МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ИЗВЕСТИЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ
ПРИБОРОСТРОЕНИЕ
ИЗДАНИЕ САНКТ-ПЕТЕРБУРГСКОГО НАЦИОНАЛЬНОГО ИССЛЕДОВАТЕЛЬСКОГО УНИВЕРСИТЕТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
Журнал издается с января 1958 г.

ТОМ 55 **АВГУСТ 2012** **№ 8**

ТЕМАТИЧЕСКИЙ ВЫПУСК

ПЕРСПЕКТИВНЫЕ МЕТОДЫ И СРЕДСТВА ОБРАБОТКИ ИНФОРМАЦИИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

Под редакцией доктора технических наук, профессора М. Ю. Монахова

СОДЕРЖАНИЕ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

THEMATIC ISSUE

PERSPECTIVE METHODS AND MEANS OF THE PROCESSING OF INFORMATION IN THE DATA TRANSMISSION NETWORK

By Edition of M. Yu. Monakhov, Doctor of Technical Science, Professor

CONTENTS

INFORMATION SECURITY OF DATA COMMUNICATION NETWORKS

Editor-in-Chief E. B. Yakovlev

ПРЕДИСЛОВИЕ

Формирование интегрированного информационного пространства в России является одной из приоритетных задач разработчиков систем. Эффективность и темпы ее решения в первую очередь зависят от качества проектирования и реализации коммуникационной инфраструктуры, которую составляют разнородные сети передачи данных (СПД), начиная от сотовых GSM- и CDMA-сетей и заканчивая корпоративными СПД со сложной разветвленной топологией.

С целью решения научно-практической задачи создания коммуникационной инфраструктуры и обеспечения качества ее функционирования необходимо разрабатывать новые технологии анализа и проектирования СПД, повышать эксплуатационные характеристики сетей, обеспечивать надлежащий уровень информационной безопасности.

Тематический выпуск журнала освещает проблемы и перспективы развития методов обработки и передачи информации. В него включены статьи научно-исследовательских коллективов кафедры информатики и защиты информации и кафедры вычислительной техники Владимирского государственного университета. Полученные в рамках совместной работы кафедр, выполняемой по госбюджетным и хоздоговорным НИР, результаты и внедрение их на предприятиях и в организациях Владимирской области и других регионах позволили выработать ряд практических рекомендаций по эффективному проектированию и использованию СПД.

Первый раздел выпуска посвящен технологиям анализа и проектирования сетей передачи данных. В статьях развивается методология проектирования сетевых устройств и протоколов, описывается опыт практического применения разработанных методов и средств СПД. Авторы предлагают новые подходы к оценке качества и помехоустойчивости каналов связи, описывают протоколы и механизмы, улучшающие характеристики процесса обмена данными.

Второй раздел содержит статьи, посвященные эффективной эксплуатации коммуникационной инфраструктуры. В работах предложены подходы к автоматизации администрирования сетей, направленные на обеспечение функциональной устойчивости корпоративной СПД, анализируются вопросы инвентаризации и ранжирования информационных ресурсов, представлен комплекс, предназначенный для контроля достоверности информации в ходе ее обмена.

Завершают тематический выпуск статьи, посвященные информационной безопасности сетей передачи данных, криптографическим методам защиты информации. Авторы исследуют воздействие информационных атак на производительность СПД.

Доктор технических наук, профессор
Владимирского государственного университета
им. А. Г. и Н. Г. Столетовых, М. Ю. МОНАХОВ

PREFACE

Formation of an integrated informational space in Russia is one of priority tasks for the designers of information systems. Effectiveness and rates of the task accomplishment depend primarily on the designs quality and on realization of the communication infrastructure constituted by various data communication networks (DCN), from cellular GSM and CDMA networks to corporate DCNs with complex branched topology.

It the framework of scientific and practical task of building the communication infrastructure and of providing its operational quality, it is necessary to develop new technologies for DCN analysis and design, and also to improve the networks operation quality and to ensure appropriate information security level.

This special topic issue of the journal highlights problems and perspectives of progress in methods of information processing and transmitting. It includes papers written by scientific research teams of Department of Informatics and Information Security and of Department of Computer Science at Vladimir State University. The results obtained from budget and commercially funded collaborative work of the departments were implemented at enterprises and organizations of Vladimir and other regions. These achievements made it possible to formulate a series of practical recommendations aimed at effective design and utilization of DCNs.

The first Section of the issue is devoted to the technologies of analysis and design of the data communication networks. In the papers a methodology of network devices and protocols design is progressed and an experience in practical applications of the developed DCN methods and means is described. The authors propose new approaches to evaluation of the communication links quality and noise resistance, and present protocols and mechanisms improving the data exchange quality.

The second Section contains articles devoted to effective operation of communication infrastructure. The papers propose approaches to automation of the networks administration focused on providing functional stability of the corporate DCNs. The papers also analyze topics of inventory and ranging of information resources and present a toolset for control of the information authenticity during the data exchange.

This special topic issue is concluded with articles considering the digital communication networks security and the cryptographic methods of the information protection. The authors investigate how the informational attacks affect the DCNs performance.

Doctor of Technical Sciences,
Professor M. Yu. MONAKHOV

ТЕХНОЛОГИИ АНАЛИЗА И ПРОЕКТИРОВАНИЯ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

УДК 621.376.9

А. С. Меркутов, Д. В. Крутин, А. Н. Числав, А. А. Плетнев

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ СОЗДАНИЯ ЦИФРОВОЙ РАДИОСТАНЦИИ НА ОСНОВЕ КОГЕРЕНТНОГО ПРИЕМА GMSK-СИГНАЛОВ

С использованием САПР ADS исследована помехоустойчивость цифрового демодулятора при введении отстроек по несущей и тактовой частоте. Разработан макет радиостанции УКВ-диапазона и экспериментально проверена возможность ее использования в составе аппаратуры, работающей в системе радиосвязи с шагом сетки частот 6,25 и 3,125 кГц.

Ключевые слова: *УКВ-радиостанция, GMSK, узкополосный прием, когерентный демодулятор.*

Постоянный рост числа абонентов современных систем сухопутной подвижной радиосвязи, работающих в УКВ-диапазоне (например, 148—174 МГц), требует повышения спектральной эффективности передачи цифровой информации по радиоканалу с обеспечением всех требований международных стандартов [1]. В современной аппаратуре, как правило, используется шаг канальной частотной сетки 25 или 12,5 кГц, рассчитанный, в первую очередь, на полосу частот, требуемую для передачи FSK-сигнала с индексом модуляции больше единицы, и применение некогерентной демодуляции. Использование относительной фазовой модуляции с предварительной фильтрацией позволяет несколько сузить спектр передаваемого сигнала, однако при этом снижается энергетическая эффективность работы радиопередающих и радиоприемных трактов, что уменьшает срок работы аккумуляторных батарей в портативных устройствах и снижает помехоустойчивость радиоканала.

Цель настоящей работы заключается в исследовании возможности создания перспективной портативной радиостанции, обеспечивающей реализацию шага частотной сетки 6,25 и 3,125 кГц на основе выпускаемой современной промышленностью элементной базы. Для передачи сигнала по радиоканалу было предложено использовать GMSK-модуляцию с контролируемой величиной параметра BT (где B — полоса гауссова предмодуляционного фильтра по уровню –3 дБ; T — длительность информационного символа), что позволило обеспечить формирование модулированного сигнала с высокой спектральной эффективностью и максимально сузить полосу пропускания тракта промежуточной частоты принимаемого цифрового сигнала. Кроме того, пакетная идеология передачи цифровых данных в сеансе связи, широко используемая в современных радиостанциях, дает возможность применить методы когерентной демодуляции принятого сигнала при цифровой обработке в приемном тракте.

Исследования показали, что при шаге сетки частот 6,25 кГц качественная передача речевого сигнала возможна при модуляционной скорости 4 кбит/с. Для параметра GMSK-

сигнала BT = 0,25 уровень излучения в соседний канал составляет γ = –69 дБ, что отвечает (с запасом) требованиям международного стандарта [1].

Известно, что оптимальная демодуляция GMSK-сигнала как разновидности сигнала модуляции с непрерывной фазой (CPM) осуществляется на основе алгоритма Витерби. Сигналы GMSK при незначительных ограничениях также могут приниматься двухканальным MSK-приемником.

Синтезированная оптимальная структура демодулятора MSK-сигнала представлена в работе [2], там же рассмотрена структура приемника при учете флуктуирующей фазы центральной частоты и точно известной задержке цифрового сигнала. В работе [3] рассмотрены особенности синтеза модели приемника GMSK-сигнала при флуктуирующих значениях фазы центральной тактовой частоты. Один из вариантов модели приведен на рис. 1.

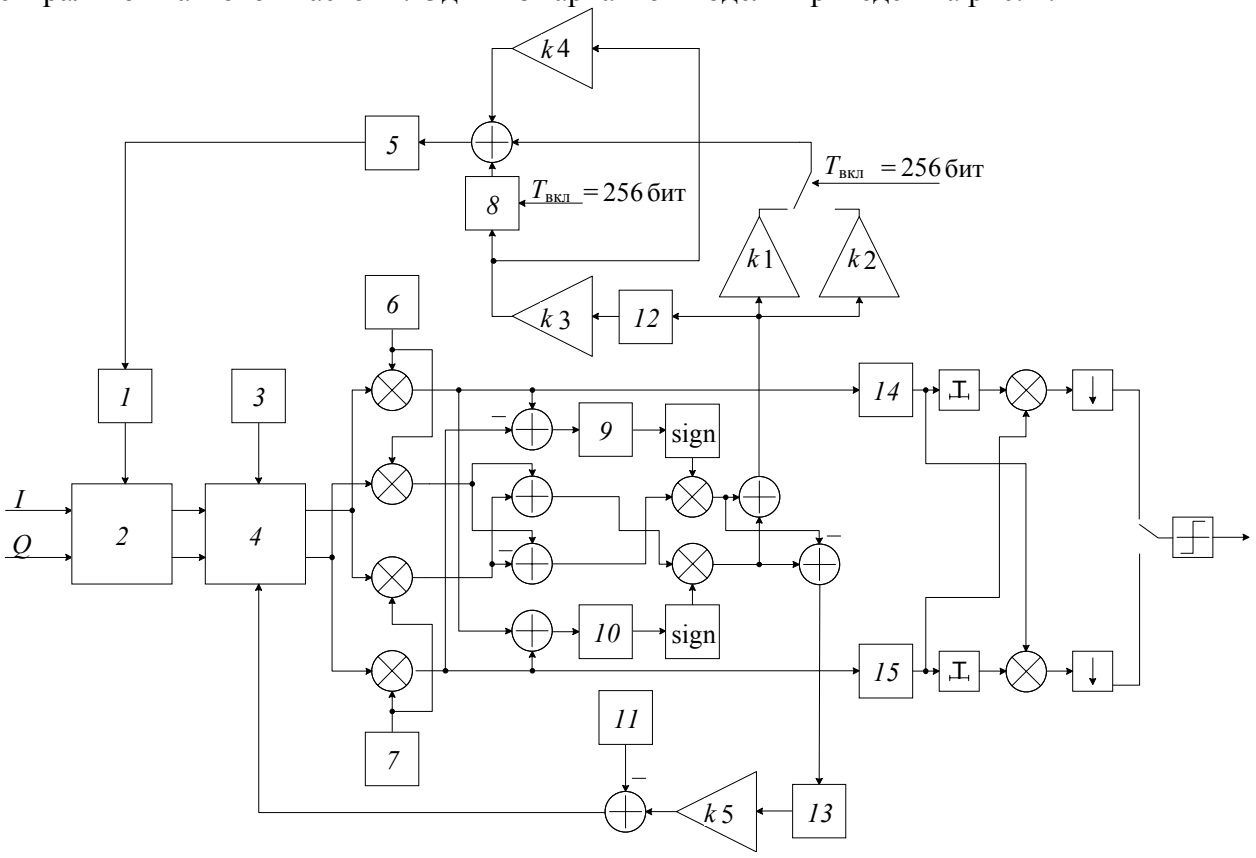


Рис. 1

При сеансовой связи передается преамбула, содержащая немодулированную центральную и четвертьтактовую частоту. Модели блоков детектирования (см. рис. 1) соответствуют функциональным схемам, приведенным в статьях [3, 4], здесь *1* — блок определения cosφ и sinφ, φ — рассогласование по частоте; *2* — комплексный множитель; *3* — блок определения начальной задержки; *4* — блок варьируемой задержки; *5* — интегратор; *6* — генератор $\sin(2\pi/4T)$; *7* — генератор $\cos(2\pi/4T)$; *8* — начальная отстройка частоты; *9*, *10* — скользящее суммирующее окно длиной T; *11* — фиксированное смещение оценки текущей задержки, *12* — скользящее суммирующее окно с периодом $200T$; *13* — скользящее суммирующее окно с периодом $900T$; *14* — интегратор на интервале $[(2k + 1)T, (2k + 1)T]$; *15* — интегратор на интервале $[(2k + 1)T, 2kT]$). Характеристики следящих петель фазовой и тактовой синхронизации исследованы в статье [4].

Проведено моделирование работы демодулятора при BT=0,4 с использованием подсистемы имитационного моделирования САПР Advanced Design System (ADS). Моделирование проводилось как для случая идеальной тактовой и фазовой синхронизации, так и для случая уходов несущей и тактовой частоты.

На рис. 2 приведены результаты расчета зависимости вероятности битовой ошибки ($P_{ош}$) от отношения средней энергии бита к спектральной плотности шума (E_b/N_0) — в условиях идеальной фазовой и тактовой синхронизации, а также при наличии относительных расстроек несущей ($\delta_н = \Delta F_н / F_{т0}$) и тактовой ($\delta_т = \Delta F_т / F_{т0}$) частоты. Здесь $\Delta F_н, \Delta F_т$ — абсолютные уходы несущей и тактовой частоты соответственно, $F_{т0}$ — номинальная тактовая частота. Также моделировалась работа демодулятора при нарастающем отклонении частоты, т.е. исследовалось влияние допплеровского эффекта при изменении скорости движения передатчика или приемника. Моделирование смещений тактовых отсчетов показало, что петля тактовой автоподстройки может компенсировать как скачкообразные, так и плавные (медленные) уходы тактовой частоты. Было установлено, что в режиме отслеживания медленных уходов несущей и тактовой частоты при их скачкообразном изменении с относительной расстройкой $\delta_н \le 0,0003$ и $\delta_т \le 10^{-4}$ помехоустойчивость демодулятора будет соответствовать кривой *1* на рис. 2 (*1* — случай идеальной синхронизации, начальная отстройка $\delta_н$ <=0,005; *2* — при скачке несущей частоты с $\delta_н = 10^{-3}$; *3* — при скачке тактовой частоты с $\delta_т = 10^{-3}$).

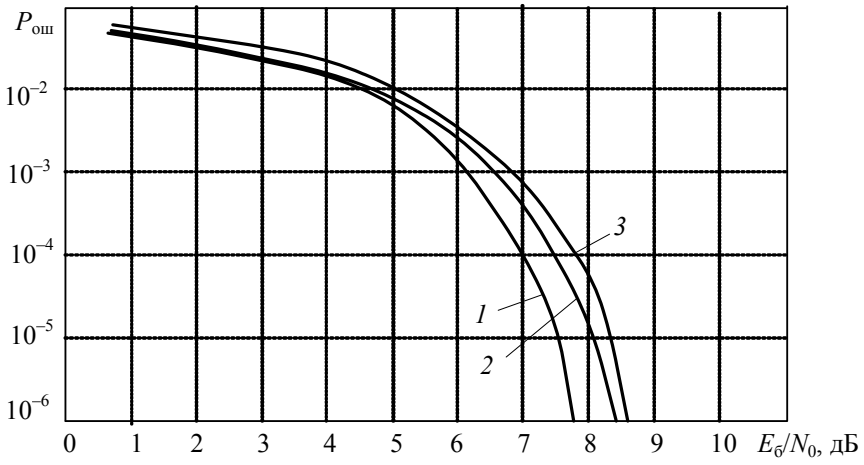


Рис. 2

В ходе исследований была также разработана структурная схема аналоговой части радиостанции. За основу при построении радиоприемного тракта была принята супергетеродинная схема с двумя преобразованиями частоты (рис. 3).

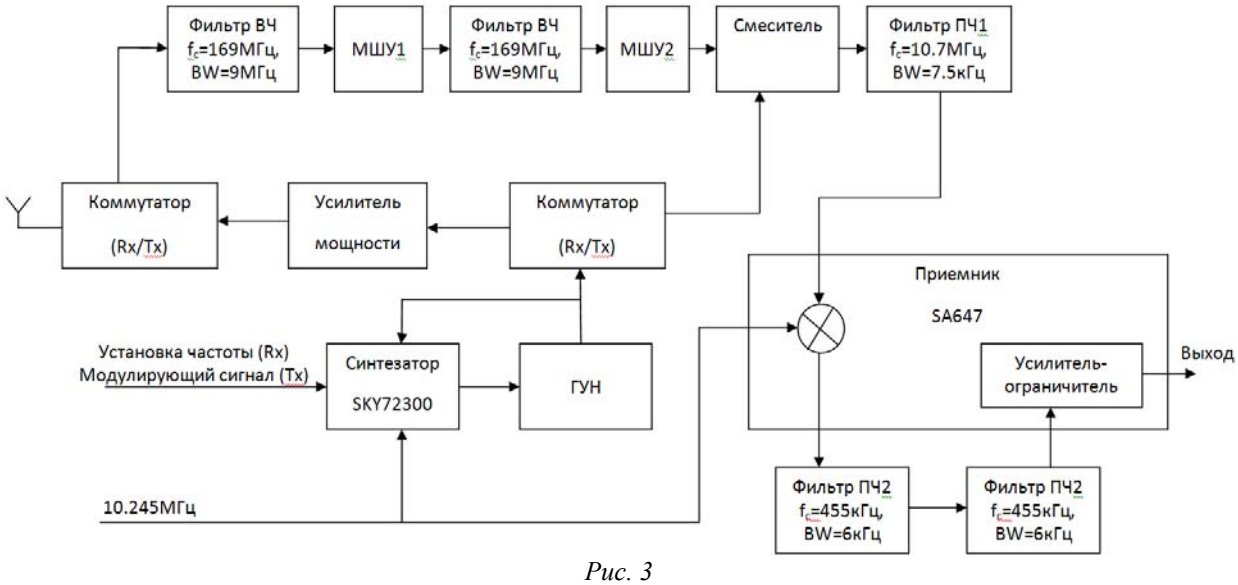


Рис. 3

Относительно узкая полоса входных частот (165—173 МГц) позволила использовать в преселекторе два фильтра на поверхностных акустических волнах, а также установить достаточно низкую первую промежуточную частоту (ПЧ) — 10,7 МГц. Это дало возможность выбрать стандартный кварцевый фильтр первой ПЧ с полосой пропускания 7,5 кГц и обеспечить более высокую стабильность частоты второго гетеродина, что очень важно при приеме узкополосных сигналов и использовании когерентных методов демодуляции, позволяющих отслеживать и компенсировать медленные изменения фазы и частоты в течение сеанса связи. В качестве первого каскада малошумящего усилителя был выбран биполярный транзистор AT45511 с хорошими динамическими характеристиками и малым коэффициентом шума. Тракт второй ПЧ (455 кГц) был реализован на микросхеме интегрального приемника SA647 с парафазными выходами и фиксированной частотой сигнала гетеродина 10,245 МГц, формируемого опорным кварцевым генератором со стабильностью не хуже 1 ppm. Основную избирательность по соседнему каналу в данном случае обеспечили два внешних керамических фильтра второй ПЧ, включенные последовательно и имеющие суммарную полосу пропускания около 5 кГц. Возможность перестройки частоты с требуемым шагом (3,125 кГц) и минимальными фазовыми шумами была реализована синтезатором частоты SKY72000 с переменно-дробным коэффициентом деления. Проведенный анализ системы фазовой автоподстройки частоты [4] и последующие исследования макета показали, что уровень фазовых шумов синтезатора на полосе 20 кГц вызывает среднеквадратичное отклонение фазы в опорном сигнале не более 0,5° (рис. 4, *1*), что практически не должно отразиться на работе когерентного демодулятора. Ограниченные по уровню парафазные сигналы с выхода тракта второй ПЧ поступают на вход квадратурного разделителя, реализованного в цифровой части радиостанции. Выходные сигналы разделителя являются входными для GMSK-демодулятора (рис. 1).

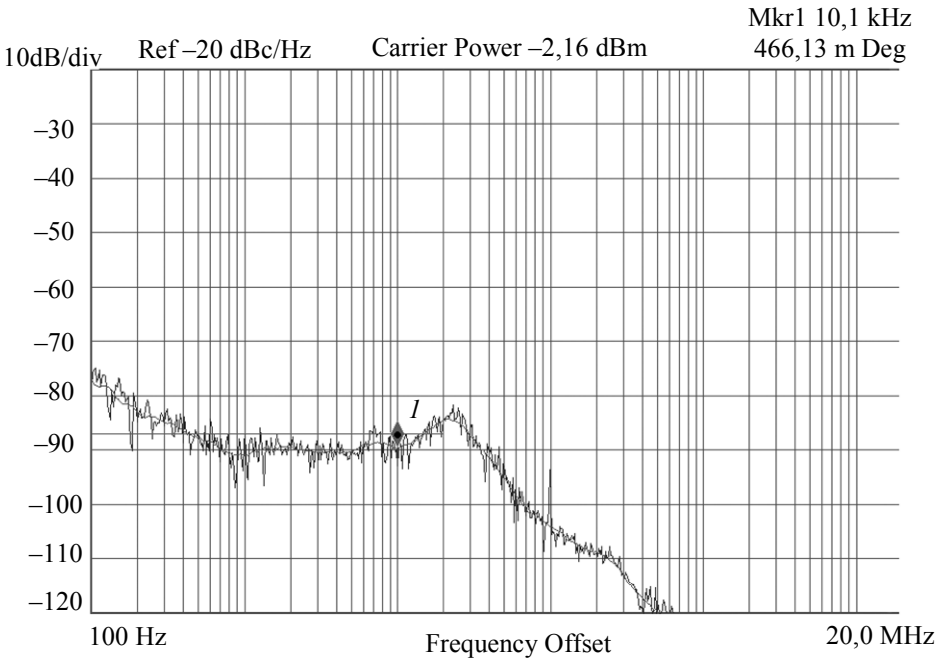


Рис. 4

Для формирования GMSK-сигнала в тракте передатчика было предложено использовать метод прямого синтеза сигнала на несущей частоте, который активно применяется в микросхемах интегральных трансиверов и может обеспечить высокую точность установки частоты девиации. Это позволило существенно снизить сложность аппаратуры и в то же время получить приемлемые значения побочных излучений в узкой полосе частот — не более –70 дБн, соответствующие требованиям международного стандарта. В результате включения на выходе усилителя мощности LC-фильтра 4-го порядка удалось снизить уровень второй гармоники

до –60 дБ относительно несущего сигнала. При проведении измерений был использован аттенюатор с коэффициентом ослабления 20 дБ.

На основании проведенных исследований были разработаны макеты радиостанции, по габаритам соответствующие типовым промышленно выпускаемым аналогам. В ходе экспериментальных исследований макета радиостанции получены следующие основные результаты: чувствительность радиоприемного тракта (скорость цифрового потока 3600 Бод, GMSK-сигнал, относительная битовая ошибка — 0,03) — не более –127 дБм; избирательность по побочным каналам приема — не менее 65 дБ; избирательность по соседнему каналу (отстройка — 6, 25 кГц) — не менее 50 дБ; уровень побочных излучений передатчика в полосе 1 ГГц — не более –60 дБн; уровень побочных излучений на частоте соседнего канала (±6,25 кГц) — не более –80 дБн; мощность передатчика — 1,6 Вт.

Сравнение экспериментальных результатов с техническими характеристиками выпускаемых аналогов показывает целесообразность использования полученных схемотехнических и алгоритмических решений при разработке перспективной связной аппаратуры нового поколения.

СПИСОК ЛИТЕРАТУРЫ

1. ETSI 300 113: June, 1996.

2. *Белоусов Е. Л., Харисов В. Н.* Оптимальный прием частотно-манипулированных сигналов с минимальным сдвигом // Радиотехника и электроника. 1984. № 3. С. 440—449.

