождать использованную память. Такая оптимизация позволила сократить требуемый размер памяти для хранения коэффициентов b в $(N+1)(N+2)/2$ раз и, как следствие, увеличить скорость работы программы.

4) Большая часть алгоритма может выполняться в многопоточном режиме, поэтому были определены точки, в которых потоки должны синхронизироваться, и реализована многопоточная структура алгоритма. Этими точками при вычислении k для любого i являются:

а) Окончание расчета коэффициентов b_{ij} (14),

б) Окончание расчета коэффициентов k_{ij}, для которых $a_{ii} = a_{jj}$ и $\nu_j > 1$ (10) и для которых $a_{ii} \neq a_{jj}$ (11).

в) Окончание расчета оставшихся коэффициентов k_{ij} (11), (12), выполняющийся в один поток вычислений.

Кроме того была проведена оптимизация расчета вероятностей состояний при вычисленных коэффициентах k:

1) Из формулы 7 видно, что значения $\tilde{x}_j(t)$ для двух собственных чисел таких, что $a_{i_j i_j} = a_{i_{j+1}, i_{j+1}}$, будут удовлетворять уравнению $\tilde{x}_{i_{j+1}}(t) = t\tilde{x}_{i_j}(t)$. Таким образом, при использовании этого уравнения в (7), удается значительно сократить время работы алгоритма.

Было замечено, что при вычислении вероятностей состояний на промежутке времени от t_1 до t_2 с шагом h в (7) целесообразно сохранять значения экспоненты в отдельный вектор E длиной K. Действительно, если значения экспоненты для момента времени t_1 сохранены, тогда для вычисления вероятностей состояний в момент времени $t_1 + h$ можно воспользоваться выражением $\tilde{x}_j(t+h) = t^{\nu_j - 1} e^{a_{jj}h} E_j$. Это значительно уменьшило время работы алгоритма.

Алгоритм вычисления вероятностей состояний по (7) также был разделен на потоки.

В результате внесения приведенных выше изменений, удалось добиться существенного ускорения работы программы при повышенной точности расчетов. В разделе 5 представлено сравнение скорости с Matlab.

4. Оценка точности метода. Одним из способов проверки точности работы метода является суммирование вероятностей всех состояний в какой-либо момент времени, так как суммарная вероятность всегда

остается равной 1. В рассматриваемой модели НСО для всех заявок были установлены интенсивности поступления $\lambda = 1$ и обработки $\mu = 2$, число заявок взято $N = 100$, точность чисел — 1000 знаков. Рассчитывались вероятности состояний при $t = 50$. Сумма всех вероятностей состояний, рассчитанных численно-аналитическим методом составила $1 + 616856 \cdot 10^{-678}$. При этом, ни одна вероятность не была отрицательной. В Matlab сумма всех состояний была равна 1, но были состояния, вероятность которых меньше нуля, в частности состояние номер 5087 имело вероятность $-9{,}271964480522870 \cdot 10^{-9}$.

Для дополнительной проверки точности на Java был реализован «классический» метод Рунге — Кутты четвертого порядка с постоянным шагом. В таблице 2 приведены значения вероятности поглощающего состояния с номером 5150 при $t = 50,\ 100,\ 150$. Интенсивность поступления заявок $\lambda = 1$, интенсивность обработки $\mu = 2$, $N = 100$. Шаг по времени в методе Рунге — Кутты обозначен h.

Таблица 2. Значения состояния 5150, вычисленные разными методами

	$t = 50$	$t = 100$	$t = 150$
Matlab	$4{,}24408126 \cdot 10^{-8}$	0,47343**746**	0,9999919**7951**
Аналитический метод	$2{,}24023344 \cdot 10^{-11}$	0,47343**780**	0,9999919**9164**
Метод Рунге — Кутты ($h = 0.4$)	$3{,}64428442 \cdot 10^{-11}$	0,47343**753**	0,9999919**9068**
Метод Рунге — Кутты ($h = 0.2$)	$2{,}23763751 \cdot 10^{-11}$	0,47343**778**	0,9999919**9158**

Из таблицы видно, что чем h меньше, тем ближе значение вероятности к результату, полученному аналитическим методом и наоборот, чем шаг больше, тем значение ближе к значению, полученному с использованием Matlab.

5. Сравнительная оценка скорости работы программной реализации метода. Был проведен эксперимент по сравнению скорости работы метода с Matlab. Параметры модели брались теми же, что и в предыдущем пункте. В таблице 3 приведено время работы метода и Matlab при расчете вероятностей состояний в различные моменты времени T, с учетом времени расчета коэффициентов k.

Таблица 3. Сравнение времени расчета вероятностей

	Нахождение решения в $T = 50$, с	Нахождение решения в $T = 100$, с	Нахождение решения в $T = 150$, с	Нахождение решения в $T = 200$, с
Matlab	8,370605	14,19324	20,578149	25,971104
Аналитический метод	55,961	59,98	58,637	61,616

Особенность нашего подхода такова что, рассчитав значения коэффициентов k, можно получить значения вероятностей состояний в

любой момент времени. Поэтому был проведен еще один эксперимент с теми же исходными данными, в котором аналитический метод использовал для расчета вероятностей заранее сохраненные значения коэффициентов k. Результаты эксперимента приведены в таблице 4.

Таблица 4. Сравнение времени расчета вероятностей при использовании уже найденных k

	Нахождение решения в $T = 50$, с	Нахождение решения в $T = 100$, с	Нахождение решения в $T = 150$, с	Нахождение решения в $T = 200$, с
Matlab	8,370605	14,19324	20,578149	25,971104
Аналитический метод	4,782	04,298	04,673	04,457

В третьем эксперименте проверялось влияние размерности чисел на скорость работы алгоритма. Интенсивность поступления заявок $\lambda = 1$, интенсивность обработки заявок $\mu = 2$, количество заявок $N = 100$, момент времени $T = 100$. При 500 знаках расчет занимает 58,086 с, а при 1000 — 59,980 с.

Из таблиц 3 и 4 видно, что наш метод тратит почти одинаковое время, независимо от момента T, для которого необходимо произвести расчет; кроме того, рассчитав и сохранив матрицу коэффициентов k (трудоемкий, но однократный процесс), можно получать вероятности состояний для любого момента времени намного быстрее по сравнению с MatLab.

Таким образом, рекомендуется использовать предложенный метод для решения класса задач, описанных во введении. Как видно из результатов, при определенных условиях, он значительно превосходит численные методы (на примере методов Рунге — Кутты) по скорости.

Литература

1. *Osogami T., Raymond R.* Analysis of transient queues with semidefinite optimization // Queueing Systems, 2013. vol. 73. pp. 195–234.
2. *Wolff R. W., Yao Y.-C.* Little's law when the average waiting time is infinite // Queueing Systems, 2014. vol. 76. pp. 267–281.
3. *Sudhesh R., Vijayashree K. V.* Stationary and transient analysis of M/M/1 G-queues // Int. J. of Mathematics in Operational Research, 2013. vol. 5. no. 2. pp. 282–299.
4. *Sudhesh R., Francis Raj L.* Stationary and transient solution of Markovian queues — an alternate approach // Int. J. of Mathematics in Operational Research, 2013. vol. 5. no. 3. pp. 407–421.
5. *Czachórski T., Nycz M., Nycz T., Pekergin F.* Analytical and numerical means to model transient states in computer networks // Computer Networks. Proceedings of the 20th International Conference, CN 2013. Springer Communications in Computer and Information Science, 2013. vol. 370. pp. 426–435.
6. *Wei Y., Yu M., Tang Y., Gu J.* Queue size distribution and capacity optimum design for N-policy Geo(λ1,λ2,λ3)/G/1 queue with setup time and variable input rate // Mathematical and Computer Modelling, 2013. vol. 57. no. 5–6. pp. 1559–1571.

7. *Бубнов В. П., Тырва А. В., Еремин А. С.* Комплекс моделей нестационарных систем обслуживания с распределениями фазового типа // Труды СПИИРАН, 2014. № 6(37), С. 61–71.
8. *Бубнов В. П., Сафонов В. И., Смагин В. Л.* О загрузке вычислительной системы с изменяющейся интенсивностью поступления заданий // Автоматика и вычислительная техника, 1987. № 6, С. 19–22.
9. *Бубнов В. П., Тырва А. В., Хомоненко А. Д.* Обоснование стратегии отладки программ на основе нестационарной модели надежности // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета, 2010. № 2(97), С. 85–92.
10. *Bubnov V. P., Tyrva A. V., Khomonenko A. D.* Model of reliability of the software with Coxian distribution of length of intervals between the moments of detection of errors // Proceedings of 34th Annual IEEE Computer Software and Applications Conference (COMPSAC 2010), 2010. pp. 238–243.
11. *Bubnov V. P., Khomonenko A. D., Tyrva A. V.* Software Reliability Model with Coxian Distribution of Length of Intervals Between Errors Detection and Fixing Moments // Proceedings of 35th Annual IEEE Computer Software and Applications Conference (COMPSAC 2011), Munich, 18–22 July 2011. pp. 310–314.
12. *Тырва А. В., Хомоненко А. Д., Бубнов В. П.* Комплекс программ расчета надежности и планирования испытаний программных средств // Федеральная служба по интеллектуальной собственности, патентам и товарным знакам. Свидетельство о государственной регистрации программ для ЭВМ № 2010615617. Москва, 2010.
13. *Fehlberg E.* Low-order classical Runge—Kutta formulas with step size control and their application to some heat transfer problems // NASA Technical Report 315 (1969), extract published in Computing, 1970. vol. 6, no. 1–2. pp. 61–71.
14. Class BigDecimal. Java™ Platform, Standard Edition 7. Application Programming Interface (API) Specification // URL: http://docs.oracle.com/javase/7/docs/api/java/math/BigDecimal.html (дата обращения 10.02.2015).

References

1. Osogami T., Raymond R. Analysis of transient queues with semidefinite optimization. Queueing Systems, 2013. vol. 73. pp. 195–234.
2. Wolff R.W., Yao Y.-C. Little's law when the average waiting time is infinite. Queueing Systems, 2014. vol. 76. pp. 267–281.
3. Sudhesh R., Vijayashree K. V. Stationary and transient analysis of M/M/1 G-queues. Int. J. of Mathematics in Operational Research, 2013. vol. 5. no 2. pp. 282–299.
4. Sudhesh R., Francis Raj L. Stationary and transient solution of Markovian queues — an alternate approach. Int. J. of Mathematics in Operational Research, 2013. vol. 5. no. 3. pp. 407–421.
5. Czachórski T., Nycz M., Nycz T., Pekergin F. Analytical and numerical means to model transient states in computer networks. Computer Networks. Proceedings of the 20th International Conference, CN 2013, Lwówek Śląski, Poland, June 17–21, 2013 / Springer Communications in Computer and Information Science, 2013. vol. 370. pp. 426–435.
6. Wei Y., Yu M., Tang Y., Gu J. Queue size distribution and capacity optimum design for N-policy Geo(λ1,λ2,λ3)/G/1 queue with setup time and variable input rate. Mathematical and Computer Modelling, 2013. vol. 57. no. 5–6. pp. 1559–1571.
7. Bubnov V.P., Tyrva A.V, Eremin A.S. [A set of non-stationary queuing system models with phase-type distributions]. *Trudy SPIIRAN – SPIIRAS Proceedings*, 2014. vol. 6(37), pp. 61–71. (In Russ.)

8. Bubnov V.P., Safonov V.I., Smagin V.A. [The load of a computational system with varying customer arrival rate]. *Avtomatika i Vychislitel'naya Tekhnika – Automation and Computer Engineering.* 1987. vol. 6. pp. 19–22. (In Russ.).
9. Bubnov V.P., Tyrva A.V., Khomonenko A.D. [Software debugging strategy based on a non-stationary reliability model]. *Nauchno-tehnicheskie vedomosti Sankt-Peterburgskogo gosudarstvennogo politehnicheskogo universiteta – St. Petersburg State Polytechnical University Journal*, 2010. vol. 2(97), pp. 85–92.
10. Bubnov V.P., Tyrva A.V., Khomonenko A.D. Model of reliability of the software with Coxian distribution of length of intervals between the moments of detection of errors. Proceedings of 34th Annual IEEE Computer Software and Applications Conference (COMPSAC 2010), 2010. pp. 238–243.
11. Bubnov V.P., Khomonenko A.D., Tyrva A.V. Software Reliability Model with Coxian Distribution of Length of Intervals Between Errors Detection and Fixing Moments. Proceedings of 35th Annual IEEE Computer Software and Applications Conference (COMPSAC 2011), Munich, 18–22 July 2011. pp. 310–314.
12. Tyrva A.V., Khomonenko A.D., Bubnov V.P. [The program complex for software reliability computation and tests planning]. Russian Federal Service for Intellectual Property (Rospatent). Certificate of the state registration of a computer program No. 2010615617. Moscow, 2010. (In Russ.).
13. Fehlberg E. Low-order classical Runge—Kutta formulas with step size control and their application to some heat transfer problems. NASA Technical Report 315 (1969), extract published in Computing vol. 6, no. 1–2, 1970, pp. 61–71.
14. Class BigDecimal. Java™ Platform, Standard Edition 7. Application Programming Interface (API) Specification. Available at: http://docs.oracle.com/javase/7/docs/api/java/math/BigDecimal.html (Accessed: 10.02.2015).