3. *Королев Н. В., Меркутов А. С., Крутин Д. В.* Исследование помехоустойчивости квазиоптимального приемника GMSK-сигнала при реализации его цифровой части на ПЛИС // Вестн. Воронежского института МВД России. 2010. № 4. С. 38—42.

4. *Меркутов А. С., Крутин Д. В.* Фазовая и тактовая синхронизация сигналов в когерентном MSK-приемнике // Матер. IX Междунар. НТК „Перспективные технологии в средствах передачи информации“. Владимир: ВлГУ, 2011. Т. 2. С. 181—183.

Сведения об авторах

Александр Сергеевич Меркутов — канд. техн. наук, доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра вычислительной техники; E-mail: merkutov@yandex.ru

Денис Викторович Крутин — Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра вычислительной техники; инженер; E-mail: krutin.denis@gmail.com

Андрей Николаевич Цислав — Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра вычислительной техники; научный сотрудник; E-mail: cislav@yandex.ru

Александр Александрович Плетнев — Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра вычислительной техники; научный сотрудник; E-mail: Alexandr.Pletnerv@gmail.com

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.

УДК 621.376.9

Д. В. Крутин, М. А. Кисляков, С. Г. Мосин

МЕТОДЫ ОЦЕНКИ КАЧЕСТВА КАНАЛА СВЯЗИ. ТЕХНОЛОГИЯ WCDMA

При функционировании систем сотовой связи, использующих кодовое разделение каналов, необходимо контролировать мощность абонентского терминала путем оценки отношения сигнал—шум (ОСШ). Предложены методы определения ОСШ с использованием технологии WCDMA.

Ключевые слова: *WCDMA, кодовое разделение каналов, ОСШ.*

Поскольку современное общество все больше нуждается в передаче больших объемов информации, разработка и исследование алгоритмов приема и обработки сигналов в многоканальных системах мобильной цифровой связи весьма актуальны. В наши дни основная нагрузка по передаче информации приходится на системы связи третьего поколения, среди которых наибольшее распространение в Европе и России получила технология WCDMA.

WCDMA (Wideband Code Division Multiple Access) — одна из технологий многостанционного доступа, которая использует кодовое разделение каналов и обеспечивает высокую скорость передачи данных. В качестве основного типа модуляции используется QPSK (Quadrature Phase Shift Keying). В таких системах для разделения сигналов применяют скремблирующие коды, уникальные для каждого абонентского терминала. В качестве таких кодов используют коды Голда благодаря хорошим авто- и взаимокорреляционным свойствам [1, 2].

В системах связи с кодовым разделением каналов полоса частот используется одновременно несколькими абонентами. Поэтому для каждого абонента сигналы других пользователей сети являются помехой, которая может ухудшить качество связи. В случае, когда базовая станция (БС) одновременно работает с несколькими абонентскими терминалами (АТ), мощность сигнала от АТ, расположенных вблизи, значительно выше, чем у находящихся на значительном удалении. Таким образом, качество канала связи между БС и удаленным АТ резко ухудшается при появлении АТ в ближней зоне. Поэтому возможность точного и быстрого управления мощностью является одним из наиболее важных аспектов функционирования систем связи стандарта WCDMA.

Для решения этой проблемы в технологии WCDMA применяется быстрое управление мощностью по замкнутому контуру. Критерием оценки в этом случае является отношение сигнал—шум (ОСШ).

В радиоинтерфейсе WCDMA используют фреймы длительностью 10 мс, состоящие из 15 слотов, в каждом из которых в специальных полях (TPC) передают команды управления мощностью. На рис. 1, *а* представлена структура слота восходящего канала управления; *б* — нисходящего [3].

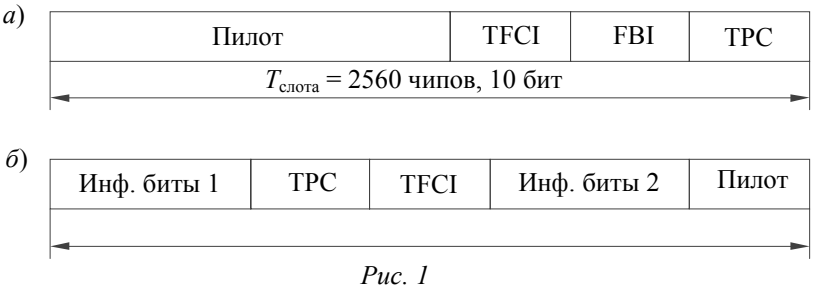


Рис. 1

Если измеренное ОСШ выше необходимого, то базовая станция посылает команду АТ понизить мощность, в противном случае — повысить. Такие измерения производятся 1500

раз в секунду (1,5 кГц) для каждого АТ, т.е. чаще, чем могут возникать изменения в канале связи. Таким образом, управление мощностью по замкнутому контуру позволяет предотвратить какой-либо ее дисбаланс для всех восходящих каналов, принимаемых БС. Иными словами, целью контроля мощности является достижение минимального уровня ОСШ, достаточного для обеспечения качественного приема сигнала.

Для регулировки мощности используются две вложенные петли управления (рис. 2). Внутренняя (быстрая) петля управления мощностью оценивает ОСШ восходящего канала и сравнивает полученное значение с целевым параметром. На основе результатов сравнения по нисходящему каналу передаются команды управления мощностью для АТ. Целевое значение ОСШ устанавливается внешней (медленной) петлей управления мощностью на основе измерений уровня блоковой ошибки BLER (Block Error Rate), проводимых с частотой 10—100 Гц [2].

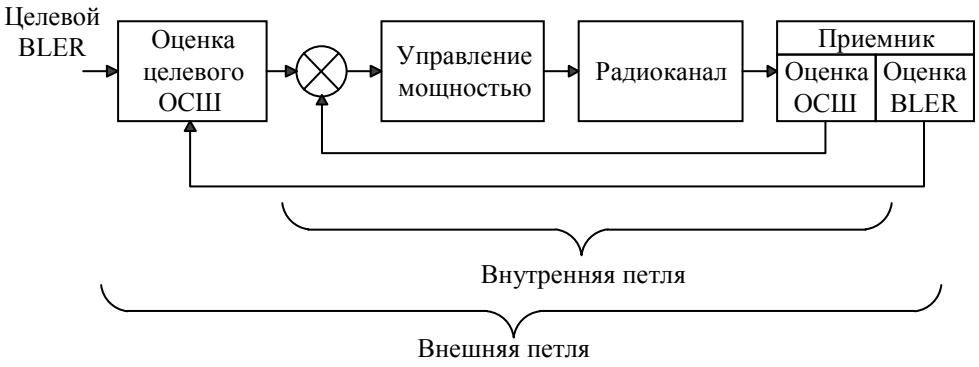


Рис. 2

Для повышения скорости передачи в восходящем канале также применяется модуляция более высокого порядка (4PAM), которая требует точной оценки мощности принимаемого сигнала. Неточная оценка ОСШ негативно влияет на работу петли контроля мощности между БС и АТ, что, в свою очередь, снижает возможности увеличения скорости передачи данных в восходящем канале. В настоящей работе представлено несколько методов оценки ОСШ, обеспечивающих достаточно высокую точность.

В большинстве случаев оценку отношения сигнал—шум удобно проводить на основе специальных последовательностей символов пилот-канала, применяемых для фазовой и частотной подстройки. В зависимости от формата в слоте может передаваться от трех до восьми символов [3]. Поскольку сигнал управления передается в квадратурной составляющей, то последовательность извлеченных символов определяется следующим выражением:

$$s_i = \frac{1}{\mathrm{SF}} \sum_{n=1}^{\mathrm{SF}} [\mathrm{Im}(S_n) c_{256,k,n}], \tag{1}$$

где S_n — демодулированные символы, SF (Spreading Factor) — коэффициент расширения спектра, а $c_{256,k,n}$ — последовательность, используемая для расширения спектра [4]. Далее вычисляются значения параметров RSCP и ISCP:

$$\mathrm{RSCP}_i = \frac{1}{N} \sum_{n=1}^{N} (s_n p_n)^2 , \tag{2}$$

$$\mathrm{ISCP}_i = \frac{1}{N} \left(\sum_{n=1}^{N} s_n p_n \right)^2 , \tag{3}$$

где N — число символов пилот-канала в одном фрейме; p_n — детерминированная последовательность пилотных символов, определенная в работе [3].

Тогда ОСШ определяется по формуле:

$$\text{ОСШ}_i = \frac{\text{RSCP}_i}{\text{RSCP}_i - \text{ISCP}_i}. \quad (4)$$

Для обеспечения большей точности оценки также можно проводить усреднение ОСШ на нескольких фреймах, тогда итоговое значение вычисляется по формуле

$$\overline{\text{ОСШ}} = \frac{1}{A}\sum_{i=1}^{A} \text{ОСШ}_i, \quad (5)$$

где A — окно усреднения.

Проведенные исследования показали, что при частоте расчета 100 Гц погрешность оценки ОСШ не превышает 1 дБ, в то же время при использовании усреднения на нескольких фреймах точность значительно увеличивается. Однако в отдельных случаях данный подход не может применяться. Например, в канале случайного доступа (Random Access Channel, RACH) при установлении сеанса связи между АТ и БС необходима достаточно быстрая оценка параметров сигнала. Ниже приведен алгоритм расчета ОСШ, используемый при детектировании преамбулы в канале RACH.

На первом шаге вычисляется общая мощность принятого сигнала:

$$\text{RTWP} = \frac{1}{N}\left(\sum_{n=1}^{N} I_n^2 + Q_n^2\right), \quad (6)$$

где I_n, Q_n — синфазная и квадратурная составляющие сигнала, N — окно корреляции.

Сигнал на выходе корреляционного детектора, используемого для детектирования преамбул, определяется как

$$z_i = \frac{1}{N}\left(\sum_{n=1}^{N} S_i p_{i+n}^*\right), \quad (7)$$

где p_i — эталонный сигнал нормированной амплитуды.

При наличии преамбулы в слоте доступа на выходе детектора фиксируется ярко выраженный корреляционный отклик. Энергию полезного сигнала и мощность шума можно определить по выражениям:

$$e_i = \max\left(|z_i|\right), \quad (8)$$

$$n_i = \text{RTWP} - e_i. \quad (9)$$

В этом случае ОСШ определяется по формуле:

$$\text{ОСШ} = \frac{e_i}{n_i}. \quad (10)$$

Данный метод также позволяет с высокой точностью определять ОСШ в широком диапазоне значений. При интервале оценки в 500 мкс погрешность не превышает 1,5 дБ.

Основным достоинством представленных методов оценки ОСШ по сравнению с аналогичными решениями является высокая точность оценки и экономия ресурсов при практической реализации.

СПИСОК ЛИТЕРАТУРЫ

1. *Tanner R., Woodard J.* WCDMA – Requirements and Practical Design. NY: JohnWiley&Sons Ltd, 2004. 447 p.
2. *Holma H., Toskala A.* WCDMA for UMTS. Radio Access for Third Generation Mobile Communications. NY: JohnWiley&Sons Ltd, 2004. 481 p.
3. 3GPP TS 25.211. Physical channels and mapping of transport channels onto physical channels (FDD). 2010.
4. 3GPP TS 25.213. Spreading and modulation (FDD). 2010.

Сведения об авторах

Денис Викторович Крутин — Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра вычислительной техники; инженер; E-mail: krutin.denis@gmail.com

Максим Андреевич Кисляков — Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра вычислительной техники; младший научный сотрудник; E-mail: kislyakov.maxim@gmail.com

Сергей Геннадьевич Мосин — канд. техн. наук, доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра вычислительной техники; E-mail: smosin@vlsu.ru

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.

УДК 004.031.2

М. А. Кисляков, С. Г. Мосин, В. В. Савенкова

ПРОЕКТИРОВАНИЕ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

Рассмотрены теоретические вопросы проектирования беспроводных сенсорных сетей. Описаны отдельные этапы проектирования. Сети классифицированы по типу топологической структуры.

Ключевые слова: *беспроводная сенсорная сеть, маршрут проектирования, статическая топология.*

Использование беспроводных сенсорных сетей (БСС) является одним из наиболее активно развивающихся методов сбора и передачи данных. Прогресс в этом направлении в основном связан с расширением сферы применения таких сетей. Таким образом, вопрос унификации процесса проектирования БСС становится все более актуальным.

Сенсорные сети уже частично заняли свой сегмент рынка, большое количество компаний предлагают свои решения в области беспроводного мониторинга. Существующие аппаратно-программные комплексы БСС в основном предназначены для решения узкоспециализированных задач, что затрудняет процесс адаптации систем к изменяющимся условиям. Более того, даже при необходимости внесения небольших модификаций требуется пройти все этапы проектирования заново.

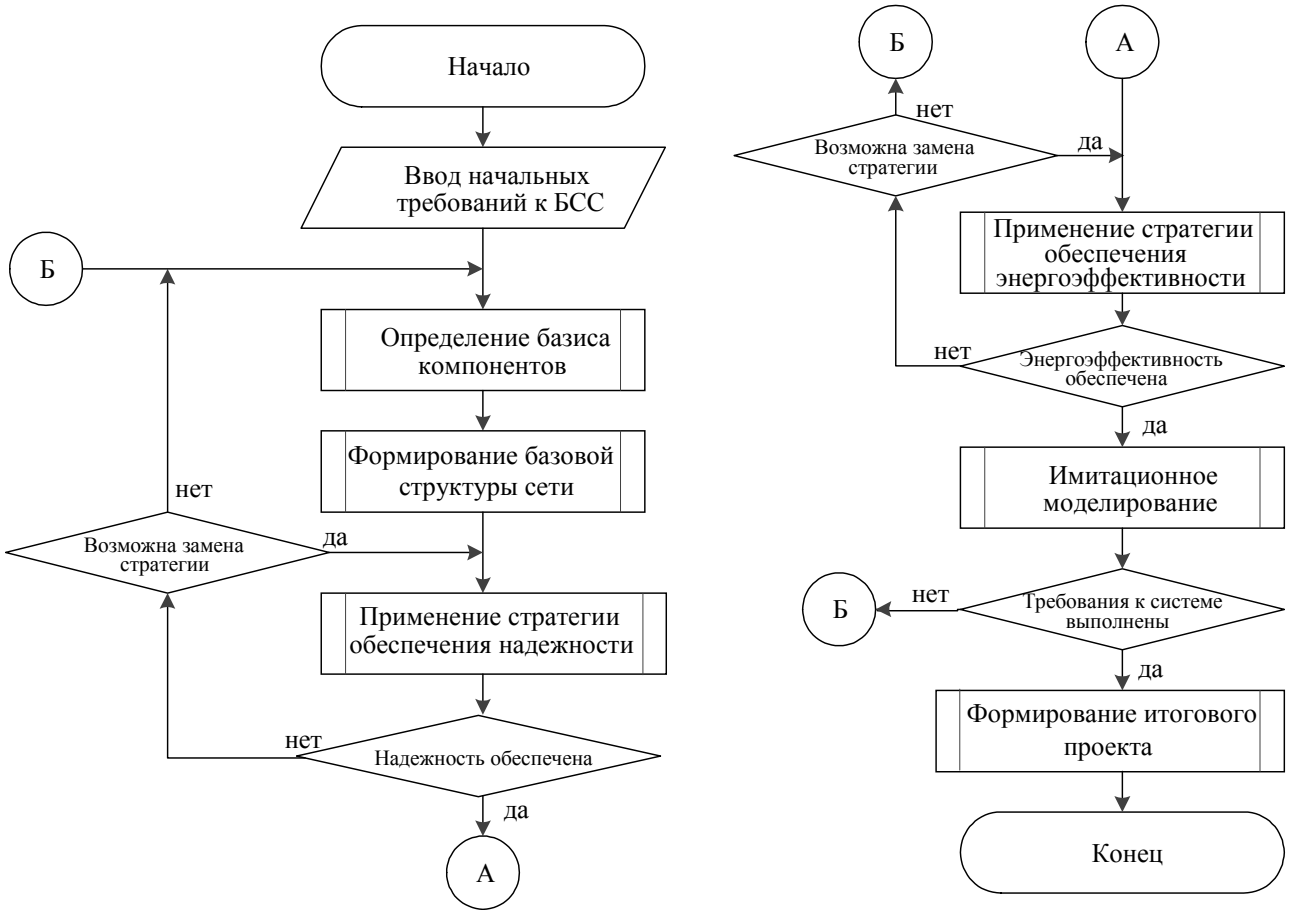
На данный момент унифицированных средств проектирования БСС не существует. Каждая компания использует собственные, закрытые для анализа характеристик разработки. По этой причине решения, ориентированные на выполнение одной конкретной задачи, не могут быть использованы в другой предметной области.

Беспроводная сенсорная сеть — это распределенная, самоорганизующаяся совокупность множества датчиков и исполнительных устройств, объединенных посредством радиоканала. Область покрытия подобной сети может составлять от нескольких метров до нескольких километров за счет ретрансляции сообщений от одного элемента к другому [1, 2].

Авторы работы [3] выделяют общие свойства сенсорных сетей, такие как ограниченное время функционирования узлов вследствие наличия автономного источника питания на каждом из них, ненадежная связь между узлами, поскольку радиоканал используется в качестве среды передачи, необходимость в самоорганизации — автоматической либо с минимальным участием человека.

Процесс проектирования сенсорной сети во многом зависит от ее целевой задачи. Однако разработка отдельных маршрутов для каждой задачи трудоемка и нецелесообразна.

В качестве классификационного признака может выступать тип топологической структуры, в соответствии с которым различают статические, слабодинамические и динамические системы [4]. В настоящей работе представлен процесс проектирования БСС со статической топологией узлов (см. рисунок). На основе блок-схемы рисунка можно выделить ряд основных этапов.



Ввод начальных требований к БСС, устанавливаемых на основе анализа целевой задачи. К списку требований следует относить такие параметры, как: жизненный цикл сети, зона покрытия, степень актуальности информации, скорость передачи данных и уровень надежности сети. Формализация ввода представленных параметров может иметь различную степень детализации, что определяет точность исходных данных. Формальное описание действий на этапе ввода начальных требований можно представить следующей формулой:

$$\mathbf{Q} = f(\mathbf{X}), \tag{1}$$

где $\mathbf{X} = \{x_1, \ldots, x_n\}$ — вектор начальных требований, $\mathbf{Q} = \{q_1, \ldots, q_n\}$ — вектор формализованных требований, $f(x)$ — функция формализации, n — количество требований.

Определение элементного базиса. Стремительное развитие технологии БСС в основном связано с теми достижениями в микроэлектронике, которые обеспечили формирование аппаратного базиса с должным уровнем технических характеристик. К числу основных параметров, анализируемых и используемых разработчиками в процессе проектирования сенсорных сетей, следует отнести: частотный диапазон; скорость передачи данных и дальность действия, чувствительность и выходную мощность сигнала, напряжение питания и токи потребления в режимах приема, передачи и сна. Этап определения элементного базиса предназначен для выбора подмножества электронных устройств, достаточных для построения проектируемой сети.

Пусть $S = \{s_1, \ldots, s_k\}$ — множество доступных электронных устройств. Тогда функцию определения элементного базиса можно представить в виде выражения

$$L = f(\mathbf{Q}, S), \tag{2}$$

где $L \subset S$ — подмножество доступных компонентов, выбранных системой или разработчиком на основе анализа вектора формализованных требований $\mathbf{Q}$, $f(x)$ — функция выбора подмножества элементов.

Формирование базовой структуры сети. Базовая структура определяет минимальный набор элементов сети, необходимых для выполнения целевой задачи. Основное требование к такой структуре — обеспечение связности топологии. На данной стадии решаются две подзадачи: сегментация сенсорной сети и построение связей между сегментами и основным шлюзом. Результат выполнения этапа формирования базовой структуры — построение многокластерной топологии сети с выделением узлов-координаторов в каждом из сегментов и расположение транзитных узлов для обеспечения связи с основным шлюзом. Функцию формирования базовой структуры можно выразить формулой:

$$(\mathbf{R}, T) = f(\mathbf{Q}, L), \tag{3}$$

где $\mathbf{R}$ — вектор связей между узлами сети, T — множество транзитных узлов, добавленных в сеть для обеспечения связей между кластерами, $f(x)$ — функция формирования базовой структуры.

Применение стратегии обеспечения надежности. Одна из основных характеристик сенсорной сети — степень ее надежности [5]. В данном контексте термины *надежность* и *отказоустойчивость* являются синонимами. Надежность определяет вероятность сбоя в работе системы при воздействии внешних факторов. Основным методом изменения надежности сети является перестроение ее топологической структуры. Очевидно, что сбои связаны с нарушением маршрутов следования информации от источника к приемнику. Такие нарушения возможны, например, при выходе из строя одного из транзитных узлов. Следовательно, увеличение количества возможных маршрутов передачи информации линейно повышает надежность системы в целом. Тем самым функцию обеспечения надежности можно представить следующими выражениями:

$$(\mathbf{R}', T') = f(\mathbf{R}, T, L), \tag{4}$$

где $\mathbf{R}'$ — вектор связей между узлами, дополненный новыми маршрутами, T' — множество транзитных узлов с учетом добавленных на данной стадии, $f(x)$ — функция добавления новых маршрутов;

$$y_r = g(\mathbf{R}', T', \mathbf{Q}), \tag{5}$$

где $y_r \in \{0,1\}$ — результат проверки надежности сети, $g(x)$ — функция проверки на надежность.

Применение стратегии обеспечения энергоэффективности. Задача обеспечения энергоэффективности сводится к повышению общего времени работы всей сети в целом. Решить такую задачу возможно, правильно разместив транзитные узлы, что позволит равномерно распределить нагрузку по всей сети и тем самым обеспечить минимальную дисперсию показателей среднего энергопотребления устройств. Второй способ достижения эффективного энергопотребления — настройка оптимального режима доступа к среде. Каждый из функциональных и транзитных узлов может находиться в одном из четырех режимов: передача, прием, вычисления и сон [6]. Минимизация временных интервалов, используемых режимами

с максимальным потреблением энергии, позволит увеличить общее время жизни сети. Функцию обеспечения энергоэффективности можно записать следующим образом:

$$(\mathbf{R}'', T'') = f(\mathbf{R}', T', L), \tag{6}$$

где $\mathbf{R}''$ — вектор связей между узлами, дополненный новыми маршрутами, T'' — множество транзитных узлов с учетом измененных и добавленных на этом этапе, $f(x)$ — функция перераспределения транзитных узлов с целью обеспечения энергетической эффективности,

$$y_e = g(\mathbf{R}'', T'', \mathbf{Q}), \tag{7}$$

$y_e \in \{0,1\}$ — результат проверки энергоэффективности сети, $g(x)$ — функция проверки на энергоэффективность.

Имитационное моделирование. На этом этапе осуществляется поведенческое моделирование спроектированной сенсорной сети. В процессе моделирования вычисляется ряд характеристик системы, которые являются основой для проведения многокритериального анализа. Если вычисленные характеристики соответствуют критериям, полученным на этапе ввода и анализа начальных требований, то инициируется переход к стадии генерации итогового проекта. В противном случае вносятся уточнения в проект, и этапы выполняются заново:

$$\mathbf{P} = f(\mathbf{R}'', T''), \tag{8}$$

где $\mathbf{P}$ — вектор выходных параметров спроектированной сети, $f(x)$ — функция расчета выходных параметров. Далее получим результат проведения многокритериального анализа по всему вектору $\mathbf{Q}$

$$y_c = g(\mathbf{P}, \mathbf{Q}), \tag{9}$$

где $y_c \in \{0,1\}$, $g(x)$ — функция многокритериального анализа.

Итоговое формирование проекта под конкретный аппаратный базис — завершающий этап маршрута. Реализация данного этапа представляет собой использование вектора выходных параметров $\mathbf{P}$ для настройки проекта. Результат процесса проектирования может быть представлен в виде скомпилированного конфигурационного файла, однозначно соответствующего выбранному аппаратному базису.

Совокупность этапов — маршрут проектирования — является основой для построения системы автоматизированного проектирования БСС. Такая САПР обеспечит унификацию средств и подхода к проектированию БСС.

СПИСОК ЛИТЕРАТУРЫ

1. *Akyildiz I. F., Su W., Sankarasubramaniam Y., Cayirci E.* Wireless Sensor Network: a Survey // Computer Networks J. 2002. Vol. 38. P. 393—422.

2. *Chong Chee-Yee, Kumar S. P.* Sensor Networks Evolution, Opportunities, and Challenges // Proc. IEEE. 2003. Vol. 91. N 8.

3. *Perillo M. A., Heinzelman W. B.* Wireless Sensor Network Protocols // Handbook of Algorithms for Wireless Networking and Mobile Computing. 2005. P. 813—842.

4. *Кисляков М. А., Савенкова В. В.* Классификация беспроводных сенсорных сетей по типу топологической структуры // 50-я Междунар. науч. студ. конф. „Студент и научно-технический прогресс“. 2012.

5. *Мочалов В. А.* Разработка и исследование алгоритмов построения отказоустойчивых сенсорных сетей: Автореф. дис. … канд. техн. наук. М., 2011.

6. *Мочалов В. А., Турута Е. Н.* Интеллектуальная САПР сенсорных сетей // Матер. конф. „Интеллектуальные САПР“. 2009.

Сведения об авторах

Максим Андреевич Кисляков — Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра вычислительной техники; младший научный сотрудник; E-mail: kislyakov.maxim@gmail.com

Сергей Геннадьевич Мосин — канд. техн. наук, доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра вычислительной техники; E-mail: smosin@vlsu.ru

Вероника Вячеславовна Савенкова — Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра вычислительной техники; инженер; E-mail: savenkova.nika@gmail.com

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.

УДК 681.5

С. Г. Мосин

МЕТОДИКА ТЕСТОПРИГОДНОГО ПРОЕКТИРОВАНИЯ АНАЛОГО-ЦИФРОВЫХ СХЕМ

Предложена методика тестопригодного проектирования аналого-цифровых схем с использованием параллелизма, поддерживающего одновременное выполнение проектных процедур на современных многоядерных или многопроцессорных вычислительных системах. Предусмотрена процедура выбора методов внешнего и внутрисхемного тестирования.

Ключевые слова: *тестопригодное проектирование, внутрисхемное тестирование, аналого-цифровые интегральные схемы, автоматизация проектирования, параллелизм.*

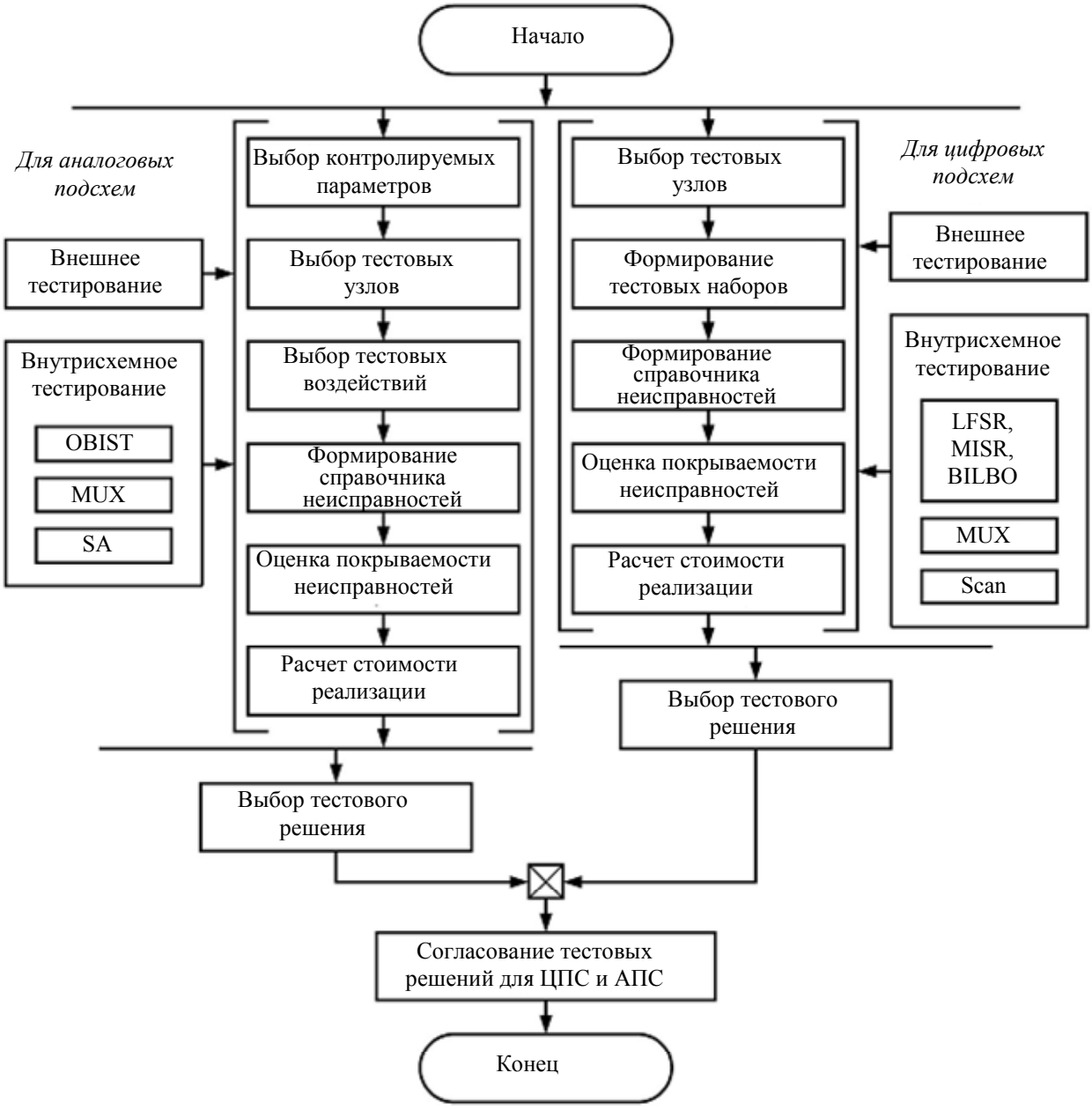
Особенность современных маршрутов проектирования интегрированной многопроцессорной системы (ИМС) — ориентация на тестопригодное проектирование (*DFT — Design for Testability*), в ходе которого наряду с разработкой интегральной схемы формируются решения и определяются сценарии, обеспечивающие в дальнейшем простоту ее тестирования [1—3]. При выборе варианта тестирования — внешнего или внутрисхемного — учитываются особенности метода (см. таблицу).

Сравнительная оценка методов внутрисхемного и внешнего тестирования

Характеристика	Внутрисхемное тестирование	Внешнее тестирование
Быстродействие	Высокое (+)	Низкое (–)
Дополнительная площадь кристалла	Требуется (–)	Не требуется (+)
Режим работы	Интерактивный/выделенный (+)	Только выделенный (–)
Используемое оборудование	Стандартное (универсальное) (+)	Специализированное (–)
Точность выполняемых измерений	Высокая (+)	Низкая (–)
Стоимость реализации	Высокая (–)	Низкая (+)

Для корректного выбора метода тестирования важно обеспечить автоматизацию всех процессов, как цифровой, так и аналоговой подсхемы проектируемого электронного устройства. Предлагаемая методика позволяет формализовать процесс выбора тестового решения (см. рисунок). Полученные количественные характеристики и результат стоимостного расчета используют при выборе наиболее эффективных методов тестирования для аналоговой и цифровой подсхем (АПС и ЦПС соответственно). Затем обеспечивается согласование этих

методов комплексного тестирования аналого-цифровой схемы. Для АПС в методике предусмотрен выбор между методом внешнего и методами внутрисхемного тестирования на основе введения дополнительных элементов, обеспечивающих автоматическую проверку (*OBIST — Oscillation Built-In Self-Test*) [4], использования мультиплексоров, повышающих наблюдаемость внутренних узлов схемы (*MUX*), и методов на основе сигнатурного анализа (*SA — Signature Analysis*) [2, 5]. Для ЦПС предложены методы внешнего и внутрисхемного тестирования на основе схем встроенного самотестирования (*LSFR — Linear Shift Feedback Register, MISR — Multi-Inpit Shift Register* и *BILBO — Built-In Logic Block Observer*), схем мультиплексирования внутренних узлов (*MUX*) и сканирующих цепей (*Scan*) [6].



При выборе контролируемых параметров (КП), тестовых узлов и тестовых воздействий для внешнего тестирования АПС используется анализ чувствительности. Амплитуда сигнала и его фазовый сдвиг рассматриваются в качестве КП. Для каждого КП формируют матрицу $\mathbf{S} \subset R(m, n)$, где m — число внутренних компонентов, n — число рассмотренных внутренних узлов. Элементы данной матрицы ($S_{i,j}$) — коэффициенты чувствительности выходного параметра схемы, контролируемого в узле j, к отклонению параметра (неисправности) компонента i.

Процесс выбора тестовых узлов сводится к поиску столбцов матрицы **S**, включающих наибольшее число максимальных значений коэффициентов чувствительности каждой строки (поиск минимального покрытия внутренних узлов максимальными значениями коэффициентов чувствительности всех компонентов).

Повысить вероятность обнаружения неисправностей можно, используя набор входных тестовых воздействий $\mathbf{T} \subset R(p)$, при этом формируется совокупность $\widehat{\mathbf{S}}$ матриц $S_{i,j}^{k}$, каждая из которых получена для определенного сигнала $T_k \in \mathbf{T}$, $1 \le k \le p$. Входные сигналы, матрицы $S_{i,j}^{k}$ для которых вошли в минимальное покрытие, образуют множество тестовых воздействий.

В методике выбор тестовых узлов и тестовых воздействий ЦПС реализуется с использованием разностной функции. Пусть $f_0(x_1, x_2, ..., x_n)$ — выходная функция комбинационной схемы, а $f_i(x_1, x_2, ..., x_n)$ — выходная функция схемы с неисправностью i. Тогда разностная функция неисправности имеет вид:

$$F_i(\mathbf{x}) \equiv F_i(x_1, x_2, ..., x_n) = f_0(x_1, x_2, ..., x_n) \oplus f_1(x_1, x_2, ..., x_n), \quad (1)$$

где $F_i(\mathbf{x})$ — функция, которая на входном наборе $\mathbf{x} = x_1, x_2, ..., x_n$ принимает значение 1, если значения $f_0(\mathbf{x})$ и $f_i(\mathbf{x})$ различны.

Входной тестовый набор $\mathbf{x}$ ($F_i(\mathbf{x}) = 1$) называется тестом неисправности *i.* В случае присутствия в схеме k неисправностей существуют k разностных функций $F_1(\mathbf{x})$, $F_2(\mathbf{x})$, …, $F_k(\mathbf{x})$. Тесты, полученные для данных неисправностей, образуют множество:

$$\mathbf{I} = \bigcup_{i=1}^{k} \left\{ \mathbf{x}^i \,\middle|\, F_i(\mathbf{x}^i) = 1 \right\}. \quad (2)$$

Данное множество входных наборов называют тестовым множеством, или тестовой последовательностью [1].

Выбор тестовых узлов. Пусть $F = \{f_0, f_1, ..., f_k\}$ является подмножеством всех возможных неисправностей **F**, включает список тех неисправностей, которые будут диагностированы, и $N = \{n_1, n_2, ..., n_p\}$ — подмножество внутренних узлов схемы **N**, содержит список всех доступных тестовых узлов. Основной результат работы метода — *таблица неисправностей* $C \subset R(k+1, p)$, строки которой, начиная со второй, соответствуют различным видам неисправностей, а столбцы — доступным тестовым узлам. Первая строка таблицы содержит характеристики исправной схемы. По результатам моделирования исправной схемы и схемы с заданным набором неисправностей F происходит формирование двойственных групп и определение всех неисправностей данных тестовых узлов N. Неисправности f_m и f_n принадлежат двойственной группе AG_j, связанной с тестовым узлом n_j, если $C_{mj} = C_{nj}$ ($m \ne n$). В итоге для каждого столбца получается конечное множество двойственных групп, которые нумеруются от 1 до m_p, где m_p — мощность этого набора для тестового узла p. Следует отметить, что неисправность, выявленная в определенном узле, может входить только в одну двойственную группу. Для удобства каждая ячейка $C_{ij} = c$ таблицы неисправностей содержит номер группы (AG_{cj}), сформированной для j-го узла и i-й неисправности. Схема является полностью диагностируемой с помощью множества тестовых узлов $N_f \subseteq N$, если для каждой пары неисправностей f_i и f_j ($i \ne j$) существует такой узел n_b ($\exists n_b \in N_f$), что $C_{ik} \ne C_{jk}$. Решение задачи выбора тестовых узлов является оптимальным, если число множеств N_f будет минимальным. Такое множество может быть сформировано на основе вычисления энтропии с использованием значения мощности двойственных групп.

Пусть X_{ij} ($i = 1, 2,\ldots,k$) — число элементов группы AG_{ij} для тестового узла n_j. Вероятность появления неисправности из группы AG_{ij} может быть вычислена как отношение AG_{ij} / k, где k — число диагностируемых неисправностей. Таким образом, энтропию для любого выбранного тестового узла n_j вычисляют с использованием выражения:

$$E_j = -\left[\frac{X_{1j}}{k}\log\left(\frac{X_{1j}}{k}\right)+\frac{X_{2j}}{k}\log\left(\frac{X_{2j}}{k}\right)+\ldots+\frac{X_{kj}}{k}\log\left(\frac{X_{kj}}{k}\right)\right] = \log(k)-\frac{1}{k}\sum_{i=1}^{k}X_{ij}\log\left(X_{ij}\right). \quad (3)$$

Количество информации, получаемой в тестовом узле n_j, становится максимальным при минимизации коэффициента энтропии:

$$ER_j = \sum_{i=1}^{k} X_{ij}\log\left(X_{ij}\right). \quad (4)$$

Тестовый узел n_j, значение $ER(j)$ в котором минимально, обеспечивает получение максимальной информации об измеряемой величине. Выбранные таким образом узлы образуют результирующее множество тестовых узлов. Алгоритм выбора тестовых узлов можно формализовать следующей последовательностью действий [2].

1. Вычислить число элементов в каждой двойственной группе для каждого тестового узла n_j.

2. Рассчитать коэффициент энтропии ER_j.

3. Добавить узлы с минимальным значением ER_j во множество выбранных ранее тестовых узлов.

4. Переформировать таблицу неисправностей в соответствии с порядком двойственных групп выбранного тестового узла, а также удалить из нее те строки, неисправности которых не входят ни в одну двойственную группу для данного узла.

5. Рассчитать коэффициент ER_j для оставшихся узлов с учетом присутствия двойственных групп в каждом из получившихся разделов таблицы неисправностей.

6. Если ER_j =0 (для всех j) или ER_j принимает то же значение, что и ранее (для всех j), процесс прекращается. В противном случае необходимо повторить пункты 3, 4.

Формирование справочника неисправностей. *Справочник неисправностей* (СН) — совокупность измерений характеристик исправной и потенциально неисправной схемы, полученных в результате моделирования работы устройства в нормальном режиме с учетом присутствия в ней неисправностей. Измерение контролируемых параметров выполняется во всех тестовых узлах при различных входных тестовых воздействиях. Процесс построения СН можно разделить следующим образом: формирование списка неисправностей; получение выходных откликов на входные воздействия при моделировании неисправности компонента схемы; формирование справочника неисправностей, обеспечивающее достижение компромисса между размерностью и количеством неисправностей.

Выбор метода тестирования (внешний или внутрисхемный) АПС и ЦПС смешанных ИМС производится с учетом расчета стоимости тестирования. Учитывается следующий набор параметров проектируемого устройства: используемая интегральная технология, объем партии изделий, сложность ИМС, соотношение площади аналоговой и цифровой подсхем, стоимость используемых САПР и *ATPG* и др.

В общем случае стоимость тестирования электронных схем составляет

$$C = C_{\text{prep}} + C_{\text{manuf}} + C_{\text{exec}}, \quad (5)$$

где C_{prep} — стоимость подготовки теста, C_{manuf} — стоимость производства тестирующей подсхемы, C_{exec} — стоимость выполнения теста.

Простейший способ выбора менее затратного метода тестирования основан на оценке и сравнении значения C для каждого решения. Выполнение неравенства $C_{\text{on}} > C_{\text{off}}$ (C_{on} и C_{off} — стоимость внутрисхемного и внешнего тестирования соответственно) — условие экономической эффективности использования внешнего тестирования, а $C_{\text{on}} < C_{\text{off}}$ — внутрисхемного [7, 8].

Заключение. Реализация предложенной методики в САПР интегральных схем позволяет автоматизировать процесс принятия решения в ходе тестопригодного проектирования. Ориентация алгоритмов на параллельную обработку и современные многоядерные и многопроцессорные варианты архитектуры вычислительных систем обеспечивает снижение временных затрат на проектирование и расширение числа возможных структурных решений внутрисхемного тестирования аналого-цифровых схем, рассматриваемых в ходе разработки.

Работа выполнена в рамках проекта № 7.4151.2011 Министерства образования и науки РФ.

СПИСОК ЛИТЕРАТУРЫ

1. *Киносита К., Асада К., Карацу О.* Логическое проектирование СБИС. М.: Мир, 1988.
2. *Ланцов В. Н., Мосин С. Г.* Современные подходы к проектированию и тестированию интегральных микросхем. Владимир: Изд-во ВлГУ, 2010.
3. *Мосин С. Г.* Исследование модели выбора оптимальной тестовой стратегии для смешанных интегральных схем // Вестн. компьютерных и информационных технологий. 2011. № 6. С. 24—28.
4. *Mosin S. G.* A Built-in Self-Test Circuitry Based on Reconfiguration for Analog and Mixed-Signal IC // Information Technology and Control. 2011. Vol. 40, N 3. P. 260—264.
5. *Mosin S.* Neural Network-Based Technique for Detecting Catastrophic and Parametric Faults in Analog Circuits // Proc. IEEE 18th Intern. Conf. on System Engineering (ICSEng'2005). Las Vegas, Nevada, USA, 2005. P. 224—229.
6. *Mosin S. G., Chebykina N. V., Serina M. S.* Technique of LFSR Based Test Generator Synthesis for Deterministic and Pseudorandom Testing // Proc. 11th Conf. "Experience of Designing and Application of CAD System in Microelectronics – CADSM'11". Polyana-Svalyava, Ukraine, 2011. P. 128—131.
7. *Мосин С. Г.* Выбор метода тестирования смешанных интегральных схем на основе экономической модели // Вестн. Костромского гос. ун-та им. Н. А. Некрасова. 2008. Т. 14, № 2. С. 29—32.
8. *Mosin S. G.* Selecting the Most Efficient DFT Techniques of Mixed-Signal Circuits Based on Economics Modeling // Proc. of IEEE East-West Design and Test Symp. (EWDTS'2007). Yerevan, Armenia, 2007. P. 158—161.

Сведения об авторе

Сергей Геннадьевич Мосин — канд. техн. наук, доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра вычислительной техники;
E-mail: smosin@vlsu.ru

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.

УДК 004.021

Ю. М. Монахов

РАСПРЕДЕЛЕННЫЙ МЕХАНИЗМ УПРАВЛЕНИЯ ПЕРЕГРУЗКАМИ В СЕТИ ПЕРЕДАЧИ ДАННЫХ

Проанализированы равновесные состояния системы управления трафиком протокола TCP. Предложен новый способ управления перегрузками TCP/IP-сети, отличительной особенностью которого является медленная адаптация и возможность выборочного изъятия пакетов из очереди.

Ключевые слова: *TCP/IP, вычислительная сеть, перегрузки, AQM, управление.*

Передача данных между конечными системами в пакетно-ориентированной сети, основанной на стеке TCP/IP, происходит за счет использования фиксированных и переменных сегментов ограниченного размера. Обычно перегрузки в пакетно-ориентированных сетях носят локальный характер, и механизм управления перегрузками используется, чтобы улучшить общую сетевую производительность сети, регулируя локальные ситуации на маршрутизаторах. Контроль перегрузки осуществляется через управление скоростью передачи потоков данных каждого источника исходя из текущего уровня загрузки сети [1]. Применение таких механизмов контроля не только позволяет справиться с перегрузками, но также приводит к более эффективному использованию доступной полосы пропускания. Этот подход ограничен, в силу того что информация о текущем состоянии сети должна доставляться по той же (перегруженной) сети передачи данных (СПД). В момент перегрузки доставка такой информации затруднена и замедлена, и поэтому узлы не получают данных об актуальном состоянии сетевой инфраструктуры [2, 3]. Это несколько ограничивает сетевую производительность всех схем управления перегрузками, основанных на таком подходе.

Для того чтобы формально описать процесс управления перегрузкой, необходимо сначала установить основные зависимости между параметрами внутри самого протокола TCP, а именно размером окна фрагментации и очередью.

Динамику этих параметров можно с необходимой точностью описать системой дифференциальных уравнений:

$$\begin{cases} \dfrac{dw}{dt} = \dfrac{a - \left(a + \dfrac{2b}{2-b} w\right) wp}{t_{RTT}}, \\ \dfrac{dq}{dt} = \dfrac{Nw}{t_{RTT}}, \\ t_{RTT} = \dfrac{q}{C} + T_p, \end{cases} \tag{1}$$

где w — размер окна фрагментации, q — длина очереди, p — вероятность ECN-маркинга (или удаления) пакетов, a — параметр протокола *TCP Increase*, b — параметр протокола *TCP Decrease*, N — число источников пакетов, C — пропускная способность канала, t_{RTT} — время между отправкой запроса и получением ответа, T_p — средняя задержка.

Так как AQM-схемы управления перегрузками работают преимущественно с очередью EWMA-усредненной длины [4], то необходимо проследить и ее динамику:

$$\frac{d\overline{q}}{dt} = \omega_q \left(q - \overline{q}\right); \;\; p = p_{\max} \frac{q - th_{\min}}{\Delta th}; \;\; \Delta th = th_{\max} - th_{\min}, \tag{2}$$

где ω_q — частота низкочастотного фильтра, $\overline{q}$ — средняя длина очереди, $p_{\max}$ — максимальная вероятность ECN-маркинга (или удаления) пакетов, $th_{\min}$ и $th_{\max}$ — минимально и максимально допустимая длина очереди соответственно.

EWMA (Exponential Weighted Moving Average) — метод усреднения, использующий следующее рекуррентное соотношение:

$$\overline{q}_n = \left(\overline{q}_{n-1}\left(1 - 2^{-\gamma}\right)\right) + \left(2^{-\gamma} q\right), \tag{3}$$

где γ — весовой коэффициент.

В AQM-схемах управляемым параметром является максимальная вероятность удаления (маркинга) пакетов.

Проанализировав систему (1) и управляющее воздействие (2), найдем ее равновесное состояние, т.е. вектор параметров ($\mathbf{w}$, $\mathbf{q}$, $\overline{\mathbf{q}}$, $\mathbf{p}$, $\mathbf{p}_{\max}$), оптимальных для функционирования СПД. При этом значение оптимальной средней длины очереди $\overline{\mathbf{q}}$ выступает в качестве начального условия, т.е. задается в процессе администрирования или внедрения системы контроля перегрузок:

$$\mathbf{w} = \frac{\overline{\mathbf{q}} + T_p C}{N}, \tag{4}$$

$$\mathbf{q} = \overline{\mathbf{q}}\,(н.у.), \tag{5}$$

$$\mathbf{p} = \frac{(2-b)aN^2}{\left(\overline{\mathbf{q}} + T_p C\right)\left(2b\left(\overline{\mathbf{q}} + T_p C\right) + (2-b)aN\right)}, \tag{6}$$

$$\mathbf{p}_{\max} = \frac{\Delta th(2-b)aN^2}{\left(\overline{\mathbf{q}} + T_p C\right)\left(\overline{\mathbf{q}} - th_{\min}\right)\left(2b\left(\overline{\mathbf{q}} + T_p C\right) + (2-b)aN\right)}. \tag{7}$$

Характер зависимости между вероятностью ECN-маркинга пакета и средней длиной очереди можно установить, изучив *следствия* из равенств (6) и (7).