Бубнов Владимир Петрович — д-р техн. наук, профессор кафедры информационных и вычислительных систем факультета автоматизации и интеллектуальных технологий, Петербургский государственный университет путей сообщения императора Александра I (ПГУПС). Область научных интересов: вероятностные модели аппаратно-программных комплексов, марковские процессы, дифференциальные уравнения. Число научных публикаций — 150. bubnov1950@yandex.ru, http://www.pgups.ru; Московский пр., д. 9, г. Санкт-Петербург, 190031, РФ; р.т.: +79052807904, Факс: +7(812)457-8606.

Bubnov Vladimir Petrovish — Ph.D., Dr. Sci., professor of informatics and computer systems department, Petersburg state transport university. Research interests: probabilistic models of hardware and software complexes, Markovian processes, differential equations. The number of publications — 150. bubnov1950@yandex.ru, http://www.pgups.ru; Moskovsky pr., 9, Saint-Petersburg, 190031, Russian Federation; office phone: +79052807904, Fax: +7(812)457-8606.

Еремин Алексей Сергеевич — к-т техн. наук, доцент кафедры информационных систем факультета прикладной математики — процессов управления, Санкт-Петербургский государственный университет (СПбГУ). Область научных интересов: численные методы решения дифференциальных уравнений, уравнения с запаздывающих аргументом, вероятностные модели. Число научных публикаций — 13. ereminh@gmail.com, http://www.spbu.ru; Университетский пр. 35, Петергоф, г. Санкт-Петербург, 198504, РФ; р.т.: +7(812)428-7159, Факс: +7(812)428-7159.

Eremin Alexey Sergeevich — Ph.D., associate professor of information systems department of the Faculty of Applied Mathematics and Control Processes, Saint-Petersburg State University. Research interests: numerical solution of differential equations, delay differential equations,

probabilistic models. The number of publications — 13. ereminh@gmail.com, http://www.spbu.ru; Universitetskii prospekt 35, Petergof, Saint-Petersburg, 198504, Russian Federation; office phone: +7(812)428-7159, Fax: +7(812)428-7159.

Сергеев Сергей Александрович — аспирант кафедры информационных и вычислительных систем факультета автоматизации и интеллектуальных технологий, Петербургский государственный университет путей сообщения императора Александра I (ПГУПС). Область научных интересов: настационарные системы массового обслуживания, программные комплексы. Число научных публикаций — 12. serega_svetl@mail.ru; Московский пр., д. 9, г. Санкт-Петербург, 190031, РФ; р.т.: 8(911)959-53-25.

Sergeev Sergei Aleksandrovich — Ph.D. student of the informatics and computer systems department, Petersburg State Transport University. Research interests: non-stationary queueing systems, software complexes. The number of publications — 12. serega_svetl@mail.ru; Moskovsky pr., 9, Saint-Petersburg, 190031, Russian Federation; office phone: 8(911)959-53-25.

Поддержка исследований. Работа выполнена при финансовой поддержке РФФИ (гранты № 13-07-00279, 13-08-00702, 13-08-01250, 13-06-00877, 13-07-12120-офи-м), Программы фундаментальных исследований ОНИТ РАН (проект No2.11)

Acknowledgements. This research is partially supported by the RFBR (grants 13-07-00279, 13-08-00702, 13-08-01250, 13-06-00877, 13-07-12120-офи-м), and by the fundamental scientific research support ONITRAS Project No. 2.11.

РЕФЕРАТ

Бубнов В. П., Еремин А. С., Сергеев С. А. **Особенности программной реализации численно-аналитического метода расчета моделей нестационарных систем обслуживания.**

В статье описывается численно-аналитический метод расчета моделей нестационарных систем обслуживания (НСО). В отличие от традиционных моделей, они позволяют моделировать процессы обслуживания на заданном временном интервале при общих предположениях о законах распределения временных интервалов между поступлениями и обслуживаниями заявок. Важным в этом случае становится решение системы уравнений Чепмена — Колмогорова.

Рассматривается способ нумерации уравнений, позволяющий найти решение в аналитическом виде, как стационарной однородной системы линейных обыкновенных дифференциальных уравнений (ОДУ) с нижнетреугольной матрицей.

Приводится алгоритм построения решения и особенности его программной реализации на языке Java. Обсуждаются вопросы повышения скорости расчетов и точности путем использования чисел типа BigDecimal.

Проводится сравнение эффективности предлагаемого подхода с результатами расчетов в комплексе MatLab, в котором реализовано решение систем ОДУ численными методами типа Рунге — Кутты.

SUMMARY

Bubnov V.P., Eremin A.S., Sergeev S.A. **Program Implementation of the Numerical-Analytical Method for Computation of Non-Stationary Service System Models.**

Numerical-analytical method for solving non-stationary queueing systems (NQS) is presented. Such models describe the processes of customers servicing in the specified time interval under general assumptions on the time distribution between customer arrival and service. The Chapman—Kolmogorov equations solution becomes important in this case.

The equations are numerated so, that the solution can be found analytically, as a solution of a stationary homogeneous system of linear ordinary differential equations (ODEs), which has a lower triangular matrix.

The algorithm of the solution computation and its implementation peculiarities with Java language are described. Computation time and precision improvements with using of the BigDecimal type are discussed.

The efficiency of the approach is compared to results of computation in MatLab, where ODEs are solved with Runge—Kutta type methods.

УДК 004.056.57

В.В. Ковалев, Р. И. Компаниец, В.А. Новиков

ВЕРИФИКАЦИЯ ПРОГРАММ НА ОСНОВЕ СООТНОШЕНИЙ ПОДОБИЯ

Ковалев В.В., Компаниец Р.И., Новиков В.А. **Верификация программ на основе соотношений подобия.**

Аннотация. Описывается подход к статической верификации исполняемых программ на основе сопоставления семантических аспектов вычислений, позволяющий построить паспорт программы. Паспорт, как результат статической верификации, может быть использован для создания среды контролируемого выполнения программ (динамической верификации реально выполняемых программ, прошедших статическую верификацию).

Ключевые слова: верификация, управляющий граф, абстрактные размерности, определяющие отношения, подобие.

Kovalev V.V., Kompanietc R. I., Novikov V.A. **Verification of Programs Based on Similarity Relations.**

Abstract. The static verification method of programs based on comparison of the semantic aspects of computing, that allows to build a program passport is described. Passport as a result of the static verification may be used to create an environment of the controlled program run (dynamic verification of the really running programs, which have passed static verification).

Keywords: verification, control graph, abstract dimensions, determinant relations, similarity.

1. Введение. Целью верификации программ, в отличие от отладки, является выявление ошибок и условий их возникновения. Кроме того, верификация - контролируемый и управляемый процесс, трудоемкость которого определяется используемым методом с предопределенным в нем объемом работ. Предлагаемый метод для получения абстрактной интерпретации состояний программы использует положения теории размерностей, а для их анализа на непротиворечивость – положения теории подобия. Получаемые в процессе символьной интерпретации критерии подобия объединяются в систему линейных однородных уравнений (СЛОУ), которая и ее решение служат паспортом программы. Опираясь на паспорт можно с помощью сопроцессора контролировать семантическую правильность (динамически верифицировать) выполнения программы, прошедшей статическую верификацию.

2. Статическая верификация исполняемых программ. Верификация осуществляется на основе анализа однозначности функциональности ветвей в пределах артикулирующих компонентов программ (АКП), т. е. АКП рассматриваются как элементы факторизации управляющего графа (УГ) программы (рисунок 1) при выявлении недекларированного выполнения (НДВ) программы на основе, например, закладки.

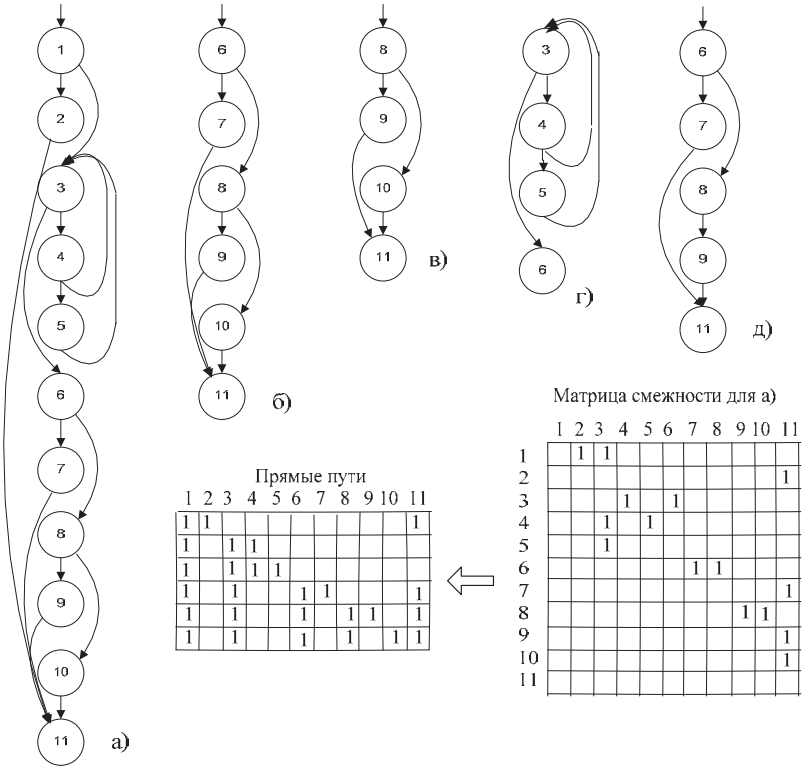


Рис. 1. Управляющий граф анализируемой подпрограммы (а) и возможные артикулирующие компоненты программ (б, в, г, д)

УГ на рисунке 1 соответствует программе, исходный текст которой приведен в листинге 1.

```
int _tmain(int argc, _TCHAR* argv[])
{
        string passwd_file = "password.txt";
        ifstream passwd_stream( passwd_file );
        if ( ! passwd_stream.is_open() )//1
        {
                string err = strerror( errno );
                cerr << "Cannot open file " << passwd_file << " : "
                 << errno << " : " << err << endl;
                exit( -1 );//2
        }
        string line;
        while( getline( passwd_stream, line ) ) {.//3
```

```
                istringstream iss(line);
                string name;
                string password;
                if ( !(iss >> name >> password) ) continue;//4
                passwords[name] = password;//5
        }
        string name, password;//6
        cout << "Enter name:"; cin >> name;//6
        cout << "Enter password:"; cin >> password;//6
        if ( name == "admin" && password == "111" ){//6
                cout << "Welcome!" << endl; //7
        }
        else{
                 if (passwords.find(name)!= passwords.end()
                 &&passwords[name]==password) //8
                         cout << "Welcome!" << endl;//9
                else     cout << "Access denied!" << endl;//10
        }
        return 0;//11
}
```

Листинг 1. Исходный текст анализируемой программы

Под АКП будем понимать как УГ отдельной подпрограммы, так и УГ фрагментов программ, ограниченных артикуляционными (субартикуляционными для вложенных фрагментов) вершинами. На рисунке 1 представлен УГ исследуемой программа и возможные АКП для неё, т.е. АКП – фрагмент УГ, ограниченный вершинами одинакового уровня вложенности. Постулируем, что в программе существует условие, выполнение которого инициирует закладку. В общем случае фрагмент программы с закладкой должен содержаться в структурах, подобных управляющим структурам, представленным на рисунке 2.

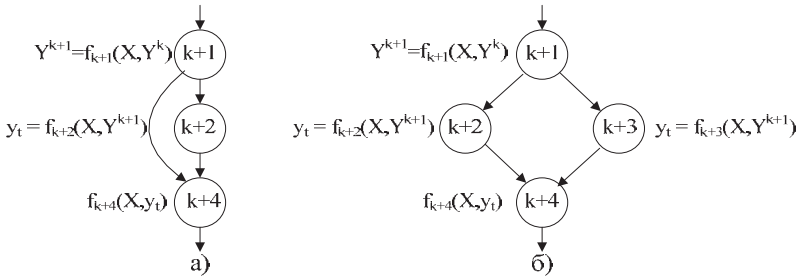


Рис. 2. Элементарные структуры-факторы

Предполагается, что проверяемые программы синтаксически правильные и описывают замкнутый вычислительный процесс Y = F (X, Y), где: X ={x_i} – множество имен исходных данных, а Y ={y_j} – множество имен результатов, включая промежуточные результаты.

Выполним формальный анализ представленных на рисунке 2 элементарных АКП (содержат точно два альтернативных пути), используя технику ограниченных символьных вычислений, положения теорий размерностей и подобия для чего предположим, что у нас имеется отображение T : X $\rightarrow$[X], которое ставит в соответствие каждому $x_i \in$ X некоторую абстрактную сущность или размерность [x_i].

Ограниченные символьные вычисления заключаются в подстановке во все содержащиеся в программе выражения E_i, вместо $y_j \in$ Y определяющих их термов, состоящих из $x_i \in$ X . Если E не содержит $y_j \in$ Y, то оно считается вычисленным или термом. Мы переносим аналитические связи между переменными и константами программы на их абстрактные сущности, т. е. действия выполняются над размерностями, что обеспечивает сохранность семантических аспектов вычислений, а выполнение подстановки делает эти выражения инвариантными к перемещениям, что позволяет объединять их в систему для совместного анализа свойств на непротиворечивость.