Следствие 1. Значение $\mathbf{p}_{\max}$ не определено для $\overline{\mathbf{q}} = th_{\min}$, т.е.

$$\lim_{\overline{\mathbf{q}} \to th_{\min}} \mathbf{p}_{\max} = +\infty. \tag{8}$$

Следствие 2. Если $\overline{\mathbf{q}} > th_{\min}$, то $\mathbf{p}_{\max} \sim \dfrac{1}{\overline{\mathbf{q}}}$ и

$$\lim_{\overline{\mathbf{q}} \to \infty} \mathbf{p}_{\max} = 0. \tag{9}$$

Обратно пропорциональная зависимость указывает на возможность построения простого адаптивного механизма, зависящего только от текущего значения средней длины очереди $\overline{q}$. Например, если текущая средняя длина очереди меньше оптимальной, то $\mathbf{p}_{\max}$ необходимо уменьшить на некоторую величину (или в некоторое число раз); и наоборот, если $\overline{q}$ больше оптимальной, то $\mathbf{p}_{\max}$ необходимо увеличить. Такой базовый алгоритм адаптации показан на рис. 1.

Обозначим величину декремента и инкремента $\mathbf{p}_{\max}$ как α и β соответственно. Допустим, что средняя длина очереди считается оптимальной, пока находится в интервале $\left[th_{\min}, th_{\max}\right]$. Тогда базовый алгоритм адаптивной AQM-схемы будет выглядеть так, как показано на рис. 1, *б*.

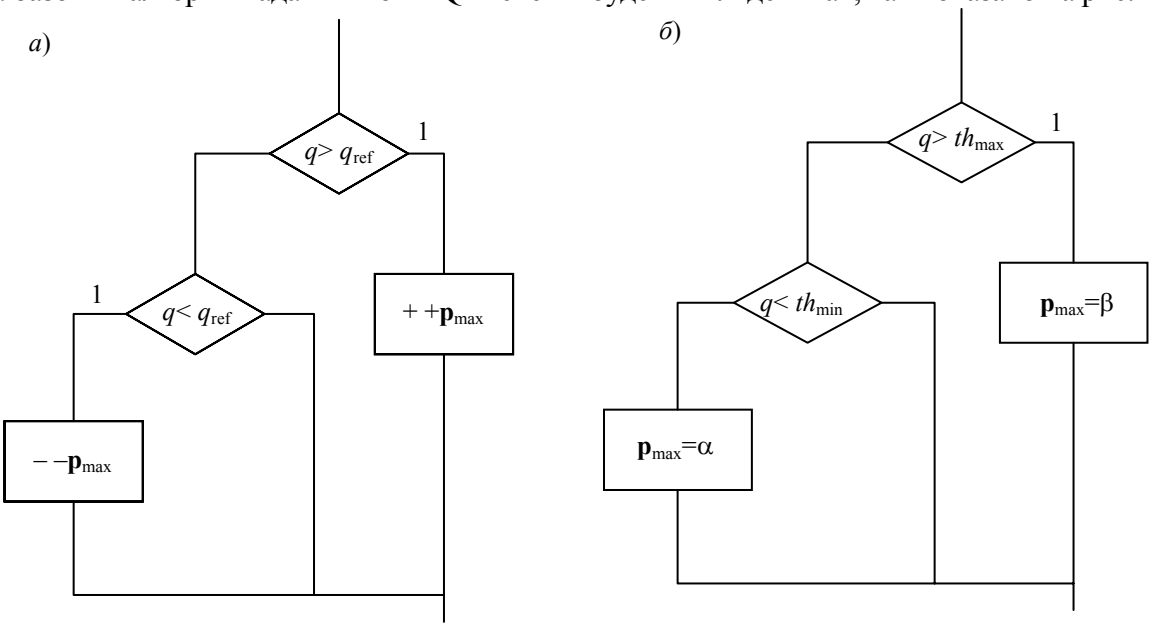


Рис. 1

Отметим, что в разных вариантах подобных адаптивных алгоритмов предельная вероятность $p_{\max}$ может изменяться как линейно, так и полиномиально и экспоненциально [5, 6]. Был выбран линейный характер изменения $p_{\max}$, чтобы протокол TCP мог корректно отработать алгоритм *slow start*.

В настоящей работе предлагается способ управления перегрузками, обладающий следующими отличительными особенностями:

— сигнатурный анализ пакетов для предотвращения информационных атак, т.е. все пакеты, соответствующие сигнатуре, поступившей из центра управления, удаляются из очереди;

— обеспечение ECN-маркинга пакетов как более эффективного способа сигнализирования о перегрузке;

— централизация процедуры выбора управляющих параметров на основе анализа сети отдельным блоком сенсоров трафика;

— медленная адаптация с целью избежания монополизации каналов и глобального увеличения фрагментации ввиду TCP-коллизий.

При таком методе управления перегрузками помимо алгоритма удаления пакетов используется протокол взаимодействия агентов и центра управления, оптимизированный под высокие нагрузки на СПД [7, 8].

Система, позволяющая реализовать способ, состоит из центра контроля перегрузок (ЦКП), агентов контроля перегрузок (АКП) и промежуточного мультиплексора (Mux) — демультиплексора (Demux), снижающего нагрузку на маршрутизаторы подсетей (рис. 2). Каждый компонент обладает ограниченным набором возможных действий, на которых и основывается протокол обмена данными.

ЦКП осуществляет следующие действия:

— пуск АКП;

— останов АКП;

— посылка контролирующего пакета, содержащего параметры алгоритма управления перегрузкой;

— посылка сигнатур вредоносных пакетов.

АКП помимо отработки адаптивного алгоритма осуществляет отправку
— сообщения о статусе (метка Вкл./Ожидание);
— информации об управляемом параметре — максимальной длины очереди;
— информации о числе пакетов, удаленных из очереди.

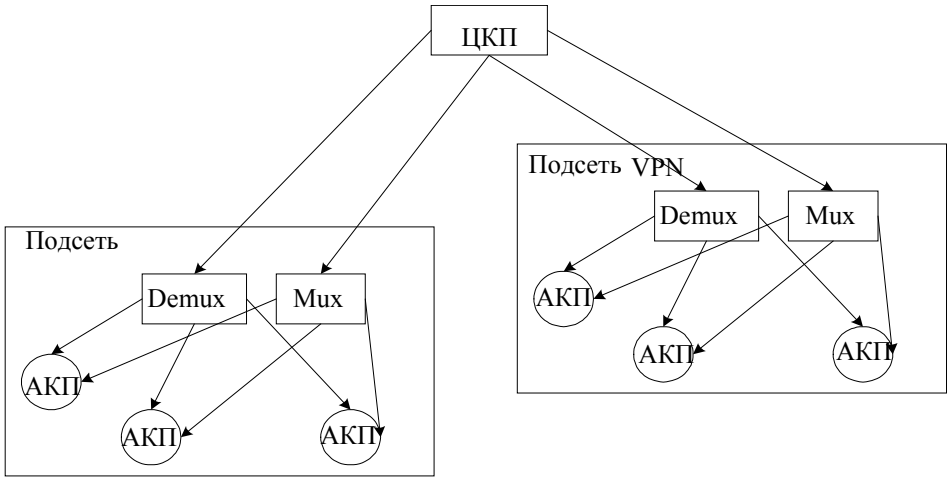


Рис. 2

Указанные действия инициируются ЦКП путем рассылки агентам управляющих пакетов. При этом благодаря мультиплексированию данных через маршрутизатор подсети проходит лишь один управляющий пакет. Рассмотрим этот протокол обмена более подробно.

1. Пуск/останов АКП

На данном шаге участвуют четыре типа пакетов: OS-REQ (On/Standby Request) — запрос пуска-останова всех АКП подсети, OS-ANS (On/Standby Answer) — результат пуска-останова всех АКП подсети, OS-REQD (Demuxed) — запрос пуска-останова одного АКП подсети, OS-ANSD — результат его пуска или останова. Через маршрутизатор проходят только пакеты OS-REQ и OS-ANS. Обмен пакетами OS-REQD и OS-ANSD осуществляется в рамках одной TCP-сессии.

2. Контролирующий запрос/ответ

На данном этапе происходит обмен параметрами алгоритма управления перегрузкой. Для этого вводится структура CTLPACK размером шесть октетов, содержащая пять полей, соответствующих параметрам α, β, $th_{\max}$, $th_{\min}$ и q_{ref}. Для возможности повышения точности в будущем резервируется дополнительный октет. Обмен на данном шаге также использует четыре типа пакетов: CTL-REQ (Control Request) — поставка параметров алгоритма всем АКП подсети, CTL-ANS (Control Answer) — мультиплексированный результат поставки параметров, содержащий максимальные вероятности ECN-маркинга ($p_{\max}$) для всех АКП подсети, CTL-REQD и CTL-ANSD — то же, но для одного АКП. В свою очередь, возможна отправка самопроизвольных CTL-ANSD-пакетов с некой регулируемой частотой (авторами предлагается посылать такие пакеты один раз в секунду) с целью обеспечить оперативное отслеживание состояния сети центром контроля перегрузок.

СПИСОК ЛИТЕРАТУРЫ

1. *Stevens W.* TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Re-overy Algorithms // RFC. 1997. January. 2001 p.

2. *Paxson V., Allman M., Dawson S., Fenner W., Griner J., Heavens I., Lahey K., Semke J., Volz B.* Nown TCP Implementation Problems // RFC. 1999. March. 2525 p.

3. *Paxson V.* End-to-End Internet Packet Dynamics // Proc. SIGCOMM '97. Cannes, France, 1997.

4. *Mathis M., Mahdavi J.* Forward Acknowledgment: Refining TCP Congestion Control // Proc. SIGCOMM'96. Stanford, CA, 1996.

5. *Монахов Ю. М.* Динамика протокола TCP в условиях сетевых атак и перегрузок // Математические методы в технике и технологиях ММТТ-21. Сб. тр. XXI Междунар. науч. конф. Секция 6 / Под общ. ред. *В. С. Балакирева*. Саратов: Сарат. гос. техн. ун-т, 2008. Т. 7. С. 264.

6. *Монахов Ю. М.* Уязвимости протокола транспортного уровня TCP // Алгоритмы, методы и системы обработки данных / Под ред. *С. С. Садыкова, Д. Е. Андрианова*. М.: Горячая линия – Телеком, 2006. С. 203—210.

7. *Монахов Ю. М., Макаров Р. И.* Автоматизированная система обнаружения аномального функционирования распределенной вычислительной среды АСУ // Системный анализ: теория и практика. 2009. № 3. С. 86—89.

8. *Монахов Ю. М.* Использование farima-модели для описания и предсказания поведения сети передачи данных в условиях атак типа „отказ в обслуживании“ // Горный информационно-аналитический бюллетень. 2008. № 10. С.133—137.

Сведения об авторе

Юрий Михайлович Монахов — канд. техн. наук, доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: unclefck@gmail.com

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.

УДК 654.924

А. В. Тельный, О. Р. Никитин, И. В. Храпов

ОБ ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ РАСПРЕДЕЛЕННОЙ СРЕДЫ ИНТЕГРИРОВАННЫХ СИСТЕМ ОХРАНЫ И БЕЗОПАСНОСТИ

Представлены критерии оценки и способы организации информационного обмена в распределенной информационной среде интегрированных систем охраны и безопасности различных производителей.

Ключевые слова: *интегрированные системы безопасности, SCADA-системы.*

Актуальность задачи обеспечения информационного обмена между интегрированными системами безопасности (ИСБ) разных производителей определяется [1, 2]:

— необходимостью оборудования или дооборудования объекта техническими средствами охраны и безопасности в результате строительных перепланировок, ремонтных работ и т.д.;

— развитием телекоммуникационных систем, технически позволяющих объединять в информационную систему безопасности (с созданием единого центра и единого автоматизированного рабочего места (АРМ) ИСБ) пространственно-распределенные объекты, на которых установлены ИСБ различных производителей.

Заметим, что использование одной организацией на распределенных объектах различных АРМ ИСБ, не поддерживающих информационного обмена между собой, экономически нецелесообразно, требует дополнительных затрат на обслуживание и обучение персонала, снижает уровень контроля безопасности объектов в целом.

Для небольших объектов использование нескольких программных комплексов оказывается избыточным, требует дополнительного штата сотрудников. В настоящее время развитие получили концепции „умный дом“, или „интеллектуальное здание“, интегрирующие на одной аппаратно-программной платформе и едином АРМ диспетчеризации объекта подсистемы

управления инженерно-технологическим оборудованием здания, учета потребляемых ресурсов, ИСБ.

Для обеспечения информационного обмена между ИСБ разные производители систем принимают различные технические решения, зависящие от:

— используемых аппаратно-программных средств линейки оборудования ИСБ;

— ранее разработанных АРМ ИСБ и обязательств по их технической поддержке;

— наличия и уровня подготовки специалистов в области информационных технологий;

— проводимой организацией маркетинговой политики.

Анализ технических решений производителей ИСБ показывает, что разработчики оборудования и программного обеспечения (ПО) в основном используют следующие подходы:

1) создают под платформу своего ПО ИСБ программные драйверы для возможности подключения оборудования других производителей (например, ПО „Интеллект“ фирмы ITV, Москва, содержит около 40 драйверов для различных систем). Такой вариант возможен как по соглашению между разработчиками программной платформы и оборудования ИСБ, так и без соглашения (вскрытие протоколов) по инициативе заказчика или монтажной организации при проведении пусконаладочных работ на объекте;

2) используют контроллеры, запрограммированные сторонним производителем по соглашению между разработчиками, например, сервисный модуль Ultima-EXT-i от ООО „Итриум СПб“, Санкт-Петербург, для интеграции с ИСБ „Орион-Про“ и ИСБ „Стрелец“ или модули IntesisBox для протоколов ModBus производства ООО „Солитон“, Киев, Украина;

3) используют программируемые промышленные контроллеры или преобразователи интерфейсов (протоколов) различных производителей, которые программируются заказчиком или монтажной организацией при проведении пусконаладочных работ на объекте;

4) разработчики ПО ИСБ выпускают платформы с открытой архитектурой для того, чтобы пользователи могли самостоятельно в АРМ ИСБ обмениваться с ИСБ других производителей (например, на основе протокола ModBus);

5) разработчики линейки ИСБ создают для своего оборудования программируемые модули и OPC-серверы, предоставляют протоколы ModBus или используют протоколы стандарта LONWORKS с промышленно выпускаемыми контроллерами (например, фирмы Echelon). Такой подход позволяет полнофункционально интегрировать различные ИСБ на основе SCADA-платформ;

6) разработчики ИСБ интегрируют свои продукты на основе менее распространенных и более закрытых информационных технологий с использованием SCADA-платформ (пример — технология COBRA).

Оценив достоинства и недостатки каждого из технических подходов к интеграции информационного обмена между ИСБ, можно сказать, что наиболее перспективным представляется их интеграция на основе SCADA-платформ с использованием контроллеров и серверов, выпускаемых производителем оборудования по следующим причинам:

1) при программировании контроллеров заказчиком или монтажной организацией, создании драйверов оборудования ИСБ необходим высокий уровень подготовки специалистов во избежание возможных ошибок. Программисты, как правило, не являются специалистами в области эксплуатации ИСБ;

2) созданные программные продукты должным образом и в необходимом объеме не тестируются, у заказчика может не быть таких возможностей;

3) при самостоятельном создании драйверов (программировании контроллеров) без соглашения с производителем и получения от разработчиков полной информации о протоколах обмена (вскрытии протоколов) возможны критические ошибки и возникновение уязвимостей в функционировании ИСБ, о которых заказчик может не знать;

4) при обновлении линейки оборудования разработчику ИСБ, возможно, придется заново программировать контроллеры, что для заказчика экономически невыгодно. В то же время обновление драйверов от разработчика осуществляется, как правило, в порядке технической поддержки;

5) при самостоятельной разработке драйверов (программировании контроллеров) возможно неумышленное создание опасности проникновения злоумышленников в распределенную информационную систему;

6) при использовании универсального ПО ИСБ с внедренными драйверами для подключения оборудования различных производителей заказчик оказывается „привязанным“ к выбранной платформе ПО, интерфейсу пользователя, сервису ПО и т.д. Техническая поддержка драйверов (обновления) сторонним производителем ПО ИСБ, как правило, не осуществляется.

SCADA-системы поддерживают разные типы контроллеров автоматики зданий, но не поддерживают контроллеры, применяемые для систем безопасности. Для подключения контроллера к SCADA-системе требуется разработка OPC-сервера. На данный момент наиболее распространен стандарт OPC DA Version 2.05a.

OPC-набор спецификаций стандартов. Каждый стандарт описывает набор функций определенного назначения. Текущие стандарты:

— OPC DA (Data Access) — основной и наиболее востребованный стандарт. Описывает набор функций обмена данными в реальном времени с ПЛК, РСУ, ЧМИ, ЧПУ и другими устройствами;

— OPC AE (Alarms & Events) — предоставляет функции уведомления о различных событиях (аварийных ситуациях, действиях оператора, информационных сообщениях и др.) по требованию;

— OPC Batch — предоставляет функции шагового и рецептурного управления технологическим процессом (в соответствии со стандартом S88.01);

— OPC DX (Data eXchange) — предоставляет функции организации обмена данными между OPC-серверами через сеть Ethernet. Основное назначение — создание шлюзов для обмена данными между устройствами и программами разных производителей;

— OPC HDA (Historical Data Access) — предоставляет доступ к сохраненным данным;

— OPC Security — определяет функции организации прав доступа клиентов к данным системы управления через OPC-сервер;

— OPC XML-DA (XML-Data Access) — предоставляет гибкий, управляемый правилами формат обмена данными через SOAP и HTTP;

— OPC UA (Unified Architecture) — последняя по времени выпуска спецификация, которая основана не на технологии Microsoft COM, что предоставляет кроссплатформенную совместимость. Еще одна разновидность OPC-сервера — шлюз к сети полевой шины, такой как Profibus или LonWorks (обычно на компьютере с ОС Windows устанавливается адаптер fieldbus-сети, а OPC-сервер взаимодействует с этой сетью через драйвер адаптера).

Наиболее востребована программа высокого уровня OPC DA. Почти все известные SCADA-продукты являются OPC-клиентами, например, SCADA АЛГОРИТМ (БОЛИД), ЭНТЕК (ЭНТЕЛС), MasterSCADA (ИнСАТ), InTouch (Wonderware), TRACE MODE (AdAstra), Vijeo Citect (Schneider Electric), КРУГ-2000 (КРУГ), CitectSCADA (Schneider Electric), Genesis32 (ICONICS), а большинство из них и OPC-серверами (в частности, CiTect, MasterSCADA, КРУГ-2000 и TRACE MODE). Поддержка OPC HDA из российских полнофункциональных SCADA-систем реализована только в SCADA TRACE MODE, MasterSCADA и КРУГ-2000.

На отечественном рынке производителей оборудования и АРМ ИСБ в настоящее время складывается следующая ситуация по использованию интеграции систем в SCADA:

1) НВП „Болид“, Королев, ИСБ „Орион-Про“. Аппаратные средства: преобразователь протокола С2000-ПП для интеграции линейки оборудования системы „Орион“ по интерфейсу Modbus RTU. Шлюз Modbus, тип интерфейса RS-485, тип протокола Modbus-RTU. Программные средства: OPC-сервер для АРМ „Орион-Про“ (Сервер состояний: позволяет получать информацию о состоянии групп разделов, разделов, приборов, шлейфов, реле, считывателей, дверей, получать значения АЦП шлейфов, ставить и снимать с охраны разделы и шлейфы, управлять реле. Соединяется с ядром АРМ „Орион-Про“ через интерфейс XML-Rpc). OPC-сервер Orion-ModBus поддерживает интерфейс OPC DA2.0 и работает с прибором „С2000-ПП“, опрашивая его по протоколу ModBus-RTU;

2) ЗАО „Аргус-Спектр“, Санкт-Петербург: ВОРС „Стрелец“ и „Стрелец-Интеграл“. Аппаратные средства: блок преобразования интерфейсов БПИ RS-И (USB; RS232); блоки сетевых интерфейсов U.10, i.LON-10, i.LON-100, i.LON-600, PCL-TA-21, PCC-10 (Ethernet; GSM/GPRS;PCI; PCMCIA) и др. являются стандартными сетевыми интерфейсами платформы LONWORKS и производятся фирмой Echelon. Информационная среда ИСБ строится на основе стека протоколов стандарта LONWORKS LON ANSI/EIA 709.1 (EN 14908, ISO/IEC 14908). В качестве основного физического интерфейса в ИСБ используется интерфейс TP/FT-10;

3) ЗАО „Риэлта“, Санкт-Петербург, ИСБ „Ладога-А“ с использованием ПО фирмы „Eselta“. В ПО ИСБ добавлен OPC-сервер, реализующий доступ к данным и событиям Eselta благодаря технологиям OPC Data access и OPC Alarm events;

4) фирма „Сигма-ИС“, Москва, ИСБ „Рубеж-08; Р-09“. Имеется OPC-сервер к оборудованию „Рубеж“ для представления объектов технических средств (ТС) БЦП в виде тегов. Сервер разработан на основе универсального OPC-сервера фирмы FastWell (UniOPC Server);

5) фирма Honeywell (ранее Ademco) ИСБ серии VISTA и Galaxy — ПО „Compass“ (много других ПО, поддерживающих данные панели). На рынке представлено много стандартных OPC-серверов для работы с контроллерами Honeywell, например, разработанные фирмой Intesis. Intesis OPC-сервер для систем противопожарной сигнализации Notifier ID3000 series (Honeywell)-ID3000;

6) ООО „Плазма-Т“, Москва, ПО „Спрут-2“ для автоматизации пожарной сигнализации и оборудования управления противопожарной автоматикой. Имеется OPC-сервер для интегрирования комплекта „Спрут-2“ в системы диспетчерского управления и сбора данных SCADA/HMI. На сайте разработчика представлена таблица ModBus для наладки программ, поддерживающих ModBus RTU;

7) группа компаний „АСБ“, Москва, ИСБ „Пахра“, „Антел“. В ПО ИСБ „Радиосеть“ и ПО „Пахра“ использована архитектура распределенной самосинхронизирующийся среды функционирования, конфигурируемой при помощи XML. Интеграции в SCADA от производителя нет;

8) ЗАО „Теко“, Казань, ИСБ „Астра-РИМ“, „Астра-812“. Интеграции в SCADA от производителя нет;

9) фирма „Кодос“, Москва, ИСБ на основе ППКОП „Кодос А-20“. Интеграции в SCADA от производителя нет;

10) НПО „Сибирский арсенал“, Новосибирск, оборудование „Гранит“, „Карат“, ИСБ „Лавина“. Интеграции в SCADA от производителя нет;

11) ООО „Альтоника“, Москва, радиоканальные системы „Риф Стринг“ ПО „Риф Страж“. Интеграции в SCADA от производителя нет;

12) группа предприятий „Ровалент“, Минск, Беларусь, ИСБ „777“ и АРМ ИСБ „777“. Интеграции в SCADA от производителя нет.

Таким образом, выбор ИСБ при оборудовании объектов системами охраны и безопасности или выбор способа организации информационного взаимодействия между системами различных производителей необходимо осуществлять с учетом возможности объединения ИСБ

на основе SCADA-технологий. Предложенные в статье критерии оценки и способы интеграции ИСБ позволяют избежать непроизводительных финансовых затрат, повысить эффективность эксплуатации ИСБ в целом и уровень контроля функционирования ИСБ.

СПИСОК ЛИТЕРАТУРЫ

1. Системы безопасности и мониторинга — Интегрированные системы безопасности [Электронный ресурс]: <http: // rovalant.com/systems/integrated-systems.html>.

2. *Тельный А. В.* Организация взаимодействия между подсистемами интегрированной системы безопасности // Тр. X Росс. Науч.-техн. конф. „Новые информационные технологии в системах связи и управления“. Калуга: Изд-во ООО „Ноосфера“, 2011. 610 с.

Сведения об авторах

Андрей Викторович Тельный — канд. техн. наук, доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: andre.izi@mail.ru

Олег Рафаилович Никитин — д-р техн. наук, профессор; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: olnikitin@mail.ru

Игорь Викторович Храпов — канд. техн. наук; Тамбовский государственный технический университет; аналитический центр экономического развития; директор; E-mail: igor@tambov.ru

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.

ЭКСПЛУАТАЦИЯ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

УДК 621.376.9

А. В. Горячев, М. Ю. Монахов

ИССЛЕДОВАНИЕ КАЧЕСТВА БЕСПРОВОДНЫХ КАНАЛОВ СВЯЗИ РАСПРЕДЕЛЕННОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СРЕДЫ ПЕРЕДАЧИ ДАННЫХ В ПЛОТНОЙ ГОРОДСКОЙ ЗАСТРОЙКЕ

Проанализированы результаты экспериментального исследования качества канала передачи данных, организованного с использованием технологий беспроводной связи, между мобильным транспортным средством, перемещающимся по городу, и центральной станцией.

Ключевые слова: *беспроводной канал связи, мобильное транспортное средство, UMTS/HSDPA, GSM/GPRS/EDGE.*

Введение. Организация надежного и безопасного канала передачи данных между мобильным транспортным средством (МбТС), перемещающимся по городу в условиях плотной застройки, и центральной, стационарной или мобильной станцией является актуальной задачей. МбТС предназначено для „съема“ информации о функционирующих радиостанциях, попадающих в поле его видимости, и передачи предварительно обработанной информации к центральной станции. В настоящей статье анализируется возможность совместной работы станций в режиме реального времени путем организации канала передачи данных с использованием технологий беспроводной связи.

Особенности технологий беспроводной передачи данных. Существующие технологии, например, GSM/GPRS/EDGE и UMTS/HSDPA [1], позволяют решить поставленную задачу, используя все преимущества телекоммуникационной сети передачи данных городского уровня. При этом возникают проблемы обеспечения качества, надежности и защищенности такой сети. Отметим, что на работу базовых станций операторов связи влияет ряд факторов, не связанных напрямую с технологией передачи данных: район города, климатические условия, время суток, передаваемый объем информационных сообщений, факт движения устройства, зарегистрированного в сети. В рассматриваемой ситуации необходимо свести к минимуму риски обрыва соединения и нарушения целостности при передаче информации. Частично задача решается введением в стандарты сетей второго и третьего поколения сервиса обеспечения качества обслуживания — Quality of Service (QoS), непосредственно управляющего каналом связи [1]. Заметим, что качество канала связи характеризуется минимальным временем задержки передачи пакета, неразрывностью устанавливаемого соединения, целостностью передаваемых данных (минимальное число потерянных пакетов) и устойчивостью к помеховым и шумовым воздействиям.

В стандарте QoS выделяется четыре класса трафика взаимодействия: диалоговый, потоковый, интерактивный и вспомогательный с отложенной передачей данных [2]. Классы QoS пакетного трафика, организованного беспроводной средой передачи данных, ограничиваются интерактивным и вспомогательным [2]. На уровне системы управления сети оператора связи

реализован ряд функций обеспечения требуемого качества обслуживания: функция эстафетной передачи управления — хэндовер, управление мощностью, нагрузкой базовой станции и планирование распределения пакетов, поддерживающее запланированную зону охвата и высокой пропускной способности.

Экспериментальные исследования. Авторами экспериментально исследована распределенная телекоммуникационная среда передачи данных стандартов UMTS/HSDPA и GSM/GPRS/EDGE сетей операторов связи „большой тройки“.

Первая часть исследования заключалась в сборе статистической информации о передаче данных в условиях передвижения МбТС по городу. Модемное соединение обеспечивала специально разработанная программа, фиксировавшая уровень сигнала от базовой станции, количество отправленных и принятых пакетов информации, максимальное и минимальное время задержки ответа интернет-ресурса на запрос проверки соединения.

Вторая часть исследования состояла в постоянном мониторинге МбТС определенных маршрутов движения с фиксацией проблемных зон различных операторов связи. Мониторинг проводился ежедневно в течение четырех часов на протяжении одного месяца. Период опроса и передачи данных системы мониторинга МбТС составлял 20 с во время движения и 2 мин — при стоянке. При перерыве в поступлении пакетов более четырех минут на сервере мониторинга фиксировалось событие потери связи с объектом.

Результаты. За четыре часа были организованы 3 сессии передачи данных в сетях операторов связи. Передано в общей сумме 11 224 пакетов, из них потеряно 213, что составляет 1,89 % от общего количества. Зафиксирован один разрыв соединения. Минимальное время задержки ответа информационного ресурса составило 93 мс, максимальное — 2448 мс. Уровень сигнала базовой станции варьировался от –51 до –113 дБ. За месяц мониторинга было выделено 27 проблемных зон операторов связи, в которых связь с МбТС периодически пропадала на неизменном маршруте движения, из них 14, где зафиксировано пять и более случаев потери связи. Максимальное количество зафиксированных событий потери связи в одной зоне составило 46 за все время исследования.

На рисунке представлен фрагмент карты центральной части г. Владимира с выделенным жирной линией маршрутом МбТС. Кружками и эллипсами обозначены „проблемные“ зоны.

Выводы. Исследование телекоммуникационной среды передачи данных по технологиям UMTS/HSDPA и GSM/GPRS/EDGE показало, что сети операторов связи „большой трой-

ки“ в городской инфраструктуре, характеризующейся плотной застройкой, не обеспечивают равномерного покрытия городской черты и поддержки требуемого уровня QoS передачи данных в условиях движения объекта исследования. Плавный переход обслуживания объекта между базовыми станциями организован, но имеет место достаточно высокая вероятность разрыва соединения с сетью оператора. В утренние и вечерние часы вероятность потери связи с МбТС выше, чем в дневное время. Существуют „проблемные“ географические зоны, в которых зафиксированы случаи потери связи, не перекрываемые сетями операторов связи.

Имея карту „проблемных“ зон города, в целом можно организовать переключение потока данных между сетями операторов связи, основываясь на уровне сигнала от базовой станции и времени суток, увеличив тем самым надежность канала связи и целостность информации, передаваемой в распределенной телекоммуникационной среде.

СПИСОК ЛИТЕРАТУРЫ

1. *Волков А. Н., Рыжков А. Е., Сиверс М. А.* UMTS. Стандарт сотовой связи третьего поколения. СПб: Изд-во „Линк“, 2008.

2. *Holma H., Toskala A.* WCDMA FOR UMTS: Radio Access for Third Generation Mobile Communication. London: John Wiley & Sons Ltd, 2004.

Сведения об авторах

Алексей Владимирович Горячев — аспирант; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: a.goryachev@rfc-cfa.ru

Михаил Юрьевич Монахов — д-р техн. наук, профессор; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; заведующий кафедрой; E-mail: mmonakhov@vlsu.ru

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.

УКД 004.043

М. Ю. Монахов, О. И. Файман

ИНВЕНТАРИЗАЦИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ КАК ОСНОВА БЕЗОПАСНОГО ФУНКЦИОНИРОВАНИЯ АСУ

Приведен перечень информационных ресурсов автоматизированных систем управления (АСУ) на основе степени их вовлеченности в протекающие на предприятии бизнес-процессы. Определены критичные для безопасного функционирования АСУ характеристики информационных ресурсов. Предложена методика инвентаризации информационных ресурсов, проанализированы особенности ее применения.

Ключевые слова: *инвентаризация, информационные ресурсы, бизнес-процессы, информационная безопасность.*

Введение. Информационные ресурсы (ИР) являются принципиальной составляющей управления предприятием. Недостаточная систематизация и несовершенная структурная организация ИР и как следствие — неэффективность информационного обеспечения бизнес-процессов приводят к деструктивным, а порою и катастрофическим последствиям для производственной деятельности предприятия. Чаще всего подобные ситуации складываются при интеграции различных автоматизированных систем управления предприятием (АСУП), когда

достаточно убедительно продумываются интеграционные вопросы производственной деятельности, а новая информационная инфраструктура формируется путем простого объединения имеющихся ИР и средств их обработки.

Системным решением, позволяющим преодолеть подобные проблемы, является инвентаризация и структуризация имеющихся ИР с целью выявления степени их критичности для функционирования предприятия [1, 2], что потребует обеспечения их надежного хранения, поддержания целостности и достоверности содержащейся в них информации. Кроме того, часть ИР представляет собой производственную тайну, следовательно, необходимо обеспечение конфиденциальности. Насколько точно и всесторонне представлены сведения об ИР, настолько более адекватно будет система защиты информации (СЗИ) обеспечивать конфиденциальность, целостность и доступность циркулирующей на предприятии информации [3].

Классы информационных ресурсов. Для интегрированной АСУ современного предприятия характерен типовой набор ИР, который предлагается разделить на 13 классов. Внутри класса информация каждого ИР может обладать своей степенью конфиденциальности, целостности, доступности. Степень таких категорий безопасности, как правило, устанавливается собственником предприятия.

1. *Класс ИР „Производство“* содержит информацию о кадрах и структуре производства; об организации труда, о наличии оборудования и его характеристиках, уровне запасов материалов, комплектующих, готовой продукции; о резервах сырья; о применяемых материалах; о комплектующих изделиях, придающих продукции новые потребительские качества.

2. *Класс ИР „Управление“* содержит информацию о подготовке решений руководства и их исполнении; о планах по расширению производства, закупкам и продажам; о проектах экспортно-импортных планов, инвестиционных программ; об объемах капитальных вложений и строительно-монтажных работ; об эффективности экспорта и импорта товаров; о свертывании и расширении производства.

3. *Класс ИР „Финансы“* содержит информацию о плановых и фактических показателях финансового плана; о стоимости товарных запасов и оборотных средств; о показателях рентабельности производства, прибыли; об объемах финансирования капитальных вложений и затрат на внедрение новой техники; о состоянии кредита; о проведении переговоров, в том числе о границах полномочий должностных лиц по ценам, скидкам и другим условиям; о генеральной линии и тактике в валютных и кредитных вопросах.

4. *Класс ИР „Рынок сбыта“* содержит информацию об оригинальных методах изучения рынка сбыта; о состоянии рынка и перспективах рыночной конъюнктуры; о маркетинговых исследованиях; об эффективности коммерческой деятельности; о внешнеэкономической деятельности; о конкретных направлениях в торговой политике.

5. *Класс ИР „Деловое партнерство“* содержит информацию о клиентуре, компаньонах, посредниках, поставщиках, подрядчиках и спонсорах; о коммерческих связях; о местах закупки товаров; о предприятии как торговом партнере.

6. *Класс ИР „Переговоры“* содержит информацию о подготовке и результатах переговоров; о заказах и предложениях; о лицах, ведущих переговоры; о деловой политике предприятия по сделкам; о содержании переговоров с представителями иностранных фирм.

7. *Класс ИР „Контракты“* содержит информацию об условиях контрактов, сделок и соглашений; об исполнении контрактов; о номенклатуре товаров по взаимным обязательствам, предусмотренным соглашениями и протоколами о товарообороте.

8. *Класс ИР „Цены“* содержит информацию о механизмах образования цены на продукцию; о калькуляции издержек производства; о внутренних прейскурантах и тарифах скидок; о методике расчетов цен по экспорту и импорту; о себестоимости и контрактных ценах товаров и услуг.

9. *Класс ИР „Торги“* содержит информацию о подготовке к торгам или аукционам; о предполагаемом конкурсе или торгах; о приложениях к предложениям на публичных торгах.

10. *Класс ИР „Наука и техника“* содержит информацию о программах перспективных научных исследований; о конструктивных решениях разрабатываемого изделия, придающих ему новые потребительские свойства; о методах защиты от подделки товарных знаков; об исполнителях и потенциальных заказчиках НИР и ОКР; об изобретениях, научных, технических, конструкторских и технологических решениях.

11. *Класс ИР „Технология“* содержит информацию об особенностях используемых и разрабатываемых технологий; о технологических достижениях, обеспечивающих преимущества в конкурентной борьбе; о модификации и модернизации технологий, процессов и оборудования; об организации работ по качеству; о программном обеспечении АСУ.

12. *Класс ИР „Безопасность“* содержит информацию о структуре, составе, оснащении службы безопасности; об организации СЗИ; об организации и технических средствах охраны, пропускном режиме, системе сигнализации; о коммерческой тайне предприятий-партнеров.

13. *Класс ИР „Конкуренты“* содержит информацию об отечественных и зарубежных предприятиях как потенциальных конкурентах; о деловых отношениях с конкурирующими предприятиями.

Представление результатов инвентаризации. Результатом инвентаризации является формирование „Перечня информационных ресурсов“ предприятия, который постоянно поддерживается в актуальном состоянии и позволяет обеспечить документированное отображение состава и структуры ИР. Инвентаризация ИР кроме наведения „порядка“ в информационной инфраструктуре АСУ должна обеспечивать решение ряда стратегических задач построения многоуровневой СЗИ на предприятии:

— разграничение ИР по уровню конфиденциальности, целостности и доступности. Это необходимо, чтобы выделить ИР, которые нуждаются в организации специальных механизмов защиты;

— разграничение ИР по принадлежности к подразделениям, пользователям, конкретным бизнес-процессам и поддерживающим их программным приложениям (информационным процессам, ИП), что позволит упорядочить информационный обмен предприятия, построить эффективную политику разграничения доступа;

— разграничение ИР по степени „ценности“ как меры значимости (критичности) для реализации ИП, что позволит выявить дополнительные точки воздействия угроз информационной безопасности, а значит, более точно оценить уровень защищенности ИР (уровень риска) и предложить адекватные механизмы защиты.

„Перечень информационных ресурсов“ предлагается формировать в форме таблицы со следующими полями:

1) „Наименование ИР“. Вносится конкретное наименование документа, например, в классе „Производство“ — документ „Организационная структура предприятия“;

2) „Обозначение ИР“. В данное поле вносится принятое (закодированное) имя данного документа в СЗИ, включая номер класса ИР и имя ИР внутри класса, например, 3ИР1;

3) „Краткое содержание ИР“. В данное поле заносится наиболее существенная информация о документе — краткая аннотация;

4) „Уровень безопасности“. В первый столбец данного поля вносятся сведения об уровне конфиденциальности информации, содержащейся в данном ИР („строго конфиденциальная“ (СК), „конфиденциальная“ (К), „открытая“ (О)), во втором — об уровне целостности („высокая“ (ВЦ), „средняя“ (СЦ), „низкая“ (НЦ — нет требований)), в третьем — доступности („высокая доступность“ (ВД), „средняя доступность“ (СД), „низкая доступность“ (НД — нет требований));

5) „Место хранения“. В данное поле вносится информация о конкретном местонахождении данного ИР. Принят следующий формат: „Номер_подразделения“, „Номер_помещения“, „Номер_шкафа / Сейфа / Стола“, „Номер_оборудования (компьютера)“. Если ИР электронный, то добавляется имя файла и путь к нему внутри компьютера;

6) „Приложения, использующие ИР“. В данное поле вносится информация о функциональных подсистемах и прикладных сервисах, которым „принадлежит“ ИР. Заметим, что каждый конкретный ИР на предприятии используется как в задачах организационного управления („бумажный“ документ), так и в электронном документообороте (компьютерный файл или база данных). Здесь перечисляются номера ИП из „Перечня информационных процессов (функциональных подсистем и приложений)“, реализующих принятые на предприятии бизнес-процессы. Данный перечень ИП включает „закрепленных“ за каждым ИП пользователей, т.е. пользователи автоматически „прикреплены“ к ресурсам;

7) „Уровень ценности“. Для отдельных ИР владелец может задать стоимость, рассчитываемую по методике, предложенной в статье [4]. Стоимость может быть выражена в денежных или относительных единицах, или в качественных шкалах, например: „незначительный ущерб“, „существенный ущерб“ и т.д. В данной методике предлагается включить для каждого ИР показатель ценности как меры важности (полезности) ИР для реализации бизнес-процессов. За данную величину авторы принимали относительную частоту использования ИР в бизнес-процессах, приносящих наибольшую прибыль;

8) „Ответственное лицо“. Как правило, это руководитель структурного подразделения, где хранится ИР. Заметим, что ответственное лицо может не являться пользователем данного ИР. Основная функция ответственного — обеспечить безопасность ИР.

Особенности инвентаризации ИР на промышленном предприятии. В таблице представлен фрагмент Перечня ИР ОАО „Промышленное предприятие Владимирской области“.

Наименование ИР	Обозначение	Краткое содержание ИР	Уровень безопасности			Место хранения	Приложения, использующие ИР	Уровень ценности	Ответственное лицо
			К	Ц	Д				
Заказы клиентов	ЗК-2	На основе данной информации ежедневно формируются планы производства	К	СЦ	СД	4, 1, 100001 C://program files/axap.exe	Microsoft Dynamics AX, Новиков Н.Д., главный инженер	31695,15 (руб.) 0,15	Новиков Н.Д., главный инженер
Уровень запасов сырья	УЗС-1	Недопустимость этих данных делает невозможной отгрузку со складов на производство	К	ВЦ	СД	4, 1, 100001 C://program files/axap.exe	Microsoft Dynamics AX , Новиков Н.Д., главный инженер	68958 (руб.) 0,23	Новиков Н.Д., главный инженер

В результате анализа перечня были выработаны замечания и рекомендации:

1) основными сложностями при проведении работ являются организационно-технические мероприятия по сбору информации об ИР от подразделений, непонимание руководителями значимости и специфики проведения работы. Кроме того, они с трудом классифицируют ИР по уровню конфиденциальности, целостности и доступности;

2) группе, проводящей инвентаризацию ИР, необходимо тщательно подготовиться к данному процессу: внести четкость и однозначность в используемые понятия, касающиеся назначения, содержания, состава и структуры ИР; составить предварительный список

возможных ИР, специфичных для подразделения, понятный руководству; предусмотреть автоматизированные средства обработки больших объемов полученной информации.

СПИСОК ЛИТЕРАТУРЫ

1. *Королев А. В., Королев В. И.* Методика проведения инвентаризации и структуризации информационных ресурсов на объекте информатизации // Безопасность информационных технологий. 2009. № 4 [Электронный ресурс]: <http://www.pvti.ru/articles_16.htm>.

2. *Симонов С. В.* Технологии и методики классификации информационных ресурсов // Тр. ИСА РАН. 2006. Т. 27. С. 58—73.

3. Федеральный закон РФ № 149 „Об информации, информационных технологиях и о защите информации“. 2006.

4. *Файман О. И.* Математическая модель оценки информационных ресурсов в рамках управления информационными ресурсами // „Математические методы в технике и технологиях – ММТТ-22“. Сб. тр. XXII Междунар. науч. конф. 2010. Т. 11. С. 55—58.

Сведения об авторах

Михаил Юрьевич Монахов — д-р техн. наук, профессор; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; заведующий кафедрой; E-mail: mmonakhov@vlsu.ru

Ольга Игоревна Файман — Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; ассистент; E-mail: Olich06@inbox.ru

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.

УДК 004.891.3

Д. А. Полянский, М. Ю. Монахов

МОДЕЛЬ ОЦЕНКИ ФАКТОРОВ ИЗМЕНЕНИЯ ДОСТОВЕРНОСТИ ИНФОРМАЦИИ В КОРПОРАТИВНОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ

Проанализированы особенности обеспечения достоверности информации в корпоративной сети передачи данных. Определена зависимость достоверности от ряда трудноформализуемых характеристик и факторов. Предложена модель оценки достоверности информации и прогнозирования ее изменения.

Ключевые слова: *достоверность данных, информационный ресурс, корпоративная сеть передачи данных, дестабилизирующий фактор, экспертная оценка.*

Достоверность информации, циркулирующей в корпоративной сети передачи данных (КСПД), означает тождество содержания источника, носителя и приемника информации [1]. Дестабилизирующие факторы (ДФ), т.е. внутренние или внешние по отношению к КСПД события, которые приводят к изменению либо уничтожению информационных ресурсов (ИР), снижают уровень достоверности. Примерами ДФ можно назвать неправильную интерпретацию данных, неудачную установку и конфигурирование технических средств обработки данных, неверное считывание данных в процессе ввода и формирования сообщений, искажения в канале передачи, сбои в работе оборудования, ошибочные или злонамеренные действия оператора.

При высокой надежности технических средств хранения, обработки и передачи данных ДФ связаны в основном с деструктивными действиями персонала организации и внешних злоумышленников.

Возможность возникновения ДФ определяют внутренние свойства КСПД, которые будем называть структурно-функциональными недостатками (СФН). Любая КСПД имеет множество СФН, которые можно разделить на организационные, технические и программно-аппаратные.

Организационные СФН: неудачное распределение ИР, неправильная организация информационного обмена на различных уровнях информационного взаимодействия в корпоративной телекоммуникационной сети (КТКС), неправильный выбор модели разграничения доступа к ИР, неправильная организация системы резервирования данных, а также учета съемных носителей информации, недостатки контроля целостности ИР, нарушение правил эксплуатации средств обработки ИР.

Технические СФН: использование для информационного обмена технических средств, не соответствующих требованиям обеспечения достоверности данных, неправильное конфигурирование средств обработки, преобразования и представления данных, отсутствие или недостаточное количество источников бесперебойного питания.

Программно-аппаратные СФН: нелицензионное программное обеспечение (ПО), его неправильная настройка, ограниченность аудита событий, недостатки контроля доступа к ПО, повышенная нагрузка на используемые аппаратные средства.

Предлагаемая модель оценки текущего уровня достоверности данных и прогнозирования его изменения включает следующие показатели. ДФ l характеризуется относительной частотой возникновения $p_l^{\text{ДФ}}$. Совокупность элементов системы обеспечения достоверности информации (СОДИ) можно охарактеризовать показателями качества совокупности защитных механизмов передачи, хранения и обработки i-го ИР в условиях воздействия l-го ДФ: $x_{il}^{\text{п}}$, $x_{il}^{\text{х}}$, $x_{il}^{\text{о}}$. Использование этих механизмов снижает вероятность нарушения достоверности данных i-го ИР l-м ДФ $p_{il}^{\text{НД}}$.

Показатель достоверности данных i-го ИР равен:

$$D_i = 1 - \sum_{l=1}^{n} p_l^{\text{ДФ}} p_{il}^{\text{НД}} = 1 - \sum_{l=1}^{n} p_l^{\text{ДФ}} \left(1 - x_{il}^{\text{п}} x_{il}^{\text{х}} x_{il}^{\text{о}}\right), \quad (1)$$

а общий показатель достоверности ИР в КТКС:

$$D_{\text{ИР}} = \min_{i=1,z} D_i, \quad (2)$$

где z — общее количество ИР.

При оценке распределения относительной частоты возникновения ДФ (1) используются результаты экспертизы значимости и доступности каждого СФН [2, 3], оказывающего влияние на возникновение ДФ. Вследствие того что количество СФН в КТКС может достигать нескольких сотен, использование метода парных сравнений при экспертизе является весьма трудоемким.

Рассчитать относительную частоту возникновения ДФ, сократив количество сравнений без существенного снижения точности оценки, возможно следующим образом.

1. Разделим СФН на группы по функциональным особенностям и для каждой группы построим частные матрицы парных сравнений:

$$\mathbf{M}_{br} = \left\| br_{\alpha\beta} \right\|, \quad \forall \alpha, \beta = \overline{1, K_r}, \quad (3)$$

где $br = \left\{ br_1, br_r, ..., br_{K_L} \right\}$ — множество параметров группы r из K_r параметров;

$$br_{\alpha\beta} = -br_{\beta\alpha}, \quad \forall \alpha,\beta = \overline{1,K_r}, \quad \forall r = \overline{1,L}, \tag{4}$$

$br_{\alpha\beta} = \{-8...0...8\}$ соответствует $\left\{ 1/9 ... 1 ... 9 \right\}$ шкалы Саати [4].

2. Эксперт проводит парное сравнение значимости каждой группы (по условию, аналогичному (4)):

$$\mathbf{M}_B = \left\| B_{\alpha\beta} \right\|, \quad \forall \alpha = \overline{1, L}, \quad \forall \beta = \overline{1, L}. \tag{5}$$

3. В общей матрице сравнения всех СФН матрицы (3) необходимо расположить по главной диагонали, а остальные фрагменты заполнить суммой соответствующих (по индексам) значений матрицы (5) и смещений, вычисленных по соответствующим (также по индексам) строкам матриц (3).