Любое, в том числе символьное, выполнение программы осуществляется с учетом управляющей структуры. Тогда в нашем примере на рисунке 2, семантика вычисленного объекта y_t должна быть подобной для разных путей вычисления при входе в вершину b_{k+4}, где эти пути сходятся в пределах АКП. Для примеров на рисунке 2а) и 2б) можно записать следующие равенства, называемые в дальнейшем определяющими отношениями (ОО):

$$\text{для а): } [f_{k+4}(X, f_{k+1}(X, Y_k))] = [f_{k+4}(X, f_{k+2}(X, f_{k+1}(X, Y_k)))], \qquad (1)$$

$$\text{для б) : } [f_{k+4}(X, f_{k+2}(X, Y_{k+1}))] = [f_{k+4}(X, f_{k+3}(X, Y_{k+1}))]. \qquad (2)$$

В предлагаемом подходе нас будет интересовать не численное равенство правой и левой частей в (1) и (2), а их семантическое равенство или подобие как однородных по размерностям величин, т. е. имеющих одинаковые, хотя и абстрактные, размерности. Например, в известных уравнениях:

$$\begin{aligned} a &= (v_t - v_0)/t, \\ s &= v_0 t + at^2/2 \end{aligned} \qquad (3)$$

слагаемые должны иметь одинаковые физические размерности.

Выполнив подстановку *a*, получим:

$$s = v_0t + ((v_t - v_0)/t)t^2/2 = v_0t + v_tt - v_0t. \quad (4)$$

Из (4) мы получим единственное ОО:

$$[v_0t] = [v_tt] \text{ или } [v_0] = [v_t]. \quad (5)$$

Подобную, но созданную управляющими связями, ситуацию и описывают ОО (1) и (2). Для сравнения семантических форм в ОО, подобных (1), (2) и (5), будем использовать технику преобразований теории подобия, для чего ОО делением левой части на правую часть представляются в виде степенных одночленов:

$$\prod_{K=1}^{\Upsilon}[X_k]^{a_k} = 1 \text{ или } \prod_{K=1}^{\Upsilon}[X_k]^{a_k} = [.]^0.$$

Например, используя данную технику преобразований, (4) примет вид:

$$[v_0]\,[v_t]^{-1} = [.]^0. \quad (6)$$

В терминах теории подобия безразмерное соотношение (6) называют критерием подобия и используют при анализе (моделировании) подобных физических явлений, а применительно к нашей ситуации – для проверки семантического подобия альтернирующих вычислений в программах.

Для проверки тождественности критериев подобия, выявленные в АКП степенные одночлены (5) подвергаются последовательно логарифмированию:

$$\sum_{k=1}^{\Upsilon} a_k \ln[x_k] = 0,$$

и после замены переменных ln[xk]=zk, k=1,…,r, рассматриваются как:

$$\sum_{k=1}^{\Upsilon} a_k z_k = 0$$

- линейные однородные уравнения. В пределах АКП таких уравнений может быть несколько и, так как они имеют одинаковое пространство столбцов Z и инвариантны к перемещениям, то в пределах элементарного АКП их можно объединить в систему линейных однородных уравнений (ЛОУ) Az = 0 и проверить на совместность. Если абстрактные размерности назначены n переменным из *X*, то есть | *X* | = *n*, то нельзя получить более *n-1* ЛОУ. Более того, если ОО выявили, что

только k из n переменных являются независимыми по размерности, то мы можем получить систему лишь из n-k ЛОУ [2]. В нашем случае κ=2. Независимые размерности имеют v и t и можно построить только одно ОО.

Смоделируем ошибку, изменив первое уравнение в (3) на a = $(v_t - v_0)t$, (операция деления заменена умножением). После подстановки a ($a \in Y$) в $s = v_0t + at^2/2$ получим:

$$s = v_0t + ((v_t - v_0)t)t^2/2 = v_0t + v_tt^3 + v_0t^3$$

Для полученного выражения построим три ОО, при этом получим несовместную систему ЛОУ, так как порядок системы ЛОУ не меньше |X|=3, а вычитание второго ЛОУ из первого порождает третье (и наоборот, его сложение с третьим порождает первое). Кроме того [t] становится безразмерной величиной (что невозможно) – сказывается введенная нами ошибка (при манипуляциях с t) и она будет обнаружена экспертом по этим данным.

$$\begin{array}{l} [v_0t] = [v_tt^3] \quad [v_0] \quad [t]^{-2} = [.]^0 \\ [v_0t] = [v_0t^3] \longrightarrow \quad [t]^{-2} = [.]^0 \\ [v_0t^3] = [v_tt^3] \quad [v_0]\,[v_t]^{-1} = [.]^0 \end{array} \xrightarrow[[Y]= ([a], [s])]{[X]= ([v_0], [v_t], [t])} A=\begin{pmatrix} 1 & -1 & -2 \\ 0 & 0 & -2 \\ 1 & -1 & 0 \end{pmatrix}.$$

Вы можете сказать, что в нашем примере независимыми размерностями являются [s] и [t]. Это невозможно, так как $s \in Y$, а размерности мы назначаем объектам из X.

АКП могут быть вложенными. Пример анализа вложенных АКП показан на рисунке 3. После проверки соотношения $[f_9(X,Y_8)] = [f_{10}(X,Y_8)]$ и его правильности граф а) может быть редуцирован к б), а последний на основании:

$$[f_7(X,Y_6)] = \begin{Bmatrix} [f_8(X,Y_6)] \\ [f_9(X,Y_8)] \end{Bmatrix}$$

к в) без потери информации о семантических аспектах вычислений, т.е. «правильная программа» должна редуцироваться к единственной вершине.

Рассмотрим пример. Программа, представленная в листинге 1, схематично соответствует процедуре идентификации пользователя. В процедуре есть закладка, реализованная с помощью задания констант во фразе if: «if (name == “admin” && password == “1111”)», позволяющая при необходимости обойти идентификацию пользователя.

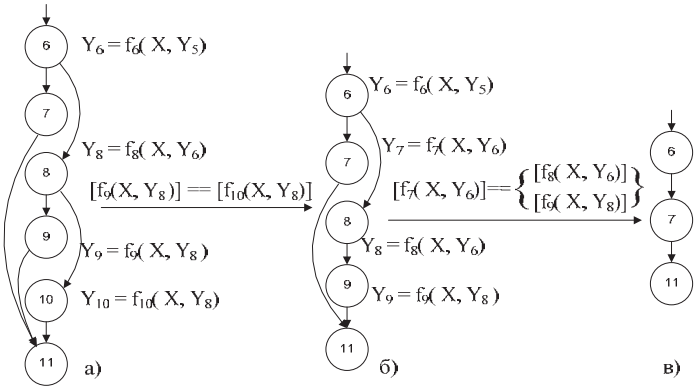


Рис. 3. Анализ (редукция) вложенных АКП

Рисунок 4 фрагментарно демонстрирует результаты анализа программы листинга 1. В общем случае предлагаемый метод должен проверять семантическую тождественность вычислений для каждого представительного АКП, а также при выполнении операций {+, -, :=, ввода-вывода, отношения, с символами и строками}. Здесь мы фиксируем выявленные представительные преобразования, которые отображаем на векторы X и Y и, выполнив подстановку, получим в итоге два ОО.

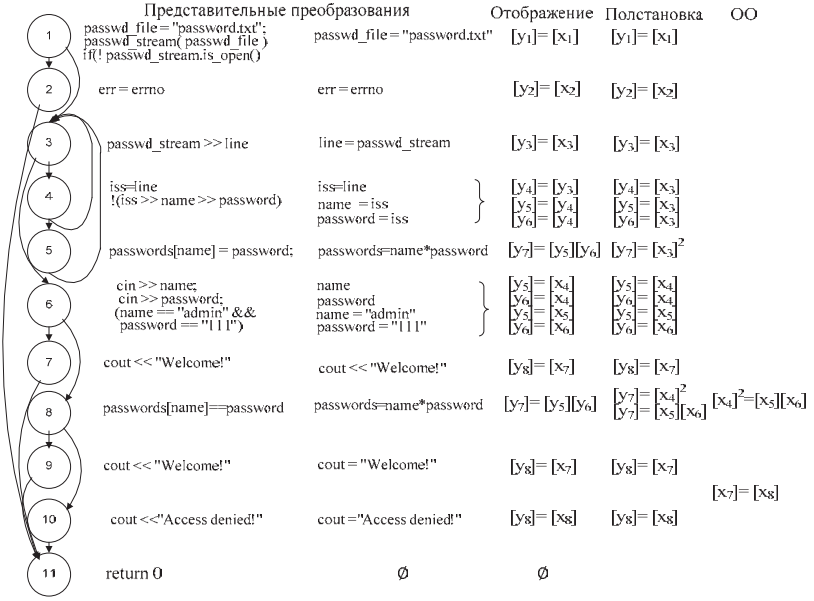


Рис. 4. Этапы анализа программы на НДВ

Процесс анализа разбит на шаги и отображается в соответствующих колонках рисунке 4.

Допустим, что мы анализируем АКП, образованный вершинами 6 – 11 (см. рисунок 4). В АКП(6-11) три пути: (6, 7, 11); (6, 8, 9, 11); и (6, 8, 10, 11). Их представляют подстановки, показанные на рисунке 5.

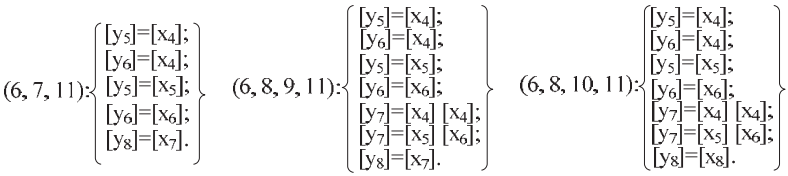
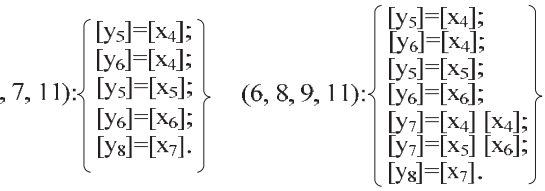
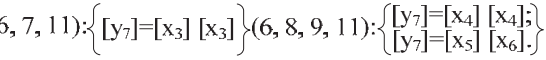


Рис. 5. Пути в АКП(6 - 11) после выполнения подстановки

Анализ АКП(6-11) начнется с анализа вложенного в него элементарного АКП(8-11), которому соответствуют пути (подстановки – символьного выполнения) (6, 8, 9, 11) и (6, 8, 10, 11). Альтернирующие пути семантически подобны, если их термы (правые части подстановок) совпадают, что имеет место если ОО $[x_7]=[x_8]$ или критерий подобия $[x_7][x_8]^{-1}=1$ имеет место быть (см. $[y_8]$). Анализ ситуации (экспертом) подтверждает это и АКП(8-11) может быть редуцирован к одному из его путей, например, (8, 9, 11). В результате, получаем элементарный АКП(6, 7, 8, 9, 11) с путями подстановки (6, 7, 11) и (6, 8, 9, 11):



Убрав из этих путей совпадающие подстановки, получим:



Подстановку [y7] = [x3][x3] для пути (6, 7, 11) мы взяли из Y5 . Для выполнения редукции АКП(6, 7, 8, 9, 11) необходимо, чтобы выполнялись следующие равенства:

$[x_3]$ = $[x_4]$ – [объект из файла1] = [объект из файла2] ;
$[x_3]$ = $[x_5]$ – [объект из файла1] = [константа1];
$[x_3]$ = $[x_6]$ – [объект из файла1] = [константа2].

Если с равенством абстрактных сущностей, вводимых из файла и консоли, эксперт может согласиться, то их равенство с предопределенными константами, как альтернативы, требует углубленного анализа функциональности АКП (6-11). Анализировать данную ситуацию должен эксперт, а выявлять подобные ситуации - инструментальный комплекс (ИК).

Подобная процедура – рекурсивная. Первым редуцируется самый вложенный АКП, поэтому АКП и рассматриваются как элементы факторизации УГП. Выявленные в них отношения между X и Y передаются без искажений и потерь в соответствии с вложенностью и следованием АКП.

Если всем переменным из X соответствуют разные сущности, то с помощью теории подобия семантика функциональных связей определяется полностью и однозначно. Превентивное назначение абстрактных сущностей переменным из X и призвано обеспечить данный эффект. Более того, назначение однотипным, с точки зрения языка программирования, переменным из X разных абстракций позволяет их разграничивать как физические сущности и контролировать конкретные функциональные связи.

Например, в интересах поиска закладок определенные в программе константы должны интерпретироваться как *предопределенные значения* для *предопределённых действий*. Поэтому пути выполнения программы, в формировании которых участвуют константы, подлежат обязательной проверке. Семантику предопределённых действий как и альтернативных действий мы обязательно обнаружим, так как заданные $[x_k]$ при подстановках в процессе символьной интерпретации конкретизируют все связи.