Пример матрицы для общего набора с двумя группами СФН:

$$\mathbf{M} = \left| \begin{array}{ccc|ccc} b1_{11} & ... & b1_{1K_1} & Sb1_{1\cup 1} + B_{12} & ... & Sb1_{1\cup K_2} + B_{12} \\ ... & ... & ... & ... & ... & ... \\ b1_{K_1 1} & ... & b1_{K_1 K_1} & Sb1_{K_1\cup 1} + B_{12} & ... & Sb1_{K_1\cup K_2} + B_{12} \\ \hline Sb1_{1\cup 1} + B_{21} & ... & Sb1_{1\cup K_1} + B_{21} & b2_{11} & ... & b2_{1K_2} \\ ... & ... & ... & ... & ... & ... \\ Sb1_{K_2\cup 1} + B_{21} & ... & Sb1_{K_2\cup K_1} + B_{21} & b2_{K_2 1} & ... & b2_{K_2 K_2} \end{array} \right|,$$

где $Sbr_\alpha = \sum_{\beta=1}^{K_r} br_{\alpha\beta}$ $\left(\forall \alpha = \overline{1, K_r}, \ \forall r = \overline{1, L} \right)$ — сумма смещений элемента α относительно всех $\beta = \overline{1, K_r}$, т.е. его превосходство, если Sbr_α >0; подавление, Sbr_α <0; равная значимость, если Sbr_α =0.

4. Установив взаимосвязи ДФ и СФН как путей их реализации $\mathbf{M}_{\text{ПСС}} = \left\| \rho_{ns} \right\|$, где s — общее количество СФН, можно рассчитать матрицу критичностей ДФ: $\mathbf{M}_{\text{к}} = \mathbf{M}_{\text{ПСС}} \times \mathbf{M} = \left\| \omega_{ns} \right\|$.

5. Суммы элементов этой матрицы по каждой строке $\omega_l = \sum_{k=1}^{s} \omega_{lk}$, $\forall l = \overline{1, n}$ характеризуют критичность каждого ДФ в отдельности.

6. Распределение значений частоты возникновения ДФ соответствует распределению значений критичности: $p_l^{\text{ДФ}} = \omega_l \left(\sum_{l=1}^{n} \omega_l \right)^{-1}$.

Возможность нарушения достоверности (уничтожение, модификация ИР) зависит от качества элементов СОДИ:

$$p_{il}^{\text{НД}} = 1 - \left(1 - \prod_{q_1} \left(1 - \delta_{ilq_1}^{\text{п}} x_{ilq_1}^{\text{п}} \right) \right) \left(1 - \prod_{q_2} \left(1 - \delta_{ilq_2}^{\text{х}} x_{ilq_2}^{\text{х}} \right) \right) \left(1 - \prod_{q_3} \left(1 - \delta_{ilq_3}^{\text{о}} x_{ilq_3}^{\text{о}} \right) \right), \tag{6}$$

где $x_{ilq_1}^{\text{п}}, x_{ilq_2}^{\text{х}}, x_{ilq_3}^{\text{о}}$ — показатели качества q-го механизма защиты процесса передачи, хранения или обработки соответственно i-го ИР в условиях воздействия l-го ДФ; $0 \le \delta_{ilq} \le 1$ — предел достаточности q-го механизма защиты при условии, что он является единственным

механизмом, противодействующий *l*-му ДФ, который способен нарушить достоверность данных *i*-го ИР.

Качество механизма защиты можно определить, оценив его отдельные характеристики. Часть характеристик — количественные. Для их оценки необходимо определить оптимальное значение показателя. Это можно сделать экспертным путем. Эксперты определяют границы и наиболее вероятное оптимальное значение. Средневзвешенное оптимальное значение, по оценкам всех экспертов, равно [5]:

$$x^{\text{опт}} = \sum_{\varepsilon=1}^{m} x_{\varepsilon}^{\text{опт}} \nu_{\varepsilon},$$

где ν_{ε} — коэффициент авторитета ε-го эксперта.

Описание нечеткого количественного параметра должно иметь нормальный вид функции распределения, учитывающей нелинейность распределения [5]. Для оценки характеристик, не являющихся количественными, необходимо построить функцию принадлежности на универсальном множестве $G = \{ g_1, g_2, ..., g_p \}$ характеристик КСПД. Нечеткое множество A_q, отражающее степень принадлежности *q*-го механизма СОДИ к оптимальному, определяется множеством степеней соответствия каждой характеристики СОДИ оптимальному, значению $Y_q = \{ y_1, y_2, ..., y_p \}$ и множеством степеней влияния характеристик на качество механизма в целом $\Sigma_q = \{ \sigma_1, \sigma_2, ..., \sigma_p \}$.

Используя базовые отношения каждой характеристики СОДИ и операции над нечеткими множествами, можно получить функцию принадлежности для любого качественного экспертного описания, построенного на основе базовых.

Степень влияния характеристики СОДИ на качество механизма можно найти из матрицы парных сравнений [5]: $\mathbf{M}_{\varepsilon}^{\Sigma} = \left\| \sigma_{pp}^{\varepsilon} \right\|$, тогда качество *q*-го механизма можно выразить как:

$$x_{ilq}^{\varepsilon} = \sum_{\alpha=1}^{p} y_{\alpha}^{\varepsilon} \sigma_{\alpha}^{\varepsilon}. \qquad (7)$$

Показатели (7) перед подстановкой в (6) должны быть откорректированы с учетом коэффициентов авторитета экспертов.

Обеспечение требуемого уровня достоверности ИР в КСПД основано на повышении качества функционирования различных элементов СОДИ и дополнении ее новыми элементами. Прогнозирование изменения частных показателей (1) и общего показателя достоверности (2) возможно путем частичного пересчета тех характеристик КСПД, которые сами претерпели изменение. Таким образом, представленная методика позволяет как оценить текущий уровень достоверности информации, так и спрогнозировать его изменение.

СПИСОК ЛИТЕРАТУРЫ

1. *Мамиконов А. Г.* Достоверность, защита и резервирование информации в АСУ. М.: Энергоатомиздат, 1986. 304 с.

2. *Полянский Д. А.* Применение методики экспертных оценок для расчета вероятностей возникновения угроз безопасности информационной системе предприятия // Тр. XXVI Междунар. науч.-техн. конф. „Проблемы эффективности безопасности функционирования сложных технических и информационных систем“. Серпухов: Серпуховской ВИ РВ, 2007. № 1. С. 68—72.

3. *Полянский Д. А., Монахов М. Ю.* Методика определения значимости условий возникновения ошибок при обработке информации в АСУП // Автоматизация в промышленности. 2008. № 11. С. 10—12.

4. *Саати Т. Л.* Принятие решений. Метод анализа иерархий. М.: Радио и связь, 1993. 278 с.

5. *Полянский Д. А., Файман О. И.* Комплексная защита объектов информатизации. Кн. 16. Экономика защиты информации. Владимир: Изд-во ВлГУ, 2009. 96 с.

Сведения об авторах

Дмитрий Александрович Полянский — канд. техн. наук, доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: polyansk@rambler.ru

Михаил Юрьевич Монахов — д-р техн. наук, профессор; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; заведующий кафедрой; E-mail: mmonakhov@vlsu.ru

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.

УДК 004.942

Д. А. Полянский, О. И. Файман, С. Ю. Кириллова

ИНСТРУМЕНТАЛЬНЫЙ КОМПЛЕКС КОНТРОЛЯ ДОСТОВЕРНОСТИ ИНФОРМАЦИИ В КОРПОРАТИВНОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ АСУ

Рассмотрены структура и состав комплекса инструментальных средств контроля достоверности данных, циркулирующих в корпоративной сети. Проанализированы особенности применения инструментального комплекса.

Ключевые слова: *достоверность данных, информационный ресурс, корпоративная сеть, дестабилизирующий фактор, экспертная оценка.*

Контроль текущего уровня достоверности информации, циркулирующей в корпоративной сети передачи данных (КСПД), предполагает выполнение большого количества операций, в том числе действий по математической обработке экспертных данных. Любое варьирование структуры и/или состава средств системы обеспечения достоверности информации (СОДИ) приводит к изменению общих показателей.

Следовательно, для оперативного контроля уровня достоверности информации, а также с целью выбора комплекса средств обеспечения достоверности путем сравнения получаемых общих показателей необходим инструментальный комплекс (ИК), позволяющий решать следующие задачи:

— поддержка базы знаний дестабилизирующих факторов (ДФ), структурно-функциональных недостатков (СФН), информационных ресурсов (ИР), оценочных таблиц и результатов ранее проведенных исследований [1];

— обеспечение процесса проведения экспертизы корпоративной телекоммуникационной сети (КТКС) на основе базы знаний;

— математическое обеспечение процесса получения частных показателей качества КТКС и СОДИ и показателей достоверности.

Сказанное выше определяет состав ИК: база знаний, модуль поддержки базы знаний, модуль обеспечения процесса проведения экспертизы КСПД и вычислительный модуль.

Высокая структурная сложность моделей определения качества средств защиты и необходимость в решении сопутствующей задачи оценки рисков и экономической эффективности СОДИ [2] диктуют требования к ИК.

Требования к базе знаний и модулю ее поддержки как к единому целому следующие:

— поддержка хранения в систематизированном виде списков ДФ, СФН, ИР и оценочных лингвистических таблиц;

— поддержка возможности добавления новых ДФ, СФН, ИР и оценочных лингвистических таблиц;

— поддержка возможности изменения формулировок ДФ, СФН, ИР и описаний в лингвистических таблицах;

— поддержка возможности изменения структуры и классификации ДФ, СФН и ИР.

Требования к модулю обеспечения процесса проведения экспертизы:

— поддержка возможности выбора из базы знаний ДФ, СФН, ИР, актуальных для исследуемой КТКС;

— обеспечение процесса ввода оценок количественных показателей: „стоимость“, „весовой коэффициент“, „степень выполнения“;

— обеспечение процесса выбора по лингвистическим таблицам первичных оценок качественных показателей: „сравнительная значимость“, „ценность“, „доступность“, „причинно-следственная связь“, „предел достаточности“, „степень соответствия“, „степень влияния“.

Вычислительный модуль выполняет расчеты:

— относительной частоты возникновения ДФ;

— возможности нарушения достоверности ИР;

— ущерба, вызванного нарушением достоверности данных ИР;

— экономических характеристик использования ресурсов;

— рисков при отсутствии и наличии СОДИ;

— достоверности данных ИР в КТКС.

Потребности в проведении переоценок различных показателей вследствие изменения конфигурации КТКС диктуют дополнительные требования к ИК:

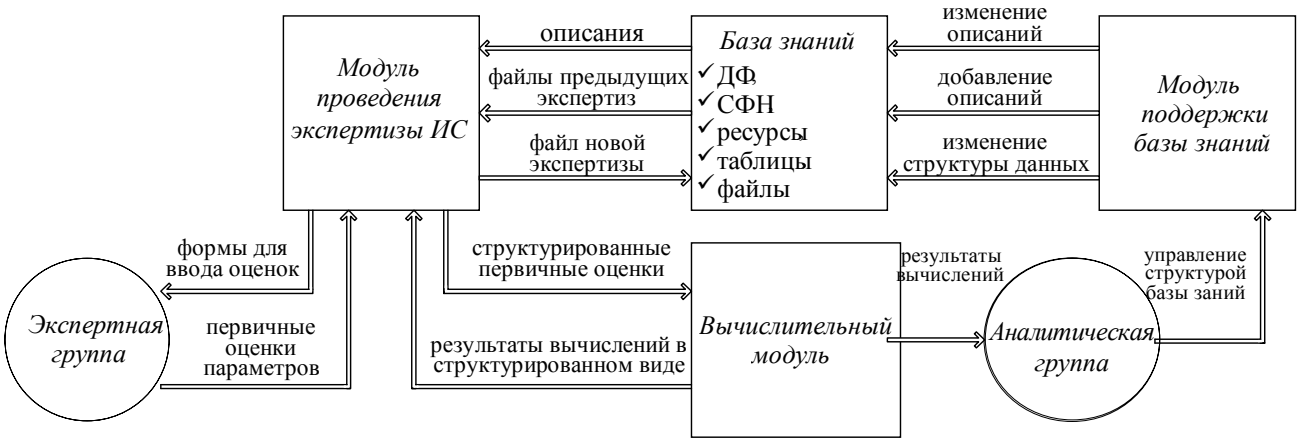
— хранение результатов экспертизы КТКС и оценки достоверности информации в формате текстового документа;

— возможность пересчета итоговых показателей в автоматическом режиме после внесения изменений в файл экспертных данных;

— возможность сравнения и расчет эффективности изменений, вносимых в КТКС с целью повышения достоверности представленных новым файлом экспертных данных;

— дружественный интерфейс в использовании, обновлении и добавлении информации в базу знаний.

Функциональная схема работы ИК, представленная на рисунке, отражает приведенные выше задачи, состав и требования к системе, а также информационное взаимодействие с ней аналитической и экспертной групп.



Анализ особенностей проведения экспертизы для предприятий с разной как по размерности, так и по структуре информационной системой показывает, что база знаний должна со-

держать следующие массивы данных, а также экспериментально установленные отношения и описания:

— классификатор типов ДФ;

— массив наименований ДФ, ассоциированных с каждым типом, и их описания;

— классификатор типов СФН;

— массив наименований СФН, ассоциированных с каждым типом, и их описания;

— массив видов ИР;

— оценочные таблицы описаний для исследования всех качественных характеристик КТКС;

— файлы экспертных данных, содержащие результаты исследования КТКС предприятий в виде полных массивов ДФ, СФН, ИР, ресурсов системы обработки информации, средств СОДИ, а также рассчитанные величины рисков и показателей достоверности информации.

Вычисление текущего уровня достоверности данных ИР основано на исследовании КТКС предприятия. Решить эту задачу позволяет модуль проведения экспертизы, который реализует интерфейс взаимодействия эксперта с базой знаний:

— выбор из базы знаний ДФ и СФН, актуальных для исследуемой КТКС;

— выбор из базы знаний описаний ИР;

— ввод первичных оценок отдельных параметров в формы, созданные модулем на основе выборки ДФ, СФН и ИР;

— изменение исходных данных предыдущего исследования КТКС и их дополнение на основе файлов предыдущих экспертиз, хранящихся в базе знаний.

Модуль формирует массив исходных данных экспертизы и передает его в вычислительный модуль, где происходит их обработка и получение конечных результатов: информационные риски, экономическая эффективность и достоверность данных ИР. Первичные данные экспертизы и результаты вычислений модуль заносит в файл новой экспертизы и вносит его в базу знаний.

Дополнительным в ИК является модуль поддержки базы знаний, назначение которого состоит в управлении содержимым файлов базы знаний: изменение структуры и содержания отдельных описаний, добавление новых описаний и удаление старых.

СПИСОК ЛИТЕРАТУРЫ

1. *Полянский Д. А.* Применение методики экспертных оценок для расчета вероятностей возникновения угроз безопасности информационной системе предприятия // Тр. XXVI Междунар. науч.-техн. конф. „Проблемы эффективности безопасности функционирования сложных технических и информационных систем“. Серпухов: Серпуховской ВИ РВ, 2007. № 1. С. 68—72.

2. *Полянский Д. А., Файман О. И.* Комплексная защита объектов информатизации. Кн. 16. Экономика защиты информации. Владимир: Изд-во ВлГУ, 2009. 96 с.

Сведения об авторах

Дмитрий Александрович Полянский — канд. техн. наук, доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: polyansk@rambler.ru

Ольга Игоревна Файман — Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; ассистент; E-mail: Olich06@inbox.ru

Светлана Юрьевна Кириллова — канд. техн. наук, доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информационных систем и информационного менеджмента; заместитель заведующего кафедрой; E-mail: sv-kir@mail.ru

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.

УДК 004.021

Д. В. Мишин, М. Ю. Монахов

ОБ АВТОМАТИЗАЦИИ ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКОЙ ИНФРАСТРУКТУРЫ АСУП

Предлагаются средства автоматизации процессов администрирования информационно-технологической инфраструктуры автоматизированной системы управления предприятием, используемых в поисковых и восстановительных работах при деструктивных воздействиях на ее компоненты.

Ключевые слова: *администрирование корпоративной сети передачи данных, автоматизированная система администрирования, администратор.*

Введение. Под ИТ-инфраструктурой автоматизированной системы управления предприятием (АСУП) будем понимать композицию следующих компонентов: вычислительная техника (компьютеры пользователей, корпоративные серверы и т.д.) и периферийное оборудование (сетевые принтеры, факсы и т.д.), телекоммуникационное оборудование (коммутаторы, маршрутизаторы, аппаратные межсетевые экраны и т.д.) и кабельные системы, системное (операционная система, утилиты) и прикладное программное обеспечение (ПО), объединенных понятием „корпоративная сеть передачи данных“ (КСПД).

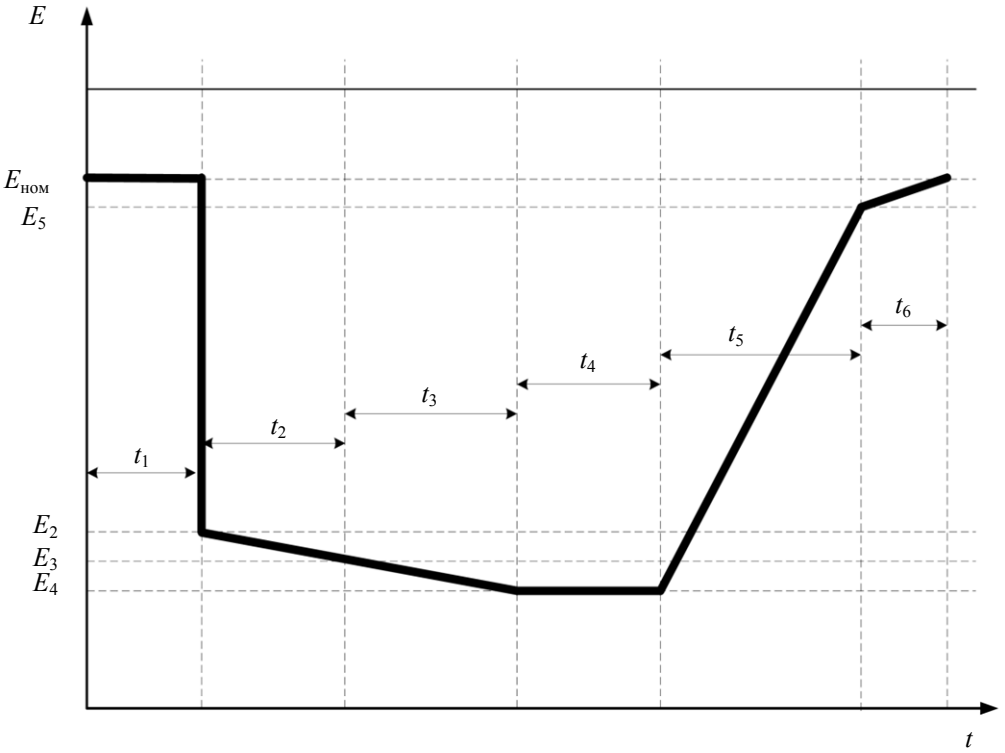
Понятие „функциональная устойчивость“ [1] КСПД включает свойства надежности, живучести и безопасности, отражает способность сохранения и/или восстановления возможности выполнения возложенных на КСПД функций, при деструктивных воздействиях (поражающих факторов, ПФ) на ее компоненты. Одной из характеристик функциональной устойчивости КСПД является время восстановления работоспособности. Все этапы технологического цикла восстановления работоспособности [2] КСПД современных предприятий реализуются, как правило, в рамках процессов администрирования [3] — операционного управления, направленного на обеспечение надежного, стабильного и безопасного функционирования КСПД на протяжении всего ее жизненного цикла сети с качеством, требуемым АСУП. Реализация процессов администрирования КСПД осуществляется службой технической поддержки (СТП) предприятия (в составе ИТ-отдела), основным звеном которой являются администраторы КСПД (будем называть их так вне зависимости от квалификации и функциональной специализации).

Централизованный оперативный контроль, управление и координация процессов администрирования (диспетчеризация) осуществляются специальным сотрудником СТП (лицом, принимающим решения, ЛПР) — диспетчером, аналитиком, главным администратором или начальником СТП — на основании личного опыта, имеющейся оперативной информации о текущих характеристиках КСПД, нормативной документации и информации об имеющихся ресурсах.

Настоящая работа посвящена исследованию методов и средств автоматизации процессов администрирования КСПД интегрированных АСУ промышленных предприятий, позволяющих снижать время восстановления работоспособности элементов КСПД и как следствие — обеспечивать ее функциональную устойчивость.

Технологический цикл восстановления КСПД. Рассмотрим технологический цикл устранения инцидента КСПД в рамках процессов администрирования при однократном воздействии ПФ на типовую КСПД (см. рисунок).

Этап 1. Штатный режим. КСПД функционирует в штатном режиме с требуемой (номинальной) эффективностью $E_{\text{ном}}$. Данный этап сопровождается итеративным контролем значений параметров элементов сети и процедурами периодического обслуживания (не приводящими к снижению $E_{\text{ном}}$), осуществляемыми администраторами с использованием специальных средств — сканеров сети, программ инвентаризации аппаратных компонентов и программного обеспечения узлов КСПД и т.д. Этап завершается при возникновении (мгновенном) инцидента (воздействии ПФ). При этом эффективность АСУП может достигнуть нуля (выход из строя системы) или некоторого значения E_2, в зависимости от типа и мощности ПФ ($0 \le E_2 < E_{\text{ном}}$).



Этап 2. Обнаружение инцидента. На этом этапе происходит обнаружение воздействия ПФ, поиск отказавших элементов КСПД, сбор информации об инциденте и его последствиях, т.е. формально — производится поиск отказавших элементов КСПД и их отклонения от заданных (эталонных) значений. В течение этапа эффективность АСУП может продолжать снижаться вследствие вторичных отказов ($0 \le E_3 \le E_2$).

Автоматизация этапа обнаружения инцидента предусматривает несколько направлений:

— создание специальной базы профилей, содержащих значения эталонных состояний элементов КСПД, и программного инструментария для получения этих значений;

— внедрение системы *Service Desk*, позволяющей пользователям оперативно информировать СТП о возникающих инцидентах;

— внедрение интеллектуальных средств анализа средств защиты информации КСПД по журналам событий — систем обнаружения вторжений, систем межсетевого экранирования, антивирусных комплексов и т.д.

Этап 3. Идентификация инцидента. Производится анализ собранной информации об инциденте (идентификация инцидента и его классификация), анализ возможных решений инцидента. Выбирается подходящее (возможно, оперативное (временное), обеспечивающее частичное повышение эффективности) решение инцидента. В течение этапа эффективность КСПД может продолжать снижаться ($0 \le E_4 \le E_3$).

Задача автоматизации этапа идентификации инцидента может решаться внедрением специальной системы поддержки принятия решения (СППР), содержащей идентификационные

признаки (базу знаний, БЗ) инцидентов КСПД, статистические сведения о динамике их возникновения, систему прогнозирования и т.д. В случае ошибки/отказа автоматизированной идентификации (неизвестный инцидент) предусматривается пополнение БЗ СППР новыми сигнатурами по результатам исследования инцидента специальной экспертной группой.

Этап 4. Формирование программы решения. Происходит выработка последовательности функций администрирования (ФА) на основе выбранного варианта решения инцидента — программы решения. ФА предлагается рассматривать как элементарные управляющие воздействия, предназначенные для получения или изменения состояний элементов КСПД — настройки конфигурационного параметра программы, замены аппаратного модуля автоматизированного рабочего места, добавления учетной записи, смены пароля пользователя, установки ПО и т.д. Из множества альтернатив выбирается „подходящий“ администратор для выполнения первой/очередной ФА. Основной участник этапа — ЛПР, целевой задачей которого является выработка наиболее эффективной (в конкретной оперативной обстановке) стратегии администрирования.

Программу решения предлагается формировать по результатам имитационного моделирования процесса функционирования СТП [4, 5]. Формальная модель администратора КСПД и алгоритмов формирования программы (выбора исполнителя ФА) представлена в работах [6, 7].

Этап 5. Исполнение ФА администратором — замена или ремонт вышедших из строя элементов, реконфигурация оборудования и программного обеспечения. Формируется отчет о выполнении. В случае отказа ФА происходит возврат к этапу 3, иначе — к 4.

Автоматизация данного этапа возможна средствами документированного обеспечения администрирования (ДОА), позволяющими администратору использовать данные информационно-технической (паспорта элементов КСПД), информационно-графической (карты и диаграммы различных уровней и детализации КСПД) и организационно-правовой (регламенты обслуживания, инструкции, положения, журналы) документации [8]. Кроме того, данный этап предусматривает создание системы регистрации в журнале деятельности администраторов — их производительности, надежности выполнения ФА, трудозатрат и т.д.

Этап 6. Завершение инцидента. Производится контроль значений параметров КСПД. Освобождаются ресурсы администрирования. По завершении этапа переходим к этапу 1, реализуя цикл процесса восстановления КСПД. На данном этапе эффективность сети должна достигнуть значения $E_{\text{ном}}$.

Восстанавливаемость КСПД определяется временем обработки ее элементов и может выражаться через сумму следующих показателей (см. рисунок): время обнаружения инцидента — t_2; время идентификации инцидента — t_3; время формирования программы решения — t_4; время выполнения программы (сумма по времени всех ФА) — t_5; время завершения инцидента — t_6. Предложенные решения по автоматизации позволяют уменьшить время реализации рассматриваемого цикла.

Особенности и рекомендации по внедрению

1. Этап 2, на наш взгляд, самый сложный. Авторы неоднократно сталкивались с такой ситуацией, когда показатели функциональных элементов „в норме“, система обнаружения вторжений с сетевым экраном не отражает подозрительной активности, а производительность КСПД падает. В таких случаях рекомендуется выделить определенное время на поиск источника инцидента (самым квалифицированным администратором), после чего (случай необнаружения) требуется делать „начальную установку“ (перезагрузку) всей КСПД.

2. В современных АСУП часто используется уникальное ПО, устанавливаемое и обслуживаемое сторонними организациями. В случае возникновения инцидента, связанного с данными элементами, приходится приглашать стороннего специалиста, т.е. увеличивается t_3, t_4, t_5. Частично преодолеть эту ситуацию возможно за счет удаленного администрирования (*freelance* и *outsourcing*).

3. Некоторые виды инцидентов в КСПД возникают регулярно, другие — редко. Необходимо поддерживать способность быстрого реагирования на возникающие события администраторов. С этой целью авторы рекомендуют создавать постоянно действующую в КСПД автоматизированную систему тренинга, моделирующую инциденты и оценивающую качество их устранения администраторами.

СПИСОК ЛИТЕРАТУРЫ

1. *Бородакий Ю. В., Тарасов А. А.* О функциональной устойчивости информационно-вычислительных систем // Информационное противодействие угрозам терроризма. Таганрог: ЮФУ, 2006. № 6. С. 79—93.

2. *Додонов А. Г., Флейтман Д. В.* Корпоративные информационные системы: обеспечение живучести // Математические машины и системы. 2005. № 4. С. 118—130.

3. ГОСТ Р ИСО/МЭК 7498-4-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Ч. 4. Основы административного управления.

4. *Мишин Д. В.* О применении среды моделирования AnyLogic в исследовании эффективности алгоритмов выбора администраторов корпоративной сети передачи данных // Тр. 5-й Всерос. науч.-практич. конф. „Имитационное моделирование. Теория и практика“ ИММОД-2011. СПб, 2011. Т. 1. 448 с.

5. *Мишин Д. В., Монахова М. М.* Имитационное исследование алгоритмов оптимизации административных ресурсов КСПД // Проблеми інформатики і моделювання. Тез. 11-і міжнар. наук.-техн. конф. Харків-Ялта: НТУ „ХПІ“, 2011. 84 с.

6. *Мишин Д. В., Монахова М. М.* О модели администратора автоматизированной системы администрирования корпоративной сети передачи данных // „Перспективные технологии в средствах передачи информации“. Матер. 9-й Междунар. науч.-технич. конф. Владимир: ВлГУ, 2011. Т. 1. 272 с.

7. *Мишин Д. В., Монахова М. М.* Алгоритм выбора администраторов корпоративной сети передачи данных // „Информационные системы и технологии ИСТ-2011“. Матер. XVII Междунар. науч.-технич. конф. Н. Новгород, 2011. С. 147—148.

8. *Мишин Д. В., Монахова М. М.* Система документированного обеспечения администрирования корпоративной сети передачи данных // Вестн. Костромского гос. ун-та им. Н. А. Некрасова. Сер. Технические и естественные науки „Системный анализ. Теория и практика“. 2010. Т. 16, № 1. С. 70—72.

Сведения об авторах

Денис Вячеславович Мишин — аспирант; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: mishin.izi@gmail.com

Михаил Юрьевич Монахов — д-р техн. наук, профессор; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; заведующий кафедрой; E-mail: mmonakhov@vlsu.ru

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.

УДК 004.021

Д. В. Мишин, М. М. Монахова, А. А. Петров

СИСТЕМА АДМИНИСТРИРОВАНИЯ КОРПОРАТИВНОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ АСУП

Предложена модель автоматизированной системы администрирования корпоративной сети передачи данных, проанализированы механизмы повышения эффективности ее функционирования, а также вопросы ее внедрения в автоматизированную систему управления промышленным предприятием.

Ключевые слова: *администрирование корпоративной сети передачи данных, автоматизированная система управления, администратор.*

Введение. Корпоративная сеть передачи данных (КСПД) является основным звеном планирования и управления производственно-хозяйственной деятельностью любого предприятия. Эффективность функционирования такой сети в значительной степени определяется уровнем квалификации обслуживающего персонала, специалистами, обеспечивающими работоспособность КСПД, ее производительность, безопасность, возможность диагностики и восстановление. В решении этих задач главенствующая роль принадлежит службе администрирования сети, функционирующей в системе технической поддержки.

Под системой администрирования понимается совокупность методов, средств и технологий, реализующих функции администрирования сети. Главная цель создания системы администрирования — обеспечение полной и постоянной работоспособности КСПД. Заметим, что службу администрирования КСПД крупного промышленного предприятия составляет не один десяток инженеров, кроме того, часть административных функций (по управлению уникальными программными комплексами) передается на аутсорсинг.

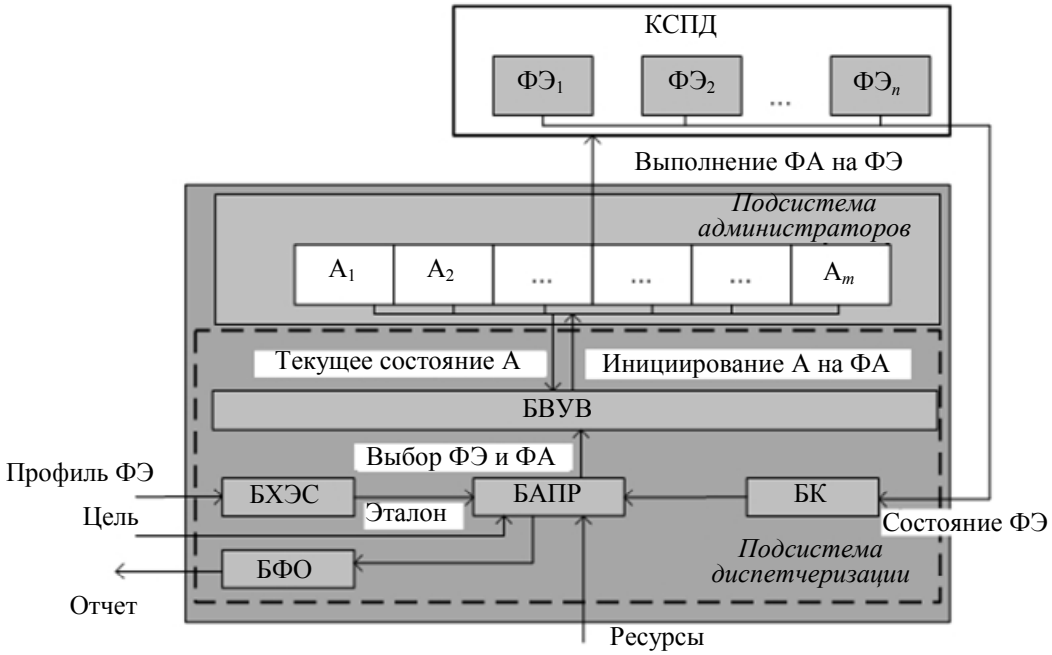
В настоящей статье предлагается модель автоматизированной системы администрирования (АСА) КСПД, эффективность функционирования которой определяется тремя компонентами: человеком, машинной и производственной средой. В статье анализируются механизмы повышения эффективности функционирования системы, а также вопросы ее внедрения в автоматизированную систему управления промышленным предприятием.

Элементы системы. Структурная схема автоматизированной системы администрирования приведена на рисунке.

Корпоративная сеть передачи данных представлена множеством функциональных элементов (ФЭ). Под ФЭ будем понимать неделимый (элементарный в рамках рассматриваемой модели) компонент узла сети, выполняющий одну или несколько элементарных функций по обработке или передаче информации в сети. Информация о текущем состоянии ФЭ поступает в блок контроля подсистемы диспетчеризации.

Подсистема администраторов. Декомпозиция процессов администрирования позволяет выделить множество элементарных функций (ФА), неделимых в рамках решения задач КСПД. Исполнителями ФА являются сотрудники службы администрирования, наделенные специализированными программными и техническими средствами, их будем называть администраторами (А) КСПД. Администраторы могут быть „универсалами“ (способными выполнять все ФА), иметь функциональную специализацию, обладать тем или иным уровнем квалификации (знаний, умений, навыков в выполнении конкретной ФА). Функции администрирования предлагается рассматривать как элементарные управляющие воздействия с целью получения или изменения состояний ФЭ КСПД, выполняемые администратором или их

группой. Множество типовых ФА, характерных для КСПД крупного промышленного предприятия, описано в работе [2].



Подсистема диспетчеризации включает в себя следующие блоки.

1. Блок выработки управляющих воздействий (БВУВ), который на основе анализа информации о текущем состоянии администраторов — занят/свободен, сможет/не сможет выполнить ФА (за приемлемое время с приемлемым качеством) и т.п., поступающей из подсистемы администраторов, и заявок на выполнение ФА на конкретном ФЭ КСПД, производит однозначный выбор конкретных администраторов на выполнение конкретных ФА. В условиях ограниченного числа администраторов оптимизация распределения по ним ФА является одной из актуальных задач в обеспечении требуемого качества функционирования КСПД. Предлагается использовать методику диспетчеризации потока задач, сформированного в виде очереди на основании приоритета как общего для всех ФЭ КСПД критерия [1].

2. Блок контроля (БК) преобразует информацию, получаемую из всех ФЭ посредством сервисов аудита и ведения журнала событий (журналирования), в данные для сравнения в БАПР с соответствующими профилями.

3. Блок анализа и принятия решений (БАПР) на основе существующих целей, текущих профилей ФЭ, имеющихся ресурсов и текущего состояния элементов КСПД вырабатывает решение о выполнении определенных ФА на конкретных ФЭ.

4. Блок хранения эталонных состояний (БХЭС) включает базу данных, содержащую значения эталонных состояний (текущих профилей) элементов КСПД, а также комплект документации на ФЭ (узлы КСПД, каналы связи и др.).

5. Блок формирования отчетов (БФО) позволяет в виде документированного отчета представить сведения о текущем, прошедшем и прогнозируемом состоянии КСПД по запросу или в случае многократных ошибок, генерируемых БАПР.

Подробно аппаратно-программная реализация блоков подсистем АСА КСПД АСУП описана в статье [3].

Внедрение. Разработанные модели и алгоритмы легли в основу программного комплекса системы администрирования сети передачи данных (СПД) администрации Владимирской области (АВО) и СПД ОАО „Завод «Автоприбор»“ (Владимир). Программный комплекс системы администрирования СПД АВО на данном этапе обеспечивает контроль и управление

более 1000 территориально распределенных узлов (ФЭ); АСА СПД обеспечивает контроль и управление более 2000 узлов.

Собранные в процессе статистического наблюдения внедренной системой данные показали, что упорядочилось функционирование административной службы ИТ-подразделения, а также количество отказов оборудования в течение дня в среднем понизилось.

СПИСОК ЛИТЕРАТУРЫ

1. *Mishin D. V., Monakhova M. M.* About the optimization of the administration corporate area networks of the data transmission under scarce administrative resources // Herald of the National Technical University "KhPI". Information Science and Modelling. Kharkov: NTU "KhPI", 2011. N 17. P. 101—108.

2. *Мишин Д. В., Монахова М. М.* О модели администратора автоматизированной системы администрирования корпоративной сети передачи данных // „Перспективные технологии в средствах передачи информации". Матер. 9-й Междунар. науч.-технич. конф. Владимир: ВлГУ, 2011. Т. 1. С. 76—79.

3. *Мишин Д. В., Монахова М. М.* Модель автоматизированной системы администрирования корпоративной сети передачи данных // „Интеллектуальные системы" Тр. 9-го Междунар. симп. М.: РУСАКИ, 2010. С. 268—271.

Сведения об авторах

Денис Вячеславович Мишин — аспирант; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: mishin.izi@gmail.com

Мария Михайловна Монахова — Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; инженер; E-mail: monakhova_mariya@bk.ru

Аркадий Александрович Петров — аспирант; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: petrov@avo.ru

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

УДК 681.3

Л. М. Груздева, М. Ю. Монахов

ПОВЫШЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ КОРПОРАТИВНОЙ СЕТИ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Формализована задача повышения производительности в условиях воздействия угроз информационной безопасности корпоративной сети как задача построения системы защиты, обеспечивающей максимально возможный уровень производительности сети при достоверном обнаружении и эффективном противодействии угрозам информационной безопасности.

Ключевые слова: *корпоративная сеть передачи данных, производительность, система защиты информации, угрозы информационной безопасности.*

Введение. Основными причинами интереса к вопросам повышения производительности корпоративной сети передачи данных (КСПД) являются возрастающая структурная сложность и размерность современных сетей, характеризующихся множественными изменяющимися во времени информационными связями, а также потребности в увеличении уровня информационной безопасности.

Снижение производительности сетей связано с недостаточной защищенностью вследствие широкого использования слабозащищенных протоколов HTTP, SNMP, FTP, TCP/IP; участия в процессе обработки информации пользователей различных категорий, их непосредственного и одновременного доступа к системным ресурсам и процессам. Современная система защиты информации (СЗИ), даже включающая систему обнаружения и предотвращения атак и вторжений IPS/IDS, не может гарантировать обнаружения 70 % информационных атак, что периодически приводит к значительному возрастанию вредоносного трафика (ВТ). В настоящее время актуальны задачи повышения достоверности обнаружения информационных атак, их идентификации, а также разработки методов и средств снижения их влияния на производительность КСПД.

Постановка задачи

1. Дано множество объектов КСПД $O = \{O_1, O_2, ..., O_{NS}\}$. Линии связи абсолютно надежны, помехоустойчивы и состоят из дуплексного канала; узлы коммутации (маршрутизаторы сегментов КСПД) имеют бесконечную память; трафик состоит из пакетов одинакового приоритета и образует пуассоновский поток; длительность обработки пакетов в узлах определяется экспоненциальным законом распределения.

2. СЗИ включает модули защиты, в состав которых входит средство обнаружения (СО, SO) воздействия угроз информационной безопасности (ИБ) из множества

$SO = \{SO_1, SO_2, ..., SO_N\}$ и средство противодействия (СП, SP) угрозам ИБ из множества $SP = \{SP_1, SP_2, ..., SP_M\}$.

3. Каждый элемент множества *SO* обладает следующими характеристиками: $p_i(t)\ \left(i = \overline{1, N}\right)$ — вероятность обнаружения угроз ИБ; $\overline{p_i}(t)\ \left(i = \overline{1, N}\right)$ — вероятность возникновения „ложной тревоги“; $t_{\text{об}i}\ \left(i = \overline{1, N}\right)$ — время обнаружения угроз ИБ, за которое достигается максимальное значение вероятности обнаружения угроз ИБ, т.е. $p_i^{\max} = \lim\limits_{t \to t_{\text{об}i}} p_i(t)$.

4. Каждый элемент множества *SP* обладает следующими характеристиками: $q_j(t)\ \left(j = \overline{1, M}\right)$ — вероятность противодействия угрозам ИБ; $t_{\text{пр}j}\ \left(j = \overline{1, M}\right)$ — время противодействия, за которое достигается максимальное значение вероятности противодействия, т.е. $q_j^{\max} = \lim\limits_{t \to t_{\text{пр}j}} q_j(t)$.

Требуется: обеспечить максимально возможный уровень производительности КСПД при достоверном обнаружении и максимально эффективном противодействии угрозам ИБ:

$$\left.\begin{array}{l} \Phi(\Pi) \to \max; \\ P_{\text{об}}(t) \to \max;\ \ \overline{P_{\text{ЛТ}}}(t) \to \min;\ Q_{\text{пр}} \to \max; \\ T_{\text{об}} + T_{\text{пр}} \le T_{\text{д}}, \end{array}\right\} \qquad (1)$$

где Ф(П) — производительность КСПД; $P_{\text{об}}(t) = \varphi_1\left(p_1(t),\ p_2(t), ..., p_N(t)\right)$ — вероятность обнаружения угроз ИБ; $\overline{P_{\text{ЛТ}}}(t) = \varphi_2\left(\overline{p_1}(t),\ \overline{p_2}(t), ..., \overline{p_N}(t)\right)$ — вероятность возникновения „ложной тревоги“; $Q_{\text{пр}}(t) = \varphi_3\left(q_1(t),\ q_2(t), ..., q_M(t)\right)$ — вероятность противодействия угрозам ИБ; $T_{\text{об}} = \varphi_4\left(t_{\text{об}1}, t_{\text{об}2}, ..., t_{\text{об}N}\right)$ — время обнаружения угроз ИБ; $T_{\text{пр}} = \varphi_5\left(t_{\text{пр}1}, t_{\text{пр}2}, ..., t_{\text{пр}M}\right)$ — время противодействия угрозам ИБ; $T_{\text{д}}$ — допустимые временные затраты на обеспечение защиты (φ_1, φ_2, φ_3, φ_4 — виды соответствующих функциональных зависимостей).

Для решения поставленной задачи была разработана СЗИ [1], функционирование которой удобно рассмотреть с помощью структурной модели обнаружения и противодействия атакам на ресурсы КСПД (см. рисунок).

Уровень обнаружения — совокупность СО. На выходе СО формируется сигнал $X_i(t)$ $\left(i = \overline{1, N}\right)$, принимающий значение либо единица (угроза ИБ обнаружена), либо нуль (угроза ИБ не обнаружена). Сигнал $X_i(t)$ характеризуется плотностью распределения вероятности его появления — $f_y\left(X_i(t)\right)$ — угроза ИБ есть, а также $f_n\left(X_i(t)\right)$ — угрозы ИБ нет:

$$f_y(X_i(t)) = \begin{cases} p_i(t) & \text{при } X_i(t) = 1, \\ 1 - p_i(t) & \text{при } X_i(t) = 0, \end{cases} \quad f_n(X_i(t)) = \begin{cases} \overline{p_i}(t) & \text{при } X_i(t) = 1, \\ 1 - \overline{p_i}(t) & \text{при } X_i(t) = 0. \end{cases}$$

В процессе формирования уровня обнаружения должны выполняться следующие условия:

1) возможность совместной работы объединяемых СО;

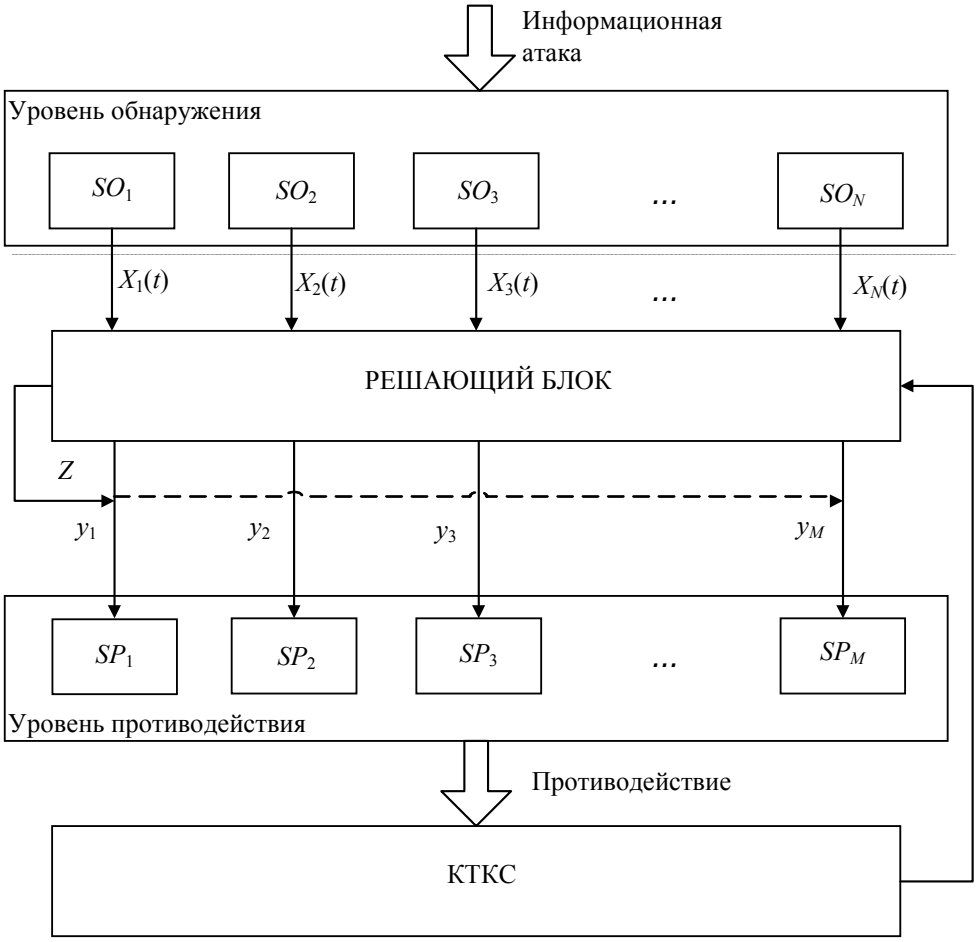
2) обеспечение оптимального времени работы по обнаружению и противодействию уг-

розам ИБ;

3) обеспечение заданной вероятности обнаружения угроз ИБ;

4) снижение средней частоты появления „ложных тревог“.

В статье [2] предложен алгоритм работы уровня обнаружения, основанный на понятии „критическая область угроз“ (КОУ). Достоинством алгоритма является учет возможного взаимного влияния различных СО, так как КОУ строится по вероятностным характеристикам уровня обнаружения, а не его отдельных модулей.



Уровень противодействия — совокупность СП, каждое из которых может быть задействовано при обнаружении угрозы ИБ.

Решающий модуль реализует следующий алгоритм: на основании показаний СП $\left(X_1(t),\ X_2(t),...,X_N(t)\right)$ принимается решение о наличии или отсутствии угроз ИБ:

$$Z=\begin{cases}1,\ \text{если угроза ИБ обнаружена,}\\ 0 \text{ — в противном случае.}\end{cases}$$

Если $Z=1$, то вырабатывается управляющее воздействие $\left(y_1,\ y_2,...,y_M\right)$, иначе — конец алгоритма.

В работе [1] предложен алгоритм определения узлов КСПД, в которых должны быть использованы СП при обнаружении угроз ИБ:

1) для каждого варианта инициирования уровня противодействия вычисляются вероятность $Q_{\text{пр}}(t)$ и производительность $\Phi(\Pi)$;

2) выбирается вариант использования СП, которому соответствует максимально возможная вероятность $Q_{\text{пр}}(t)$ при $\Phi(\Pi)\to\max$.

Реализация алгоритма позволяет обеспечить максимально возможное противодействие угрозам ИБ при максимально высоком уровне производительности.

Алгоритм работы СЗИ

Шаг 1. Запуск средств обнаружения. Время обнаружения $t = 0$.

Шаг 2. Снятие показаний, генерируемых СО $\left(X_1(t),\ X_2(t),...,X_N(t)\right)$.

Шаг 3. Если $X_1(t) = X_2(t) = ... = X_N(t) = 0$, то угроза ИБ не обнаружена $(Z = 0)$ и запуск средств уровня противодействия не производится, переход к шагу 2. В противном случае — $Z = 1$.