Отличительной особенностью предлагаемого метода верификации и выявления закладок является вовлечение в процесс анализа семантических аспектов в контексте управляющих связей в программах, исключающих аппроксимацию или пропуск функциональных связей.

3. Динамическая верификация программ. Под динамической верификацией программ будем понимать контроль правильности семантики вычислений в ходе их реального выполнения. Понятно, что данные для динамического контроля необходимо предварительно получить, как получаем исполняемый код во время компиляции. Естественным образом напрашивается идея использовать для этого результаты статической верификации в виде паспорта π программы П. Поэтому

статическую верификацию должен проходит точно тот же исполняемый код, что и динамическую верификацию.

Паспорт π исполняемой программы П создается в процессе статической верификации (по дизассемблированному коду П) и содержит:

– вектор X с именами исходных данных;

– систему определяющих соотношений как систему линейных однородных уравнений $Az = 0$ с пространством столбцов, отображаемым на X:

– любое (желательно целочисленное) частное решение $Az = 0$ – вектор исходных абстрактных размерностей для X.

Для верификации исполняемой программы П в темпе реального времени выполнения нам понадобится интерпретирующий сопроцессор.

Множество команд *K* исполняемой программы П (команды ассемблера) разбивается на три подмножества:

K_A – аддитивные команды (сложение, вычитание, сравнение,…);

K_M – мультипликативные команды (умножение, деление, сдвиг,…):

K_N – не интерпретируемые команды .

Сопроцессор интерпретирует команды основного процессора следующим образом:

– если основной процессор выполняет команду $к_i \in$ КА, то сопроцессор выполняет сравнение размерностей ее операндов;

– если основной процессор выполняет операцию $к_i \in$ КМ, то сопроцессор выполняет манипуляции с размерностями операндов (сложение или вычитание);

– если основной процессор выполняет операцию $к_i \in$ KN, то сопроцессор простаивает.

Данная интерпретация является прямой симуляцией действий, связанных с преобразованием степенных одночленов в линейные уравнения.

Выход исполняемой программы за пределы контролируемой среды (верифицированной в статике) определяется по результатам манипулирования операндами команд, для каждого из которых в памяти M^C сопроцессора отведено место и в него записано абстрактное паспортное (из зафиксированного в паспорте частного решения для Az=0) или сформированное в процессе интерпретации значение операнда.

Использование данных методов статической и динамической верификации перспективно для ПО замкнутых, не подверженных ди-

намическим изменениям программных систем. В отличие от [3] и [4] здесь связи по управлению контролируются опосредованно.

4. Заключение. Задача исчерпывающего выявления НДВ в программном коде, в общем случае, алгоритмически неразрешима, а существующие частные решения приходится аппроксимировать, чтобы избежать «комбинаторного взрыва» - сделать их сложность приемлемой для практической реализации. Чаще всего динамическую верификацию подменяют целенаправленным и многоаспектным тестированием. В предложенном методе динамическая верификация осуществляется как обязательная предопределенная процедура при каждом выполнении прошедшего статическую верификацию ПО. Данный подход позволяет исключить возможность выполнения кода не прошедшего статическую верификацию, в том числе внесенного позже в систему вредоносного кода.

Литература

1. *Седов Л.Н.* Методы подобия и размерности в механике // М: Наука. 1981. 448с.
2. *Ильин В. А., Позняк Э. Г.* Линейная алгебра // М.: ФИЗМАТЛИТ. 2004. 280 с.
3. *Компаниец Р.И., Ковалев В.В., Маньков Е.В.* Экспертиза и защита кода программ на основе автоматов динамического контроля // Защита информации. INSIDE. 2007. №3. С. 48–55.
4. Инструментального комплекс для автоматизации проведения статического и динамического анализа потоков управления в исполняемых кодах программ «IRIDA» // ТУ 425790.007.72410666.04. ООО «Газинформсервис».

References

1. Sedov L.N. *Metody podobiya i razmernosti v mehanike* [Methods of similarity and dimensionality in mechanics]. M: Nauka. 1981. 448 p. (In Russ.).
2. Ilin V.A., Poznyak E.G. *Lineinaya algebra* [Linear algebra]. M.: FIZMATLIT. 2004. 280 p. (In Russ.).
3. Kompaniez R.I., Kovalev V.V., Mankov E.V. [Expertise and protection of a program's code based on automata of dynamic control] *Zaschita informatzii.Inside – Information Security. Inside*. 2007. vol. 3. pp. 48–55 (In Russ.).
4. The tool kit for the automation of static and dynamic analysis of control flow in the executable program codes «IRIDA». TU 425790.007.72410666.04. OOO «Gazinformservice». (In Russ.).

Ковалев Виктор Васильевич — кандидат технических наук, профессор, доцент кафедры систем сбора и обработки информации Военно-космической академии имени А.Ф. Можайского. Область научных интересов: реверс инжиниринг, надежность, устойчивость функционирования и верификация программного обеспечения. Число научных публикаций — 14. ВКА имени А.Ф.Можайского, ул. Ждановская, д.13 г. Санкт-Петербург, 197198 , РФ, р.т. +7(812)347-9687.

Kovalyov Viktor Vasilevich — Ph.D., professor, associate Professor department systems collecting and processing information of Military space Academy named of A.F. Mozhayskiy. Research interests: reverse engineering; software reliability, stability and verification. The number of scientific publications — 14. MSA named of A.F. Mozhayskiy, st. Zhdanovskay, h.13 c. St. Petersburg, 197198, RF, office phone +7(812)347-9687.

Компаниец Радион Иванович — преподаватель кафедры систем сбора и обработки информации Военно-космической академии имени А.Ф. Можайского. Область научных интересов: построение трансляторов, верификация программного обеспечения. Число научных публикаций — 15. ВКА имени А.Ф. Можайского, ул. Ждановская, д.13 г. Санкт-Петербург, 197198 , РФ, р.т. +7(812)347-9687.

Kompaniets Radion Ivanovich — teacher of department systems collecting and processing information of Military space Academy named of A.F. Mozhayskiy. Research interests: construction of compilers; software verification. The number of scientific publications — 15. MSA named of A.F. Mozhayskiy, st. Zhdanovskay, h.13 c. St. Petersburg, 197198, RF, office phone +7(812)347-9687.

Новиков Владимир Александрович — к.т.н., докторант кафедры систем сбора и обработки информации Военно-космической академии имени А.Ф. Можайского. Область научных интересов: реверс инжиниринг, построение трансляторов, верификация программного обеспечения. Число научных публикаций — 34. ВКА имени А.Ф.Можайского, ул. Ждановская, д.13 г. Санкт-Петербург, 197198 , РФ, р.т. +7(812)347-9687.

Novikov Vladimir Aleksandrovich — Ph.D., doctoral candidate of the department systems collecting and processing information of Military space Academy named of A.F. Mozhayskiy. Research interests: reverse engineering; construction of compilers; software verification. The number of scientific publications — 34. MSA named of A.F. Mozhayskiy, st. Zhdanovskay, h.13 c. St. Petersburg, 197198, RF, office phone +7(812)347-9687.

РЕФЕРАТ

Ковалев В.В., Компаниец Р.И., Новиков В.А. **Верификация программ на основе соотношения подобия.**

В работе рассматриваются взаимосвязанные методы статической и динамической верификации программ, представленных в исполняемых кодах. Верификация осуществляется на основе проверки семантического подобия их поведения при достижении данного состояния по всем возможным путям, что исключает аппроксимацию функциональности верифицируемых программ. Снижение трудоемкости метода достигается отображением переменных программы на их абстрактные размерности.

В качестве моделей программ используется управляющий граф с факторизацией на артикулирующие компоненты и модели поведения альтернативных и повторяющихся фрагментов программы в процессе интерпретации программы в терминах абстрактных размерностей. Поведенческие модели представляются системами линейных однородных уравнений, анализ которых на совместность и непротиворечивость позволяет получить необходимые условия правильности функциональных связей в программах.

По результатам статической верификации строится паспорт программы, по которому с помощью сопроцессора можно осуществлять действительную динамическую верификацию данной программы в реальном времени при ее выполнении.

SUMMARY

Kovalev V.V., Kompanietc R. I., Novikov V.A. **Verification of Programs Based on Similarity Relations.**

This work represents interconnected methods of static and dynamic verification of the programs that are represented in source codes. Verification is based on the semantic similarity inspection of their behavior at the moment when they reach this state in all possible ways, which excludes functionality approximation of the verified programs. Labor intensiveness decrease is achieved by mapping program variables into their abstract dimensions.

Control graph with the factorization on the articulating components and behavioral models of alternative and repetitive fragments of the program in the interpretation of the program in terms of abstract dimensions are used as models of programs. Behavioral models are represented by systems of the linear homogeneous equations which compatibility and consistency analysis allows to obtain the necessary conditions of correctness of the functional connections in the programs.

Program passport is based on the results of the static verification, and which is used by the coprocessor to implement the valid dynamic verification of the running program.

УДК 004.77

Г.А. Аниканов, П.М. Коновальчик, В.М. Моргунов, В.А. Овчаров

КОНТРОЛИРУЕМЫЙ МНОГОМОДЕЛЬНЫЙ ДОСТУП К СРЕДЕ БЕСПРОВОДНЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Аниканов Г.А., Коновальчик П.М., Моргунов В.М., Овчаров В.А. **Контролируемый многомодельный доступ к среде беспроводных сетей передачи данных.**
Аннотация. В работе рассматривается задача разработки метода контролируемого многомодельного доступа к среде беспроводных сетей передачи данных (БСПД) стандартов IEEE 802.11, 802.16. В качестве решения предлагается продукционно-логическая система управления доступом к среде БСПД по результатам мониторинга, учитывающая влияние используемых методов на сетевую инфраструктуру.
Ключевые слова: беспроводная сеть передачи данных, уязвимость протокола, текущая ситуация, полная ситуация, активный мониторинг, пассивный мониторинг, протоколы маршрутизации, продукции, сценарии атак, модель угроз, контролируемый многомодельный доступ к среде передачи данных.

Ovcharov V.A., Anikanov G.A., Konovalchik P.M., Morgunov V.M. **The Multi-Controlled Media Access to Wireless Data Networks.**
Abstract. Paper considers the problem of developing of a method of controlled access to the multimodal environment of wireless data networks (WDN) of standards IEEE 802.11, 802.16 is considered. As a solution production-logical system of the medium access control WDN on the monitoring results, which takes into account the effect of the methods used in the network infrastructure, is proposed.
Keywords: current situation, overall situation, active monitoring, passive monitoring, routing protocols, products, wireless data network threat model.

1. Введение. В первое десятилетие 21 века беспроводные цифровые коммуникации вступили в очередную фазу динамичного развития, которая продолжается и в настоящее время. Толчком к этому послужило, с одной стороны, интенсивное развитие протоколов контроля состояния каналов связи, коммутации и междоменной маршрутизации (AODV, EGP, IDRP, LLDP, LISP, IPv6, TORA, DSR и др.), с другой – внедрение прогрессивных методов кодирования, модуляции и передачи информации, нашедших применение в технологиях IEEE 802.11ac, 802.16 (WiMax, LTE). Вместе с тем, широкое распространение и большая зона покрытия современных БСПД – главная причина нарушений безопасности, поскольку нарушитель может находиться на значительном удалении от места физического развертывания сети, а коммуникационные сигналы при распространении доступны для перехвата.

Важнейшей задачей в рамках обеспечения безопасного функционирования и расследования инцидентов информационной безопасности (ИБ) БСПД является контроль и управление доступом к среде передачи данных. Для ее решения в данной статье предлагается модель угроз, учитывающая особенности физического и канального

уровней эталонной модели взаимодействия открытых систем (ЭМВОС) ISO/OSI, являющихся наиболее уязвимыми при реализации угроз нарушителями. Для разработки эффективных мер противодействия проведена классификация соответствующих типов атак и механизмов их реализации в БСПД, а также метод контролируемого многомодельного доступа к беспроводной среде передачи.

2. Модель угроз безопасности БСПД. Проведенные авторами исследования и анализ работ [1, 2, 4, 5, 10] показал, что, как с точки зрения формирования отпечатков для средств пассивного мониторинга, так и с точки зрения получения доступа к среде передачи данных и проведения процедур мониторинга активными средствами, БСПД отличаются от проводных только на первых двух – физическом, канальном и отчасти сетевом уровнях ЭМВОС ISO/OSI. Более высокие уровни реализуются в соответствии с теми же принципами, что и в проводных сетях, а реальная безопасность сети с точки зрения получения доступа обеспечивается именно на этих, нижележащих уровнях. В соответствии с проведенным анализом была разработана модель угроз безопасности БСПД (рисунок 1).

В разработанной модели цифрами обозначены уровни ЭМВОС ISO/OSI. На каждом из уровней (группе уровней) определены критичные элементы БСПД – программные и аппаратные, на которые направлены определенные типы атак и классы угроз. Будем выделять следующие классы угроз для БСПД: нарушение политики безопасности (ПБ), эксплуатация уязвимостей ПО и микрокода оборудования, эксплуатация слабой конфигурации аутентификации, эксплуатация слабой конфигурации ограничения доступа. Данные классы угроз декомпозируются на типы, которые определяются наличием или отсутствием соответствующих условий для их реализации. В данной работе при рассмотрении характерных уязвимостей БСПД IEEE 802.11, 16 будем выделять *2 группы угроз*: угрозы на физическом (сигнальном) уровне ЭМВОС, представленные на рисунке в соответствующей области и угрозы на канальном (информационном) уровне ЭМВОС. Перечисленные на рисунке типы атак и ассоциированные классы угроз, выделенные более толстыми стрелками, как правило, используют при реализации сразу несколько уровней ЭМВОС, кроме того, часть из них, характерна и для проводных сетей стандарта IEEE 802.3.

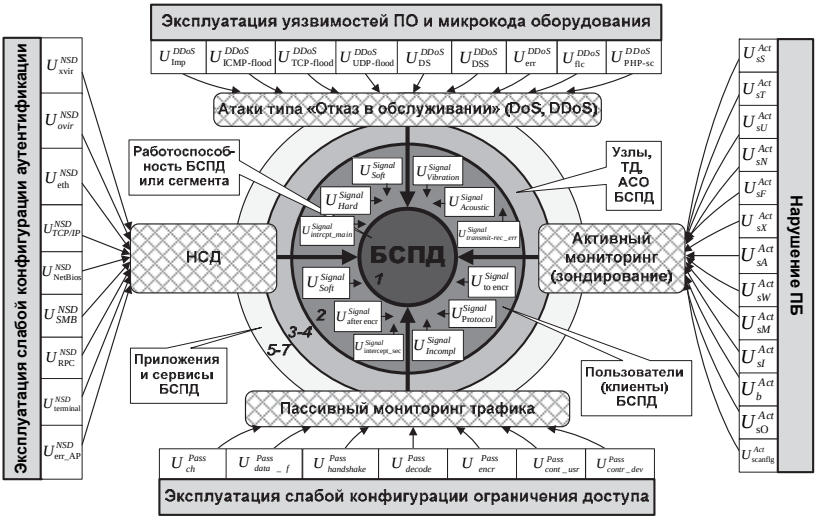


Рис. 1. Модель угроз безопасности в БСПД IEEE 802.11, 802.16

Нарушитель может использовать 4 агрегированных типа атак, как с целью получения доступа к среде передачи БСПД, так и в целях определения возможностей анонимного получения такого доступа: атаки, основанные на технологиях пассивного мониторинга трафика, несанкционированный доступ (НСД), атаки типа «Отказ в обслуживании» и атаки, основанные на технологиях активного сканирования (зондирования). Перечисленным типам атак соответствуют используемые в подсистеме идентификации событий с негативными последствиями классификаторы, описание которых представлено ниже. Данная подсистема обеспечивает как контроль инфраструктуры БСПД при выявлении потенциальных внутренних нарушителей (инсайдеров). Так и при планировании мероприятий активного мониторинга внешних (удаленных) беспроводных сегментов.

Наиболее критичная проблема на физическом уровне БСПД - возможность анонимных атак. Использование антенн и усилителей позволяет нарушителю находиться на значительном расстоянии от цели в процессе перехвата трафика и осуществления атак. Наличие уязвимостей на физическом уровне делает проблематичной защиту канального уровня, на котором должны быть предотвращены: целенаправленное искажение передаваемых и получаемых данных; перехват идентификационной и пользовательской информации; перехват управления подсистемой связи (оборудованием) БСПД.

В таблице 1 представлена систематизированная информация о типах угроз в БСПД и условиях их реализации нарушителем на физическом уровне ЭМВОС.

Таблица 1. Типы и условия реализации угроз в БСПД на физическом уровне

Угроза БСПД	Условия реализации угрозы	Уязвимый элемент БСПД	Индекс классификатора
Аппаратные и программные ошибки при разработке	Неполное тестирование аппаратуры БСПД	БСПД	U^{Signal}_{Hard}, U^{Signal}_{Soft}
Перехват сопровождающих передачу акустических и вибрационных сигналов	Доступность пунктов приема и передачи		$U^{Signal}_{Acoustic}$, $U^{Signal}_{Vibration}$
Ошибки протокола обмена	Наличие пересечений в сигнальных и логических областях команд и директив	Система управления БСПД	$U^{Signal}_{Protocol}$
Нарушения регламента связи	Неполная реализация протокола		$U^{Signal}_{Incompl}$
Ошибки при передаче и приеме сигнала	Работа в условиях помех	Приемный и передающий тракт узлов БСПД	$U^{Signal}_{trans-rec\_err}$
Перехват сигналов до и после шифрования	Наличие в каналах незашифрованной (расшифрованной) информации		$U^{Signal}_{to\ encr}$, $U^{Signal}_{after\ encr}$
Перехват сигнала в основном канале	Наличие аппаратуры, работающей на прием	Канал передачи	$U^{Signal}_{intrcpt\_main}$
Перехват сигнала в побочных каналах	Низкая фильтрация сигнала основного канала	Цепи питания и заземления	$U^{Signal}_{intercept\_sec}$

Отметим, что высокая степень защищенности канала на физическом уровне не является гарантией обеспечения столь же высокой информационной защищенности всей БСПД. Это обусловлено тем, что основным показателем успешного функционирования отдельной подсистемы БСПД является реализация его целевой функции. При этом физический уровень обеспечивает нейтрализацию конфликтного компонента (угрозы) только на своем участке.

Методы пассивного мониторинга трафика БСПД основаны на использовании нарушителем различных анализаторов пакетов, методов доступа к среде передачи, механизмов обработки протокольных блоков данных, дешифрования и декодирования на канальном, сетевом, сеансовом и прикладном уровнях ЭМВОС. Соответствующие типы и условия реализации угроз представлены в таблице 2.

Таблица 2. Типы угроз в БСПД при пассивном мониторинге трафика

Угроза БСПД	Условия реализации угрозы	Уязвимый элемент БСПД	Индекс классификатора
Выявление канала передачи для перехвата	Наличие в передаваемых данных отличительных признаков, работа на одном канале	Подсистемы шифрования и управления каналами	U_{ch}^{Pass}
Определение формата данных	Использование стандартных форматов без дополнительной коррекции	Подсистемы кодирования и шифрования	$U_{data\_f}^{Pass}$
Восстановление пакетов (кадров)	Отсутствие маскировки синхронизации и маркеров доступа	Подсистема управления обменом данными	$U_{handshake}^{Pass}$
Линейное декодирование	Возможность сбора статистики передачи информации, использование при передаче открытых кодов	Кодер/ декодер	U_{decode}^{Pass}
Дешифрование декодированных данных	Наличие коррелятов в базе перехваченного сигнала, компрометация ключей, получение блока нешифрованного сигнала	Подсистема организации обмена данными	U_{encr}^{Pass}
Передача управляющих последовательностей абоненту	Возможность получения мастер-кодов, компрометация кодов систем защиты	Подсистема управления сеансами связи (сессиями)	$U_{cont\_usr}^{Pass}$
Передача управляющих последовательностей оборудованию	Возможность получения мастер-кодов, компрометация кодов систем защиты, доступ к ЦП и ПО управления	Подсистемы управления связью и коммутации	$U_{contr\_dev}^{Pass}$

Активное обнаружение элементов БСПД реализуют многочисленные инструменты: NMap, Zmap, Netstumbler, MiniStumbler, Inssider и др. При этом, работа ряда инструментов нарушителей основана на недокументированной возможности библиотеки hcf, драйвера беспроводного устройства, работе от имени непривилегированного пользователя. В таблице 3 приведены типы и условия реализации угроз БСПД при реализации методов активного сканирования (зондирования).

Уязвимость протокола TCP к низкоскоростным атакам обусловлена необходимостью достижения компромисса между максимальной производительностью и контролем потоков в различных условиях. Технологии низкоскоростных DoS-атак используют потоки трафика со специально подобранной величиной и длительностью пиков, повторяющихся в определенный промежуток времени [3, 11], что затрудняет их обнаружение средствами IDS, NIDS, IPS, применяемыми и в БСПД.

Таблица 3. Типы угроз в БСПД при активном мониторинге трафика

Угроза БСПД	Условия реализации угрозы	Уязвимый элемент БСПД	Индекс классификатора
TCP SYN сканирование	Наличие привилегий для отправки raw-пакетов	Порты TCP/UDP	U_{sS}^{Act}
TCP сканирование с использованием высокоуровневых системных вызовов	Соединение с целевым узлом по указанному порту путем системного вызова connect	Службы, порты TCP/UDP	U_{sT}^{Act}
Различные типы UDP-сканирования	Отправка заголовка UDP на целевой порт	Службы UDP, порты UDP	U_{sU}^{Act}
TCP NULL, FIN-, Xmas-сканирование	Манипуляция TCP флагами, установленными в пакетах запросов	Статус портов TCP/UDP	$U_{sN}^{Act}, U_{sF}^{Act}, U_{sX}^{Act}$
TCP ACK сканирование		Фильтруемые порты на брандмауэре	U_{sA}^{Act}
TCP Window сканирование		Особенности реализации ОС при разделении портов на открытые и закрытые	U_{sW}^{Act}
TCP сканирование Мэймона		Особенности реализации стека в ОС FreeBSD	U_{sM}^{Act}
Нетривиальное TCP-сканирование	Задание специфичных TCP-флагов	Открытый/ фильтруемый TCP-/UDP-порт	$U_{\text{scanflags}}^{Act}$
Idle-сканирование	Использование предсказуемой последовательности, генерация ID IP-фрагментов для сбора информации о портах	Доверительные отношения между элементами БСПД, порты TCP/UDP	U_{sI}^{Act}
Сканирование с использованием протокола IP	Отправка модифицированных заголовков IP-пакетов	Поддерживаемые протоколы на целевом узле	U_{sO}^{Act}
Сканирование типа FTP bounce	Подключение к FTP-серверу	Открытые порты TCP/UDP	U_{b}^{Act}

Задача лавинообразных распределенных DDoS-атак – максимальное потребление предоставляемых ресурсов активного сетевого оборудования (АСО) с целью прекращения предоставления пользователям ресурсов БСПД. Атакуемыми ресурсами являются: ширина канала доступа к БСПД, процессорное время АСО и конкретные реализации протоколов. Отдельно отметим уязвимости при реализации ПО

удаленного управления в АСО БСПД с использованием php-сценариев, приводящие к возможности осуществления удаленного отказа в обслуживании. В таблице 4 приведены типы и условия реализации угроз БСПД при реализации низкоскоростных и лавинообразных TCP-ориентированных DoS, DDoS-атак.

Таблица 4. Типы угроз в БСПД при реализации атак «Отказ в обслуживании»

Угроза БСПД	Условия реализации угрозы	Уязвимый элемент БСПД	Индекс классификатора
Импульсная TCP-ориентированная DoS-атака	Неавторизованный доступ к ресурсам БСПД	АСО, клиенты БСПД	U^{DDoS}_{Imp}
Лавинообразная распределенная DDoS-атака (TCP-/UDP-/ICMP-flood		БСПД в целом	$U^{DDoS}_{\text{TCP-flood}}$, $U^{DDoS}_{\text{UDP-flood}}$, $U^{DDoS}_{\text{ICMP-flood}}$
Передача ложного сигнала в ходе имитации вызова	Возможность определения протокола обмена	Подсистема приема и управления приемом	U^{DDoS}_{DS}
Передача ложного сигнала в ходе сеанса связи	Возможность выделения и определения идентификационных преамбул		U^{DDoS}_{DSS}
Легальная передача ложной информации	Наличие логического или физического адреса объекта атаки	БСПД в целом	U^{DDoS}_{err}
Искажение сигнала передачи	Возможность вскрытия синхронизации и входа в канал без нарушения	Приемо-передающая подсистема	U^{DDoS}_{flc}
Удаленный отказ в обслуживании	Ошибки реализации php-сценариев управления АСО БСПД	АСО, БСПД в целом	$U^{DDoS}_{\text{PHP-sc}}$

Несанкционированный доступ (НСД), являющийся реализацией преднамеренной угрозы безопасности БСПД представим атаками 4 типов [4]:

- атаки, направленные на получение информации при непосредственном доступе к элементу (ТД, ПЭВМ) БСПД (локальный НСД);
- атаки без непосредственного доступа к элементу БСПД (удаленный НСД);
- атаки с целью получения НСД к информации в канале связи с другими клиентами БСПД;
- атаки с отслеживанием побочных электромагнитных излучений (ПЭМИ) ПЭВМ, приведенные в таблице 1.

В таблице 5 приведены типы и условия реализации угроз БСПД при реализации НСД к ресурсам БСПД.

Таблица 5. Типы угроз в БСПД при реализации НСД

Угроза БСПД	Условия реализации угрозы	Уязвимый элемент БСПД	Индекс классификатора
Атака целевым вирусом	Отсутствие механизмов проверки целостности, использование возможностей защищенного режима ЦП	Приложение, драйвер, ПЭВМ БСПД	U^{NSD}_{xvir}
Атака общим вирусом			U^{NSD}_{ovir}
Атаки на основе уязвимостей протокола Ethernet	Отсутствие (ошибки при конфигурировании) встроенных функций защиты БСПД, механизмов аутентификации, авторизации, аудита	БСПД в целом	U^{NSD}_{eth}
Атаки на основе уязвимостей стека TCP/IP, NetBios			$U^{NSD}_{\text{TCP/IP}}$, U^{NSD}_{NetBios}
Атаки на основе уязвимостей протокола SMB, RPC		Участники информационного обмена	U^{NSD}_{SMB}, U^{NSD}_{RPC}
Атаки на протоколы терминального доступа	Отсутствие средств шифрования канала	Оборудование БСПД	$U^{NSD}_{\text{terminal}}$

Проведенные исследования [6, 8] показали, что в настоящее время ни одна из современных систем обнаружения атак с открытым исходным кодом (STAT, Prelude, Bro, SNORT и др.) не покрывает всё множество сформулированных классов атак. Данные системы используют неадаптивные методы обнаружения и не покрывают все уровни наблюдения за БСПД. Поэтому на следующем этапе, в целях выделения особенностей, позволяющих осуществлять доступ как к БСПД общего назначения, включающих проводные (магистральные) сегменты, так и к автономным беспроводным сегментам, рассмотрим механизмы реализации типовых атак на различные компоненты БСПД.

3. Декомпозиция сценариев реализации типовых атак на компоненты БСПД и протоколы маршрутизации. На основе разработанной модели угроз синтезируем декомпозированную схему вероятных сценариев атак на БСПД (рисунок 2), связывающую соответствующие типы угроз, механизмы реализации (эксплуатации) уязвимостей и методов доступа к беспроводной среде передачи данных.

В соответствии с приведенным выше рисунком любые сценарии атак на БСПД можно представить в виде логической цепочки, однозначно и полно характеризующей используемые технологии и методы доступа к среде передачи БСПД

Угроза БСПД → Механизм реализации уязвимости → Метод доступа

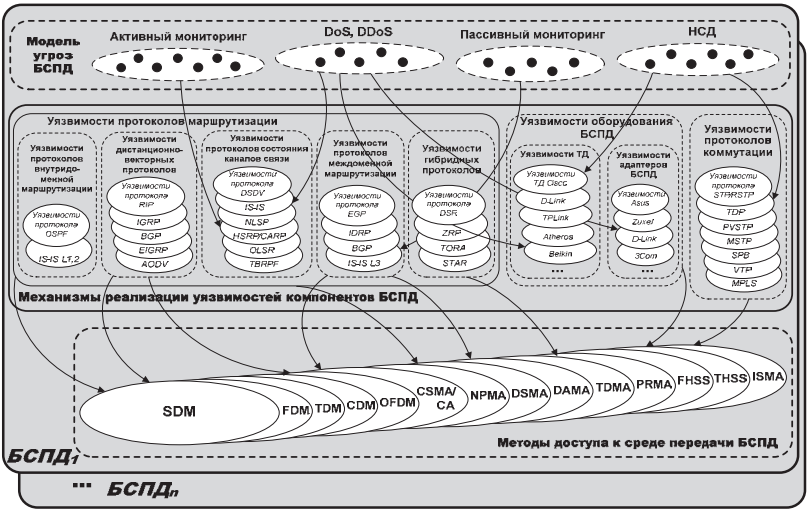


Рис. 2. Вероятные сценарии атак на БСПД

Для последующего анализа применимости методов доступа к среде передачи свяжем БСПД типы атак на БСПД с механизмами реализации уязвимостей компонентов БСПД в соответствии с таблицей 6.

Таблица 6. Типы атак на БСПД и механизмы реализации уязвимостей

№	Тип атак на БСПД	Уязвимый компонент	Особенности	Связь с др. типами атак
1	*«Черная дыра»/«серая дыра»*	Протокол AODV	Модификация/предварительный отбор проходящих пакетов и создание ложных маршрутов на основе анализа легитимных запросов к узлам, перегрузка АСО БСПД	12, 13
2	*Переполнение таблицы маршрутизации*	DSDV, CGSR, WRP, RIP, OSPF, FSR, TBRPF, OLSR	Переполнение маршрутных таблиц АСО БСПД	4, 13
3	*Переполнение буфера (buffer overrun)*	Протокол SRP	Переполнение внутреннего буфера обработки SRP (CVE-2014-3512)	
4	*«Испытание бессонницей»*	Ad Hoc сети, протоколы GRAB, SAR, MCFA	Генерация повышенного энергопотребления АСО БСПД, используя запросы маршрутной информации, или переадресуя некорректные пакеты другим узлам	1, 11, 12

№	Тип атак на БСПД	Уязвимый компонент	Особенности	Связь с др. типами атак
5	*Идентификация местоположения* узлов и АСО БСПД	Протоколы ICMP, ICMPv6	Определение контрагентов, физического расположения узлов, структуры БСПД путем отправки сообщений с недостаточным значением предела числа hop-ов	6, 14
6	*Манипуляции ресурсами (resource manipulation)*	Протокол ARAN	Подмена доверенного источника (эмитента) сертификатов	12
7	*Разрыв связей* в подсистеме обмена маршрутной информацией	Протоколы BGP, Grid Routing	Отправка модифицированных пакетов из проводного/беспроводного сегментов узлами, замаскированными под легитимные	7, 8, 9
8	*Нарушение конфиденциальности (confidentiality violations)*		Перехват и анализ маршрутной и конфигурационной информации	1, 14
9	*Воспроизведение* (*replay*)		Повторное использование перехваченных сообщений	12
10	*Вставка сообщений* (*message insertion*)		Вставка сообщений на основе предсказания порядковых номеров при перехвате TCP-сессий	12
11	*Удаление сообщений (message deletion)*		Удаление легитимных сообщений	12
12	*Изменение сообщений* (*message modification*)		Скрытная синтаксически корректная модификация сообщений без изменения размера TCP-данных	12
13	*«Человек посередине» (man-in-the-middle)*		Эксплуатация уязвимостей, связанных с отсутствием технологий аутентификации партнеров	1
14	*Dos-атаки на службы*	Протоколы BGP, SRP (CVE-2014-5139), AODV	Анонсирование большого числа специфичных маршрутов с длинными префиксами, приводящее к росту трафика и размеру таблиц маршрутизации, до неприемлемых для системы	1
15	*Пассивные атаки*	АСО, узлы БСПД	Несанкционированный перехват и анализ трафика протоколов маршрутизации, раскрытие информации о взаимодействии между узлами, выявление адресов, определение расположения узлов и топологии	4, 12

Протоколы маршрутизации в БСПД являются основой ее инфраструктуры, контролируя и управляя потоками данных. Нарушитель может полностью контролировать маршрутизатор для реализации наи-

более разрушительных, внутренних атак на БСПД. В результате компрометация сетевой инфраструктуры может привести к отказу служб, раскрытию (модификации) чувствительной маршрутной информации, сетевого трафика, или некорректному использованию ресурсов БСПД.

Перечислим атаки на протоколы маршрутизации БСПД и их последствия:

- *network congestion* (перегрузка сети) – через сегмент БСПД пересылается больше данных, чем он способен обработать;
- *delay* (задержка) – данные, адресованные узлу, пересылаются по более длинному пути, чем обычно;
- *looping* (петли) – данные передаются по замкнутому пути и никогда не будут доставлены;
- *eavesdrop* (перехват) – данные пересылаются через маршрутизатор или сегмент сети, которые не должны их обрабатывать;
- *partition* (принудительная сегментация сети) – некоторые сегменты кажутся отделенными от сети, хотя на самом деле это не так;
- *cut* (отключение) – некоторые сегменты могут казаться отрезанными от сети, хотя реально остаются подключенными;
- *churn* (волны) – скорость пересылки в БСПД лавинообразно изменяется, что приводит к вариациям времени доставки пакетов и неблагоприятно влияет на работу системы контроля насыщения;
- *instability* (нестабильность) – нестабильная работа протокола маршрутизации не позволяет достичь сходимости таблицы маршрутов;
- *overload* (перегрузка) – BGP-сообщения становятся значительной частью передаваемого в сеть трафика;
- *resource exhaustion* (истощение ресурсов) – BGP-сообщения отнимают слишком много ресурсов маршрутизатора (пространства таблиц) вследствие реализации перегрузки;
- *address spoofing* (обманные адреса) – данные пересылаются через подставной маршрутизатор (сегмент БСПД), служащие для перехвата (искажения) информации.

Таким образом, связанные с протоколами маршрутизации риски нарушения доступа к среде БСПД обусловлены тремя основными типами уязвимостей:

- отсутствием в реализации протоколов внутреннего механизма обеспечения сильной защиты целостности и актуальности данных, аутентификации партнеров для сообщений, передаваемых между узлами;
- отсутствием механизма проверки полномочий AS для анонсируемой информации NLRI;

- отсутствием механизма обеспечения достоверности атрибутов пути, анонсируемых AS.

Таким образом, для БСПД недостаток поддержки фиксированной инфраструктуры, частые изменения сетевой топологии выдвигают на первый план проблемы безопасной маршрутизации. При этом, основная проблема заключается в том, как безопасная связь между источником и приемником может быть установлена перед тем, как будет проложен маршрут между ними. Например, при использовании протокола OADV (RREQ, RREP) необходимо использовать дополнительные атрибуты безопасности и уровни доверия для каждого узла. Также необходима схема, основанная на использовании DSR, в которой каждому узлу приписывается оценка стоимости, а также использование методов сторожевых таймеров и адаптивной маршрутизации, управляющих работой узлов и выбором маршрутов. Проанализированные протоколы маршрутизации (SRP, AODV, ARAN) реализованы многочисленными производителями оборудования (Buffalo, JOLT, Korenix, Surplus Communications, TTI Wireless и др.) и широко используются в современных БСПД. В то же время, инфраструктура маршрутизации остается важнейшим компонентом БСПД и имеет слабые места в системе защиты. Поэтому, кроме вышеперечисленных рекомендаций, требуются новые криптографические методы для обеспечения безопасной работы БСПД.

4. Анализ применимости методов доступа к среде передачи в БСПД IEEE 802.11, 802.16 при проведении мониторинга. Указанные достоинства беспроводных технологий определяются тем, что в основе БСПД лежит технология широкополосного (шумоподобного) сигнала. В то же время, для функционирования БСПД требуются специальные протоколы управления доступом к среде (MAC) ввиду фундаментальных отличий от кабельной среды: отсутствует полная связность, беспроводная среда не защищена от внешних сигналов, и ее свойства по распространению сигналов асимметричны и изменчивы во времени. Понимание эффективности, достоинств и недостатков, аспектов использования различных технологий доступа к среде передачи в БСПД необходимо для эффективного управления потоками в беспроводной среде, классификации и парирования возможных атак на БСПД с использованием уязвимостей канального и физического уровня, разработки эффективной политики безопасности (ПБ) в контролируемой БСПД.

Решение задачи доступа многих пользователей к ограниченному ресурсу среды передачи (множественного доступа) основана на выделении каждому каналу связи (КС) пространства, времени, частоты и/или кода с минимумом взаимных помех и максимальным использо-

ванием характеристик передающей среды. Основные группы методов доступа к среде передачи в БСПД IEEE 802.11, 802.16 и их определяющие свойства сведем в таблицу 7.

Таблица 7. Сводная таблица свойств методов доступа к среде передачи в БСПД IEEE 802.11, 802.16 (WiMAX, LTE)*

Свойство	Наименование группы методов доступа к среде БСПД											
	SDM	FDM	TDM	CDM	FHSS/THSS	OFDM	CSMA/CA	EY-NPMA	DSMA/ ISMA	DAMA	TDMA	PRMA
D	+	+	+	+	+	+	-	-	-	-	-	-
S	-	-	-	-	-	-	+	+	+	+	+	+
*V***	А/Ц	А/Ц	-/Ц	А/Ц	А/Ц	А/Ц	А/Ц	А/Ц	А/Ц	А/Ц	А/Ц	А/Ц
*W****	М	М	Ф	М	М	М	М	М	М	М	М	М
X	-	-	-	-	GFSK	-	-	-	DBPSK/ DQPSK	-	-	-

D – детерминированность, *S* – случайность, *V* – способ передачи, *W* – тип доступа, *X* – тип модуляции, * – на основе данных [1, 4]; ** : *А* – аналоговый, *Ц* – цифровой; *** : *Ф* – фиксированный, *М* – мобильный.

Множественный доступ с пространственным разделением (SDM) основан на разделении сигналов в пространстве, когда каждое беспроводное устройство может вести передачу данных только в границах пространственной области. С появлением аппаратуры и стандартов, обеспечивающих адаптивную перестройку мощности передатчиков абонентских и базовых станций (БС), антенн с перестраиваемой диаграммой направленности, данный метод получил широкое распространение в системах сотовой телефонной связи и системах с цифровым формированием диаграмм направленности.

Множественный доступ с частотным разделением (FDM) предполагает, что каждое устройство работает на строго определенной частоте, поэтому несколько устройств могут вести передачу данных. Это наиболее распространенный метод, используемый в современных системах беспроводной связи. Несмотря на это, данный метод приводит к неоправданному расходу частотных ресурсов, требуя выделения отдельной частоты для каждого беспроводного устройства.

Множественный доступ с временным разделением (TDM) является более гибким. В данном методе каналы распределяются по времени – каждый передатчик транслирует сигнал на одной частоте, но в различные, циклически повторяющиеся промежутки времени при строгой синхронизации процесса передачи. Данная схема удобна, так как временные интервалы динамично перераспределяются между уст-

ройствами БСПД. Недостаток TDM-методов – мгновенная потеря информации при срыве синхронизации в канале, например, из-за помех, случайных или преднамеренных (с участием нарушителей при осуществлении попыток НСД).

Мультиплексирование с кодовым разделением (CDM) предполагает передачу сигналов всеми передатчиками на одной частоте, но с различными базовыми кодами. Каждый передатчик заменяет каждый бит исходного потока данных на CDM-символ (кодовую последовательность длиной в 11, 16, 32, 64 бит, уникальную для каждого передатчика). Достоинство CDM-уплотнения заключается в повышенной защищенности и скрытости передачи данных: не зная кода, невозможно получить сигнал, а в ряде случаев – и обнаружить его присутствие. Недостаток – сложность технической реализации приемников и необходимость точной синхронизации передатчика и приемника для гарантированного получения пакета.

Методы расширения спектра посредством частотных и временных скачков (FHSS/THSS) обеспечивают определенную защиту от прослушивания и помех. Метод FHSS (частотного уплотнения с изменением частотной полосы) широко применяется в технологии Bluetooth. Метод временных скачков (THSS) аналогичен временному уплотнению, только моменты начала трансляции пакетов передатчика не строго периодичны, а изменяются по псевдослучайному закону. Метод реализован с системах связи со сверхширокой спектральной полосой компании Time Domain.

Метод мультиплексирования посредством ортогональных несущих (OFDM) – производная методов кодового и частотного уплотнения, используется в БСПД IEEE 802.11, DVB, является одним из основных механизмов стандартов IEEE 802.16e, LTE, CDMA200 Rev.C, сетей 4G. Весь доступный частотный диапазон разбивается на поднесущие. Передача данных ведется одновременно по всем поднесущим. Распределение поднесущих в ходе работы может динамически изменяться, что делает метод не менее гибким, чем FDM-метод.

Метод множественного доступа с детектированием несущей и предотвращением конфликтов (CSMA/CA) используется в БСПД стандарта IEEE 802.11. После определения незанятости канала время ожидания выбирается случайно в некотором временном промежутке (аналогично бесприоритетному множественному доступу с исключением (EY-NPMA)).

Метод множественного доступа с детектированием подавления (DSMA/ISMA) использует вышеприведенный принцип работы. Различие между DSMA и ISMA в том, что занятость канала определяется

посредством посылки БС пакета, в котором определяется статус канала. БС должна быть синхронизирована с передатчиками так, чтобы они не передавали данные во время передачи статуса канала. Современные БСПД используют сочетание механизмов централизованного назначения временных интервалов и методов конкурентного доступа. На первом этапе осуществляется резервирование временных интервалов, на втором – передача данных в отведенном интервале. Механизмы резервирования увеличивают время задержки получения пакета при слабой загрузке системы, но при этом обеспечивают ей более высокую пропускную способность.

Метод множественного доступа с распределением по запросу (DAMA) во многом аналогичен вышеприведенному и используется в спутниковых системах связи. Он относится к схемам с явным резервированием, когда каждый интервал для передачи резервируется явно.

Метод конкурентного доступа с резервированием (TDMA) предполагает, что каждому устройству назначается временной минииинтервал, в течение которого оно сообщает, будет ли передавать данные. Метод гарантирует каждой зарезервировавшей канал БС определенную пропускную способность. Остальные БС могут пересылать данные в течение не зарезервированных интервалов, но на принципах конкурентного доступа и без гарантии доставки пакетов.

Метод с резервированием пакетов (PRMA) основан на рассылке списка с распределением временных интервалов в начале каждого цикла центральным устройством. Передающее устройство регулярно получает список с зарезервированными интервалами и случайным образом принимает решение о том, в каком временном интервале можно передавать данные.

Описанные методы доступа к среде БСПД необходимо использовать в сочетании друг с другом. Так, для сетей GSM одновременно могут использоваться схемы уплотнения SDM, TDM и FDM, в системах стандарта IEEE 802.16 сочетаются технологии OFDM, CDM, FDM/TDM, SDM. Основная задача методов доступа к среде БСПД - организация совместного использования КС различными абонентами, разделение единого ресурса на каналы передачи. При этом разрешение конфликтов представляет собой один из подходов к организации безопасного совместного использования КС с минимальными потерями производительности БСПД. Алгоритмы разрешения конфликтов, реализованные в соответствующих методах, позволяют получить малую задержку при большом числе слабо нагруженных узлов, при этом устойчивости функционирования БСПД должно уделяться особое внимание.

5. Метод контролируемого многомодельного доступа. Разработанный метод, схема которого приведена на рисунке 3, предполагает учет различных способов доступа к среде передачи и адаптивный характер управления данным процессом.

Архитектуру БСПД представим в виде набора отдельных элементов, подсистем и логических связей между ними, свойства которых оговариваются стандартом. Она определяет набор сервисов и методы их предоставления. В рамках одного стандарта существуют различные способы физического соединения отдельных элементов, каждый такой способ является примером топологии сети. В целом архитектура БСПД представляет собой распределенную структуру с единым обслуживающим центром.

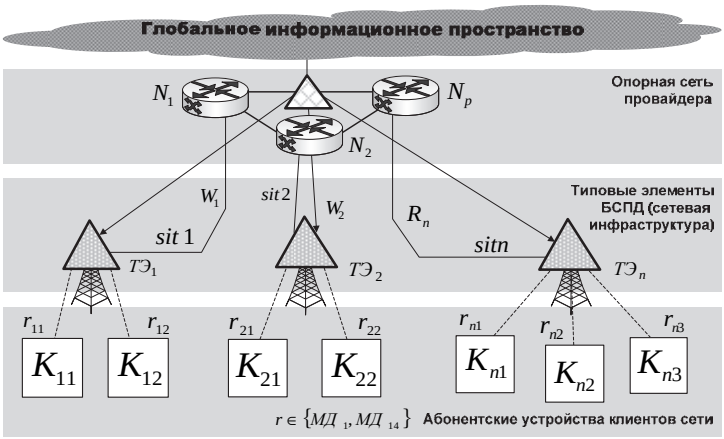


Рис. 3. Схема контролируемого многомодельного доступа к среде БСПД

Каждое абонентское устройство *K* в БСПД в зависимости от ее архитектуры, решаемых задач, особенностей аппаратной реализации и поддержки тех или иных сетевых сервисов может использовать различные методы доступа *МД*, или сочетания различных методов доступа, приведенные в таблице 1, к среде передачи, формируя логические каналы *r*. В общем случае $r \in \{МД_1, МД_{14}\}$.

В свою очередь, каждая БС или ТД, являясь элементом более высокого уровня сетевой инфраструктуры (типовым элементом), взаимодействует с опорной сетью провайдера. Введение в опорной сети провайдера дополнительного управляющего элемента (гипервизора) позволит управлять БС с использованием языка ситуационного управ-

ления [7, 9], в котором элементарный акт управления представляется в виде соотношения:

$$S_d; Q_j \overset{u_k}{\Rightarrow} Q_l,$$

где Q_j – текущая ситуация на БС (ТД); S_d – состояние системы управления и технология управления, которые допускают возможность использования u_k; u_k – воздействие (запрещение или разрешение доступа к БСПД с использованием определенного метода (комбинации методов)), которое преобразует текущую ситуацию Q_j в новую Q_l; Q_l – новая ситуация на БС (ТД).

Под текущей ситуацией $Q_j (j \in J)$ на БС (ТД) понимается совокупность всех сведений об используемых методах доступа абонентов в данный момент времени.

Полная ситуация [7] – это совокупность, состоящая из текущей ситуации, знаний о состоянии системы управления в данный момент времени и знаний о технологии управления.

Далее акт управления представим в виде продукции:

$$i; Q; P; A \Rightarrow B; N,$$

где i – имя (порядковый номер) продукции ($i \in I$, I – конечное множество); Q – сфера применения продукции (разделение на сферы позволяет ускорить процесс поиска нужной продукции); $A \Rightarrow B$ – ядро продукции; P – условие применимости ядра продукции (представляется в виде логического выражения (предиката)); N – постусловие продукции (действия и процедуры, которые необходимо выполнить после реализации В из $A \Rightarrow B$).

Отличительной особенностью ситуационного многомодельного доступа является высокая скрытность проводимых действий за счет маскирования под реальные элементы, характеристики которых, как и БСПД в целом, получены в ходе мониторинга беспроводных каналов связи.

Содержание метода раскрывается последовательным решением взаимосвязанных задач:

- выбора ПО для проведения мониторинга БСПД;
- определения мест нахождения клиента и времени его пребывания в них;
- определения точек устойчивого приема от клиента и от БС;
- манипуляции информационными потоками;
- добавления пользователя с соответствующими правами;
- внедрения специализированного ПО (СПО).

Успех доступа к среде БСПД объясняется прохождением информационного потока через открытую среду (радиоэфир). С точки зрения безопасности проводимых мероприятий наиболее оптимальными являются воздействия типа eavesdrop и address spoofing. Однако, применение методик, связанных с использованием СПО мониторинга, предоставляет значительно больше возможностей по сбору информации. Для сбора информации о БСПД необходимо выполнить последовательность действий $d_{i_j}^{сб}$: по одному $d_{i_j}^{сб}$ из каждого заданного множества $D_j^{сб}$. Каждое действие выполняется в течение известного времени $\Delta t^{сб}(d_{i_j}^{сб})$.

$$d_{i_1}^{сб} \in D_1^{сб}(i_1 \in I_1),\ d_{i_2}^{сб} \in D_2^{сб}(i_2 \in I_2),\ldots$$
$$d_{i_k}^{сб} \in D_k^{сб}(i_k \in I_k);$$
$$D_i^{сб} \cap D_j^{сб} = 0 (i \neq j; i, j = 1, k).$$

Качество собранных сведений определяется некоторой функцией φ:

$$\varphi(d_{i_1}^{сб}, d_{i_2}^{сб}, \ldots, d_{i_k}^{сб}) \in [0,1], \varphi \geq \varphi^{задан},$$

где $\varphi^{задан}$ - некоторое заданное значение функции φ, $\varphi^{задан} \in [0,1]$;

$$\Delta t^{сб}(d_{ij}^{сб}) \in (0, T_{задан}].$$

В соответствии с введенными выше терминами и обозначениями продукционная система адаптивного управления доступом к среде БСПД в системе продукции представления процессов мониторинга будет иметь вид:

$$PS_{дост.}^{(S)} = \{PR_{дост.}, BD_{дост.}, SY_{дост.}\},$$

где $PR_{дост.}^{(S)} = \{PR_1, PR_2, \ldots, PR_{10},\}$ – система продукций методов доступа, применимых в БСПД с идентификатором S, $BD_{дост.} = \{R_1, R_2\}$ – база данных с множеством отношений, $SY_{дост.} = \{Y_1, Y_2, \ldots, Y_{10}\}$ – множество элементов системы управления продукциями.

Например, если сумма характеристик анализируемых потоков в БСПД ($\sum = \lambda_1 V_1 + \lambda_2 V_2 + \ldots + \lambda_k V_k$, где λ - интенсивность анализируемых потоков пакетов, V - объем анализируемых пакетов, являющиеся контролируемыми параметрами) находится в пределах $0 \leq \sum \leq \lambda V_1$ –

осуществляется действие d_1 «обработка запросов всех устройств на интерфейсе *V_KPr* без выделения из них группы абонентов, являющихся клиентами ТД Td_2»:

$$\langle 1\rangle;\langle P_1(0,\sum,\lambda V_1)\rangle \xrightarrow{d_1} \langle P_2(V\_KPR,\ Td_2)\rangle,\langle 1,-\rangle,\langle F_1(t_k,t\_d1)\rangle,\langle 1,-,2\rangle .$$

Если сумма характеристик анализируемых потоков в БСПД ($\sum=\lambda_1 V_1+\lambda_2 V_2+...+\lambda_k V_k$) находится в пределах $\lambda V_1 \le \sum \le \lambda V_2$ – осуществляется действие d_2 «выделение из подключенных и идентифицированных на интерфейсе *V_KPr* клиентов БСПД группы абонентов *Gr_1* и установка для них приоритета обработки запросов»:

$$\langle 2\rangle;\langle P_1(\lambda V_1,\sum,\lambda V_2\rangle \xrightarrow{d_2} \langle P_2(V\_KPR,\ Gr\_1)\rangle,\langle 1,-\rangle,\langle F_1(t_k,t\_d_2)\rangle,\langle 1,-,3\rangle .$$

После установки приоритета обработки запросов появляется возможность осуществить доступ к БСПД с использованием протокола парольной аутентификации SRP [10, 12], устойчивый к прослушиванию канала, атакам перебора по словарю и «человек посередине» (MITM), не требующий третьей доверенной стороны и, тем не менее, не лишенный уязвимостей. Рассмотрим стадии информационного обмена в протоколе SRP (рисунок 4). С точки зрения реализации воздействия на данный протокол наиболее уязвимы стадии обработки и распространения запроса, а также ответа промежуточных узлов на запрос маршрута.

Рис. 4. Уязвимые стадии информационного обмена в БСПД с использованием протокола SRP

На этапе № 4, когда узел-источник *S* получает ответ, он проверяет адреса источника и приемника Q_{ID} и Q_{seq} и уничтожает ответ, если он не соответствует текущему ожидаемому запросу. Иначе, он сравнивает маршрут ответа от источника с обратным маршрутом внутри пакета ответа, а также поля SRP заголовка и $K_{s.t}$. В случае успешной проверки, *S* уверен в том, что запрос и ответ не были испорчены во время передачи. Таким образом, информация является подлинной.

На этапе № 5 появляется возможность модифицировать пакеты данных или ответы на запрос маршрута. Когда такие маршруты посылаются как ответы, объекты атаки записывают такие недействительные маршруты и могут использовать их в будущем. Поэтому для устойчивости к атакам, запись маршрута обычно не используется, и промежуточные узлы не обязаны отвечать на запросы маршрута. Если промежуточный узел N имеет активный маршрут к приемнику T, а между источником S и приемником N существует безопасная сессия, то приемник N может сгенерировать ответ. И это единственная ситуация, при которой запрос маршрута не достигает места назначения.

Если на предыдущих этапах цель (получение доступа к БСПД) не достигнута, задействуется последний из оставшихся доступных способов – действие d_{10} (если сумма характеристик анализируемого потока пакетов $(\sum=\lambda_1 V_1+\lambda_2 V_2+...+\lambda_k V_k)$ находится в пределах $4\lambda V_6 \le \sum \le 10\lambda V_6$):

$$\langle 10\rangle;\langle P_1(4\lambda V_6,\Sigma,10\lambda V_6)\rangle \xrightarrow{d_{10}} \left\langle P_6(W_s^* \mid \min_{i=\{1,2,...,k\}/(i^*\cup j^*\cup l^*)} \sum_i)\right\rangle,\langle 1,-\rangle,\langle t_k, t\_d_{10}\rangle,\langle 1,-,-\rangle.$$

В случае если все доступные методы доступа были задействованы, а цель воздействия не достигнута, осуществляется принудительное отключение всех используемых устройств и активация подсистемы сбора информации о БСПД.

При этом, разработанная подсистема контроля доступа позволяет: идентифицировать возможные события с негативными последствиями, определять, накапливать в локальной БД и анализировать ответные реакции стандартных средств информационной безопасности БСПД.

6. Заключение. Предложенный подход к обеспечению контролируемого многомодельного доступа позволяет осуществлять управление доступом (доступ запрещен, доступ разрешен, доступ разрешен с ограничениями) к среде передачи БСПД на основе ситуационного подхода к представлению и обработке результатов мониторинга, с использованием заранее определенных, практически отработанных способов, а также данных пассивного мониторинга об используемых протоколах и технологиях доступа, а также их влиянии на сетевую инфраструктуру и опорную сеть провайдера. Отличительной особенностью представленного подхода является ситуационная технология синтеза особых условий для работы системы мониторинга БСПД за счет анонимизации трафика. Для обеспечения скрытой передачи данных модификации подвергаются физические и логические параметры узлов БСПД.

При проведении дальнейших исследований видится целесообразным рассмотреть вопросы обеспечения требуемой устойчивости функционирования (в том числе при НСД), скорости передачи данных и минимизации задержек в БСПД в тесной взаимосвязи, что позволит

более глубоко понять природу уязвимостей соответствующих беспроводных протоколов, технологий и оборудования. Отдельным направлением выступает разработка методики определения последствий нежелательных событий и вычисления величины риска проведения процедур активного мониторинга БСПД.

Литература

1. *Nguyen L.T., Zhang J.* Wi-Fi fingerprinting through active learning using smartphones // UbiComp '13 Adjunct Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication. 2013, pp. 969-976.
2. *Беделл П.* Сети. Беспроводные технологии // М.: НТ Пресс. 2008. 448 с.
3. *Бейс Р.* Введение в обнаружение атак и анализ защищенности // М.: Информзащита. 1999. 298 с.
4. *Вишневский В.М.* Теоретические основы проектирования компьютерных сетей // М.: Техносфера. 2003. 512 с.
5. *Вишневский В.М., Портной С.Л., Шахнович И.В.* Энциклопедия WiMax. Путь к 4G // М.: Техносфера. 2010. 465 с.
6. *Климов С.М.* Методы и модели противодействия компьютерным атакам // Люберцы.: КАТАЛИТ. 2008. 316 с.
7. *Клыков Ю.И.* Ситуационное управление большими системами // М.: Энергия. 1974. 134 с.
8. *Котенко И.В., Саенко И.Б.* К новому поколению систем мониторинга и управления безопасностью // Вестник Российской академии наук. 2014. Том 84. № 11. С.993–1001.
9. *Поспелов, Д.А.* Ситуационное управление: теория и практика // М.: Наука. 1986. 288 с.
10. *Столлингс В.* Беспроводные линии связи и сети / Пер. с англ. // М.: Изд. Дом «Вильямс», 2003.
11. *Чирилло Д.* Обнаружение хакерских атак // СПб.: Питер. 2002. 864 с.
12. *Щербаков В.Б., Ермаков С.А.* Безопасность беспроводных сетей стандарта IEEE 802.11 // М: РадиоСофт. 2010. 255 с.

References

1. Nguyen L.T., Zhang J. Wi-Fi fingerprinting through active learning using smartphones. UbiComp '13 Adjunct Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication. 2013, pp. 969-976.
2. Bedell P. *Seti. Besprovodnye tehnologii* [Network. Wireless technology]. M.: NT Press, 2008. 448 p. (In Russ.).
3. Base R. *Vvedenie v obnaruzhenie atak i analiz zashhishhennosti* [Introduction to intrusion detection and security analysis]. M.: Informzaschita, 1999. 298 p. (In Russ.).
4. Vishnevsky V.M. *Teoreticheskie osnovy proektirovanija komp'juternyh setej* [Theoretical bases of designing computer networks]. M.: Technosphere. 2003. 512 p. (In Russ.).
5. Vishnevsky V.M., Portnoy S.L., Shahnovich I.V. *Jenciklopedija WiMax. Put' k 4G* [Encyclopedia WiMax. Path to 4G]. M.: Technosphere. 2010. 465 p. (In Russ.).
6. Klimov S.M. *Metody i modeli protivodejstvija komp'juternym atakam* [Methods and models to counter cyber attacks]. Lyubertsy: Katale. 2008. 316 p. (In Russ.).
7. Klykov Y.I. *Situacionnoe upravlenie bol'shimi sistemami* [Case management of large systems]. M.: Energia, 1974. 134 p. (In Russ.).
8. Kotenko I.V., Saenko I.B. [For a new generation of monitoring systems and security management]. *Vestnik Rossijskoj akademii nauk – Herald of the Russian Academy of Sciences*. 2014. vol. 84. no. 11. pp. 993–1001. (In Russ.).
9. Pospelov D.A. *Situacionnoe upravlenie: teorija i praktika* [Contingency management theory and practice]. M.: Nauka. 1986. 288 p. (In Russ.).

10. Stallings W. *Wireless Communications and Networking*. Prentice Hall. 2002. 576p. (Russ. ed.: Stollings V. *Besprovodnye linii svjazi i seti*. M.: Publishing. House "Williams", 2003. 640p.).
11. Cirillo D. *Obnaruzhenie hakerskih atak* [Detection of hacker attacks]. SPb.: Peter. 2002. 864 p. (In Russ.).
12. Shcherbakov V.B., Ermakov S.A. *Bezopasnost' besprovodnyh setej standarta IEEE 802.11* [Wireless Security standard IEEE 802.11]. M.: RadioSoft. 2010. 255 p. (In Russ.).

Аниканов Геннадий Александрович — соискатель кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: компьютерная безопасность, защита информации. Число научных публикаций — 2. nkcfm@rambler.ru; ул. Ждановская, д. 13, Санкт-Петербург, 197198; р.т.: +7(812)237-19-60.

Anikanov Gennadiy Aleksandrovich — applicant of systems for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: computer security, information protection. The number of publications — 2. nkcfm@rambler.ru; 13, Zhdanovskay street, St.-Petersburg, 197198, Russia; office phone: +7(812)237-19-60

Коновальчик Павел Михайлович — д-р техн. наук, профессор кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: компьютерная безопасность, защита информации. Число научных публикаций — 20. sklinsman@yandex.ru; Ждановская, д. 13, Санкт-Петербург, 197198; р.т.: +7(812)237-19-60.

Konovalchik Pavel Mikhailovich — Ph.D., Dr. Sci., professor of systems for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: computer security, information protection. The number of publications — 20. sklinsman@yandex.ru; 13, Zhdanovskay street, St.-Petersburg, 197198, Russia; office phone: +7(812)237-19-60.

Моргунов Владимир Михайлович — к-т техн. наук, старший преподаватель кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: защита информации. Число научных публикаций — 1. i9224966@icloud.com; Ждановская, д. 13, Санкт-Петербург, 197198; р.т.: +7(812)237-19-60.

Morgunov Vladimir Mikhailovich — senior lecturer of systems for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: information protection. The number of publications — 1. i9224966@icloud.com; 13, Zhdanovskay street, St.-Petersburg, 197198, Russia; office phone: +7(812)237-19-60.

Овчаров Владимир Александрович — к-т техн. наук, докторант кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: технологии мониторинга сетей, кластерный анализ. Число научных публикаций — 27. 9823800@inbox.ru; ул. Ждановская, д. 13, Санкт-Петербург, 197198; р.т.: +7(812)237-19-60.

Ovcharov Vladimir Aleksandrovich — Ph.D., doctoral student of systems for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: technology network monitoring, cluster analysis. The number of publications — 27. 9823800@inbox.ru; 13, Zhdanovskay street, St.-Petersburg, 197198, Russia; office phone: +7(812)237-19-60.

РЕФЕРАТ

Аниканов Г.А., Коновальчик П.М., Моргунов В.М., Овчаров В.А. **Контролируемый многомодельный доступ к среде беспроводных сетей передачи данных.**

В работе рассматривается задача разработки метода контролируемого многомодельного доступа к среде беспроводных сетей передачи данных стандартов IEEE 802.11, 802.16. В качестве решения предлагается продукционно-логическая система управления доступом к среде БСПД по результатам мониторинга, учитывающая влияние используемых методов на сетевую инфраструктуру.

Рассмотрены типы угроз и условия их реализации при пассивном и активном мониторинге трафика, а также при реализации несанкционированного доступа.

Показано, что большинство разработанных в настоящее время протоколов маршрутизации в БСПД имеют уязвимости в системе защиты. Анализируются дефекты протоколов маршрутизации, возможные атаки на эти протоколы и механизмы их реализации.

SUMMARY

Anikanov G.A., Konovalchik P.M., Morgunov V.M., Ovcharov V.A. **The Multi-Controlled Media Access to Wireless Data Networks.**

The problem of development of a method of controlled access to the multimodal environment of wireless data networks standards IEEE 802.11, 802.16 is considered. As a solution production-logic system to control access to a wireless network environment data on the monitoring results, which takes into account the effect of the methods used in the network infrastructure is proposed.

The types of threats and their conditions of implementation of the passive and active monitoring of traffic, as well as the implementation of unauthorized access are described.

It has been shown that the majority of currently developed routing protocols in wireless networks have security vulnerabilities. The defects of routing protocols, possible attacks on these protocols and their implementation mechanisms are analyzed.

РУКОВОДСТВО ДЛЯ АВТОРОВ

Взаимодействие автора с редакцией осуществляется через личный кабинет на сайте журнала «Труды СПИИРАН» http://www.proceedings.spiiras.nw.ru. При регистрации авторам рекомендуется заполнить все предложенные поля данных, так как это значительно ускорит процесс оформления метаданных к новым статьям.

Подготовка статьи ведется с помощью текстовых редакторов MS Word 2007 и выше. При подаче материала в редакцию сначала отправляется только статья в формате *.docx. Для обеспечения требований слепого рецензирования при представлении статьи в журнал авторам необходимо удалить персональные данные, содержащиеся в тексте файла и его свойствах.

Объем основного текста – от 5 до 20 страниц включительно. Формат страницы документа – A5 (148 мм ширина, 210 мм высота); ориентация – портретная; все поля – 20 мм. Верхний и нижний колонтитулы страницы – пустые. Основной шрифт документа – Times New Roman, основной кегль (размер) шрифта – 10 pt. Переносы разрешены. Абзацный отступ устанавливается размером в 10 мм. Межстрочный интервал – одинарный. Номера страниц не проставляются.

Не допускается использования цветных шрифтов, цветовых выделений и цветных рисунков. Статьи должны быть полностью готовы к черно-белой печати.

Основная часть текста статьи разбивается на разделы, среди которых являются обязательными: введение, хотя бы один «содержательный» раздел и заключение. Допускается также мотивированное содержанием и структурой материала выделение подразделов.

В основную часть допускается помещать рисунки, таблицы, листинги и формулы. Правила их оформления подробно рассмотрены на нашем сайте в разделе «Руководство для авторов».

ISSN 2078-9181
9 772078 918785 >

Вып. 1(38)
ТРУДЫ СПИИРАН
proceedings.spiiras.nw.ru
С-Пб
2015