Шаг 4. Определение вероятностных характеристик:

$P_{\text{об}}(t) = \varphi_1\left(p_1(t),\ p_2(t),...,p_N(t)\right)$ — вероятность обнаружения угроза ИБ системой защиты; $\overline{P_{\text{ЛТ}}}(t) = \varphi_2\left(\overline{p_1}(t),\ \overline{p_2}(t),...,\overline{p_N}(t)\right)$ — вероятность возникновения „ложной тревоги“ СЗИ; $\Phi(P_{\text{об}}(t),\ \overline{P_{\text{ЛТ}}}(t))$ — критерий достоверности.

Шаг 5. Если $\Phi(P_{\text{об}}(t),\ \overline{P_{\text{ЛТ}}}(t)) \le \Phi_{\text{пор}}$ (значение критерия достоверности ниже порогового), то угроза ИБ не обнаружена и запуск средств уровня противодействия не производится, переход к шагу 2. В противном случае — $Z = 1$.

Шаг 6. Определение стохастической маршрутной матрицы $P_R(t)$.

Шаг 7. Запуск алгоритма определения узлов КСПД, в которых должны быть инициированы средства противодействия. Вырабатывается управляющее действие $Y = \left(y_1,\ y_2,...,y_M\right)$.

Шаг 8. Инициирование уровня противодействия в соответствии с $Y = \left(y_1,\ y_2,...,y_M\right)$. Конец алгоритма.

Выводы. Реализация предложенной модели организации защитных механизмов в КСПД позволяет обеспечивать требуемый уровень производительности за счет выбора алгоритма раннего и достоверного обнаружения угроз ИБ и оперативного использования средства противодействия угрозам ИБ в наиболее уязвимых узлах КСПД.

СПИСОК ЛИТЕРАТУРЫ

1. *Груздева Л. М.* Модели повышения производительности корпоративных телекоммуникационных сетей в условиях воздействия угроз информационной безопасности: Дис. … канд. техн. наук. Владимир: Изд-во Владим. гос. ун-та, 2011.

2. *Груздева Л. М., Монахов М. Ю.* Алгоритм раннего обнаружения атак на информационные ресурсы АСУП // Автоматизация в промышленности. 2008. № 3. С. 12—14.

3. *Груздева Л. М., Монахов М. Ю.* Алгоритм оптимизации функционирования распределенной системы защиты // Вестн. Костромского гос. ун-та им. Н. А. Некрасова. Сер. Техн. и естеств. науки „Системный анализ. Теория и практика“. 2008. Т. 14, № 2. С. 80—82.

Сведения об авторах

Людмила Михайловна Груздева — канд. техн. наук; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: glm@vlsu.ru

Михаил Юрьевич Монахов — д-р техн. наук, профессор; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; заведующий кафедрой; E-mail: mmonakhov@vlsu.ru

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.

УДК 681.3

Л. М. Груздева, К. Г. Абрамов, Ю. М. Монахов

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ КОРПОРАТИВНОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ С АДАПТИВНОЙ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Проанализированы результаты экспериментальных исследований производительности корпоративной сети передачи данных в условиях функционирования системы защиты информации, оперативно изменяющей настройки своих параметров под действием информационных атак.

Ключевые слова: *сеть передачи данных, производительность, система защиты информации, информационные атаки.*

Введение. Эффективная эксплуатация корпоративных сетей передачи данных (КСПД) в условиях воздействия информационных атак, их проектирование и модернизация невозможны без оценки показателей качества функционирования, одним из которых является производительность сети.

Анализ работ, посвященных изучению КСПД, и опыт практических исследований позволяют констатировать резкое снижение производительности в условиях воздействия информационных атак. Современные системы защиты (СЗИ) в известной степени решают данную проблему за счет частичного блокирования вредоносного трафика (ВТ), но обеспечение высокой вероятности обнаружения и задержки, связанные с противодействием, ведут к значительному расходованию ресурсов сетей, что в конечном итоге сопровождается снижением их производительности.

Экспериментально было выявлено, что отключение ряда средств противодействия (СП) не вызывает значительного снижения показателя защищенности КСПД, в то время как уменьшается средняя задержка обмена информацией.

В настоящей статье представлены результаты экспериментальных исследований характеристик производительности сети, функционирующей в условиях воздействия информационных атак, и адаптивной СЗИ, реализуемой на основе алгоритмов раннего и достоверного обнаружения информационных атак [1] и оперативного инициирования СП только в наиболее уязвимых узлах КСПД [2].

Экспериментальная установка. Схема сети представлена на рис. 1. Сеть состоит из двух сегментов, объединенных коммутатором: пять компьютеров моделируют подсеть, на которую непосредственно были организованы атаки, остальные три компьютера были задействованы для служебных нужд и как компоненты консоли распределенной сетевой системы обнаружения вторжений D-NIDS (Distributed Network IDS). Основные характеристики используемого оборудования представлены ниже.

1. Рабочая станция — Intel Core2 Duo CPU E8400 3 Гц, 2 ГБ RAM DDR2, HDD 256 ГБ.
2. Виртуальная рабочая станция — Virtualbox 3, PCnet-Fast3, 128 МБ RAM.
3. Сетевое оборудование — Intel Express 330T Hub, Compex PS2208B, кабель UTP-5.

Исследуемая сеть строилась на базе концентраторов (все компьютеры образуют единый домен коллизий, благодаря чему передающиеся по сети пакеты определяются сенсорами IDS). Для увеличения количества узлов сети были использованы инструменты виртуализации: на каждом компьютере были развернуты по три виртуальные машины, работающие под управлением MS WindowsXP. В качестве платформы для виртуализации

выбрана Sun VirtualBox3. Конфигурации программного обеспечения (ПО) всех виртуальных рабочих станций и сенсоров IDS одинаковы.

В качестве сенсоров созданной D-NIDS выбран Snort IPRoute2. Сведения о выявленных атаках хранятся сервером баз данных, на этом же компьютере установлено ПО для синхронизации времени всех узлов сети. В качестве СУБД использован MySQL-сервер версии 5.0.

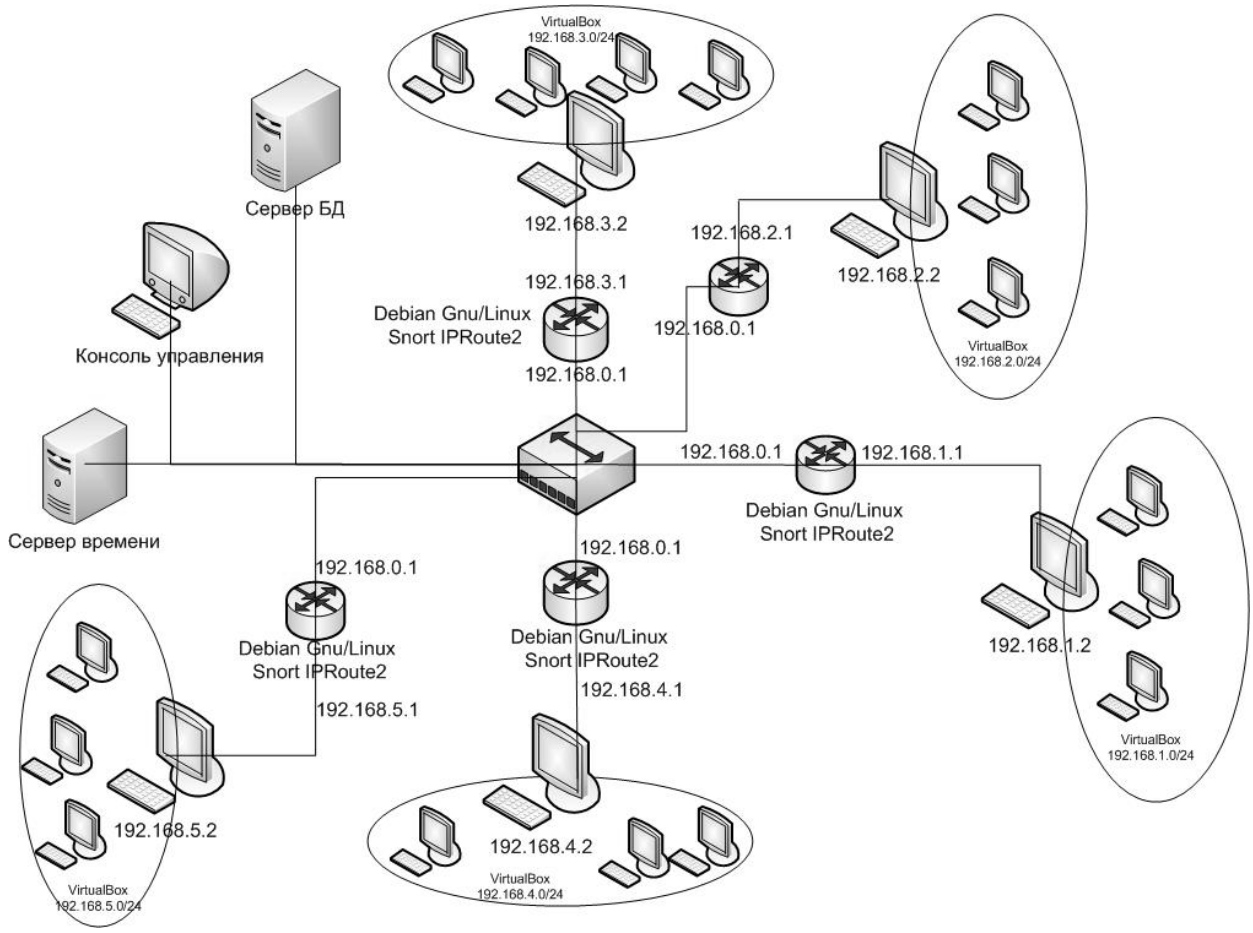


Рис. 1

Результаты и анализ экспериментальных исследований. В статье [3] рассмотрены результаты экспериментов по исследованию характеристик производительности КСПД, характеризующейся передачей больших объемов трафика в условиях воздействия угроз ИБ. Рассмотрим эксперимент по оптимизации СЗИ в сети. График изменения производительности в сети в условиях воздействия ВТ и динамического построения адаптивной СЗИ представлен на рис. 2.

Вредоносный трафик в системы стал поступать с 10-й секунды. Производительность сети с этого момента стала падать. В отсутствие СЗИ (кривая *1*) среднее время задержки пакета t_3 возросло до 0,33 с (производительность упала приблизительно в 6 раз за 40 с). В условиях типовой СЗИ (кривая *2*, в каждом узле типовой комплект) среднее время задержки возросло до 0,28 с, и после того как СЗИ блокировала ВТ (приблизительно на 50 с) оно уменьшилось до 0,18 с (производительность по сравнению с исходным вариантом снизилась примерно в 3 раза, что может обеспечить нормальное функционирование корпоративной сети).

Наилучший вариант, приводящий к снижению производительности всего лишь в 2 раза (кривая *3*), обеспечивается следующими механизмами: за счет использования алгоритма „критическая область угроз“ [1] снижается время обнаружения ВТ (примерно на 20 %), с помощью алгоритма расстановки СЗИ в узлах сети [2] в максимальный режим включается лишь

часть узлов СЗИ. В данном эксперименте вместо пяти СЗИ, функционирующих в максимальном варианте защиты, процедура подключила только три.

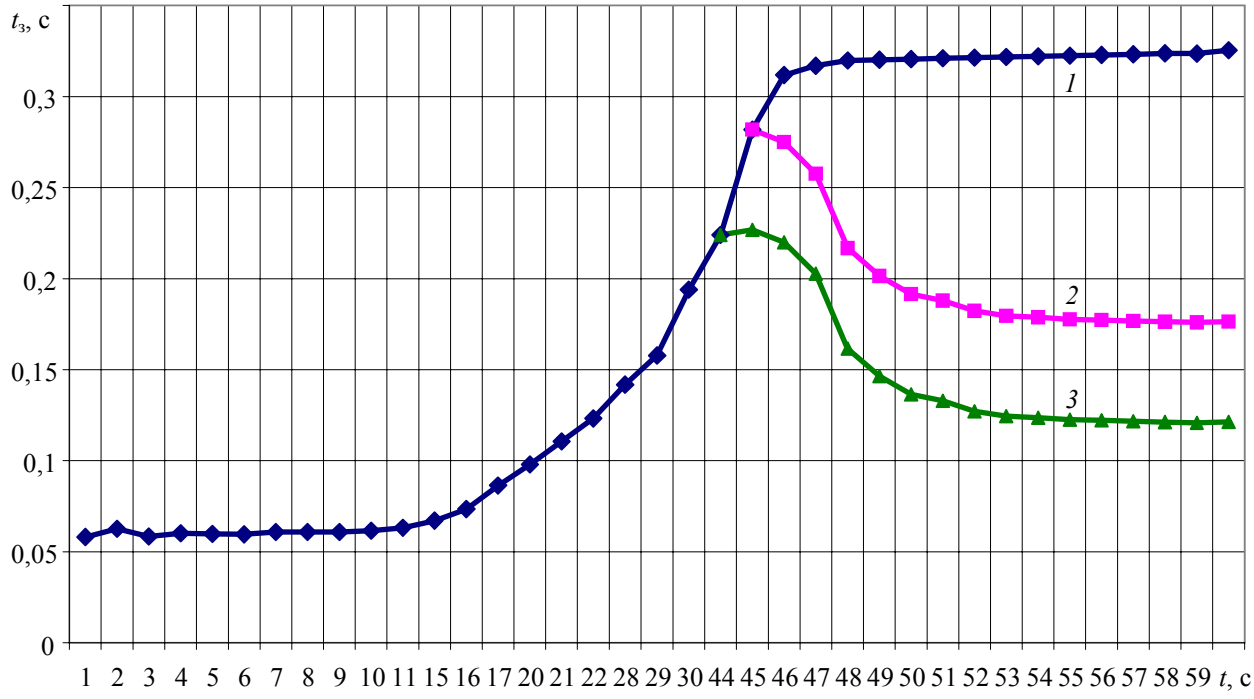


Рис. 2

Выводы. Раннее обнаружение информационных атак (результаты экспериментов показали снижение времени обнаружения на 20—25 % по сравнению с традиционными логическими схемами обнаружения угроз ИБ) позволяет оперативно использовать средства противодействия угрозам ИБ в наиболее уязвимых узлах КСПД. В результате производительность КСПД в условиях воздействия угроз ИБ остается на требуемом уровне (снижение не более чем в 2 раза), что обеспечивает нормальное функционирование корпоративной сети.

СПИСОК ЛИТЕРАТУРЫ

1. *Груздева Л. М., Монахов М. Ю.* Алгоритм раннего обнаружения атак на информационные ресурсы АСУП // Автоматизация в промышленности. 2008. № 3. С. 12—14.

2. *Груздева Л. М., Монахов М. Ю.* Алгоритм оптимизации функционирования распределенной системы защиты // Вестн. Костромского гос. ун-та им. Н. А. Некрасова. Сер. техн. и естеств. науки „Системный анализ. Теория и практика“. 2008. Т. 14, № 2. С. 80—82.

3. *Груздева Л. М., Монахов Ю. М., Монахов М. Ю.* Экспериментальное исследование производительности корпоративной телекоммуникационной сети // Проектирование и технология электронных средств. 2009. № 4. С. 21—24.

Сведения об авторах

Людмила Михайловна Груздева — канд. техн. наук; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: glm@vlsu.ru

Константин Германович Абрамов — аспирант; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: abramovk@vlsu.ru

Юрий Михайлович Монахов — канд. техн. наук, доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: unclefck@gmail.com

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.

УДК 519.6

А. В. Александров

УСТОЙЧИВОСТЬ SMT-ПРОТОКОЛА К АТАКАМ ПРОТИВНИКА В МОДЕЛИ БЕЗОПАСНОСТИ ДОЛЕВА—ЯО

Устанавливаются свойства конфиденциальности SMT-протокола (Secure Message Transmission Protocols) с общей памятью. Конфиденциальность понимается как устойчивость протокола передачи к атакам активного или пассивного противника в обобщенном канале связи, подчиненного модели безопасности Долева—Яо.

Ключевые слова: *криптографические протоколы передачи, схема разделения секрета, модель безопасности Долева—Яо.*

Введение. Практическая стойкость, которая лежит в основе современных криптосистем и криптографических протоколов, обеспечивает противодействие взлому закрытого текста или протокола передачи данных на время, большее времени сохранения конфиденциальности и жизни самого передаваемого документа. Возрастание вычислительной мощности компьютеров, появление новых видов криптографических атак на ключи шифрования и криптографические протоколы [1, 2] могут резко снизить порог практической стойкости современных криптографических средств. При создании практически стойких криптографических схем используется теория сложности алгоритмов и, в частности, так называемые односторонние функции. Доказательство существования односторонних функций опирается на не доказанную гипотезу о несовпадении классов алгоритмически P-сложных и NP-сложных задач: $P \neq NP$.

В криптографии востребован конфиденциальный обмен, обладающий параметрами стойкости и надежности в абсолютном или почти абсолютном смысле. В работе К. Шеннона [3] решен вопрос о существовании абсолютно стойкого шифра, обеспечивающего противодействие пассивному противнику. Современные исследования по абсолютно или почти абсолютно секретной и надежной связи развиваются в рамках так называемых SMT-протоколов (Secure Message Transmissions Protocols) и обобщают результаты К. Шеннона по нескольким важным направлениям. На основе этого возникла современная модель безопасности Долева—Яо [4], в соответствии с которой возможность противостоять противнику в канале связи переносится на сетевой граф. Кроме того, противник помимо прослушивания трафика может производить быструю подмену сообщений в определенных ветвях графа. Последнее, в частности означает, что воздействие противника приравнивается к воздействию некоторого шума в обобщенном канале связи.

(n,n)-пороговые и (k,n)-пороговые схемы разделения секретного сообщения. Основным инструментом в SMT-протоколах выступают пороговые схемы разделения секретного сообщения (секрета), работающие в конечных полях. Схема предложенная А. Шамиром, представляет собой классическую (n,n)-пороговую схему разделения секрета, позволяющую вычислять доли секрета S для любых значений n. Схема разделения секрета Шамира использует многочлены степени n–1 над полем Галуа GF_p:

$$p_{n-1}(x) = a_n x^{n-1} + \ldots + a_1 x + S \,,\; a_{n-1}, \ldots, a_1 \in \text{rand}\, GF_p \,. \qquad (1)$$

Долей секрета $Share_i(S)$ является упорядоченная пара:

$$Share_i(S) = (i, p_{n-1}(i)),\; i \neq 0 \,.$$

Теорема о полиномиальной интерполяции для многочленов (1) над полем GF_p сохраняет свою силу, поэтому при наличии не менее n совокупностей попарно различных долей секрет S восстанавливается по интерполяционной формуле Лагранжа:

$$p_{n-1}(x) = \prod_{i=1, j\neq i}^{n-1} \frac{x - x_i}{x_j - x_i},\ p_{n-1}(0) = S.$$

Можно показать, что при количестве долей секрета мощностью менее n значение S не только неопределенно, но и с равной вероятностью распределено по всему полю, так что любой элемент поля может приобрести значение S. Аналогичным образом, на основе многочленов над полем строятся (k,n)-пороговые схемы разделения секрета $k>n$. В работе [5] отмечено, что (k,n)-пороговые схемы разделения для $k=3n+1$ эквивалентны кодам Рида—Соломона, исправляющим ошибки в канале связи.

SMT-протоколы. Современные работы по SMT-протоколам обширны (см. обзоры [3, 4]). Свойства конфиденциальности SMT-протоколов с нулевой общей памятью и некоторыми дополнительными условиями на пути в канале связи, а также их криптоанализ приведены в [4].

В настоящей статье рассматривается протокол конфиденциального обмена с общей памятью между абонентами A и B. Абоненты расположены в вершинах ориентированного графа и связаны между собой, по крайней мере, $n>1$ непересекающимися путями. Такие графы называются графами высокого порядка связности. Степень активности противника в рамках модели Долева—Яо предполагается такой, что он может контролировать почти все каналы связи в режиме прослушивания и некоторую часть каналов — в режиме перехвата и быстрой замены проходящего трафика. Эти случаи различаем терминами „пассивный противник“ и „активный противник“ соответственно.

Основные определения. Пусть $G(V, R)$ — ориентированный граф, с множеством вершин V, включающим в себя элементы $\{A, B\}$ и ребра $R = \{\Gamma_1, ..., \Gamma_n, q\}$, $n>1$ такие, что:

$\Gamma_1, ..., \Gamma_n$ — ориентированы от A к B,

q — ориентирован от B к A.

Все ребра попарно не пересекаются, за исключением своих концов в A и B, и их ориентация задает в графе направление передачи трафика в сети.

Передаваемый секрет S считаем элементом числового поля GF_p (p — простое, достаточно большое число), S находится в A. Множество пересылки сообщений $D = \{d_1 ...., d_k\}$ назовем историей переписки между A и B. Это множество всех сообщений, которыми обмениваются A и B в рамках действия протокола. Случай пустого множества D не исключается.

Обозначим $\Pi(A,B,D,S)$ — протокол обмена сообщениями между A и B, в результате которого в точке B должно быть получено числовое значение $S \in GF_p$. Во время работы всего протокола Π в графе $G(V, R)$ действует k-активный противник P ($k<n$). Это означает, что P прослушивает, вообще говоря, трафик протокола в графе $G \setminus \{A, B\}$ в k каналах связи. Более точно — противник контролирует в режиме подмены сообщений не более k каналов, и это множество противник не может изменять на протяжении выполнения всего протокола.

Определение 1. Пусть $0 \le \delta < \frac{1}{2}$. Назовем протокол Π δ-надежным, если в точке B в результате выполнения протокола с вероятностью не менее $1 - \delta \left(0 \le \delta < \frac{1}{2} \right)$ появляется сообщение $S^B = S^A$.

Определение 2. Протокол П называется абсолютно надежным, если $\delta = 0$.

Следуя работе [5], введем вероятностную функцию adv, отражающую активность соперника. Более точно — функция adv(S,r) отражает количество наблюдений r противника P за выполнением протокола, необходимых для получения S=S^A вне точки B с вероятностью c.

Определение 3 (см. [5]). Пусть $0 \le \varepsilon < 1$. Назовем протокол П ε-секретным, если для любых двух сообщений S_0, S_1 и для любого r:

$$\sum_c \left| \left[\text{adv}(S_0, r) = c\right] - \left[\text{adv}(S_1, r) = c\right] \right| \le 2\varepsilon .$$

Определение 4. Протокол П назовем абсолютно секретным, если он 0-секретен в смысле определения 3.

Определение 5. Назовем протокол $\Pi(\delta, \varepsilon)$-безопасным, если он δ-надежен и ε-секретен. Протокол П(0,0) называем совершенным.

В протоколе П(A,B,S,D,P) выделим три этапа. Первый предназначен для создания проверяемого и согласованного непустого множества D в точках A и B, а также определения тех элементов сети, которые контролируются противником P. Основным инструментом первого элемента для создания D является проверяемая схема разделения секрета Шамира [6].

В результате выполнения второго этапа на основе множества D в точке A решается задача „укладка рюкзака“ с некоторым модулярным слагаемым в поле GF_p, и необходимый набор битов (обозначим его E) для сборки решения пересылается в точку B.

На завершающем протокол третьем этапе модулярное слагаемое Δ передается в точку B. В силу того что величины Δ и S независимы, справедливо следующие равенство:

$$H(\Delta \mid S) = H(S), \qquad (2)$$

где $H(x \mid y)$ — условная энтропия по Шеннону.

Описание SMT-протокола с общей памятью

Этап I. Формирование истории переписки D и передача ее абоненту B.

В начале выполнения протокола у абонентов A и B множество переписки — пустое. Абонент A формирует случайным образом множество $D = \{d_1, ..., d_k\}$, где $d_i \in GF_p$. Для передачи $d_i \in GF_p$, $i = 1, ..., k$, используем проверяемое разделение секрета Шамира [6] порядка $(k+1, n)$ на доли d_{ij}, где $j = 1, ..., n$ — номер провода, по которому отправлена доля d_{ij} из Γ. Абонент B получает доли d_{ij} и при помощи проверяемой интерполяции пытается вычислить $d'_i = d_i$. Провода с номерами j, для которых интерполяция проведена неуспешно, признаются ошибочными или контролируемыми активным противником и в дальнейшей работе протокола не участвуют. Список ошибочных проводов абонент B отправляет по каналу обратной связи q абоненту A. Этот этап соответствует первому этапу SMT(0,0)-протокола, описанному и изученному в работе [6], за тем исключением, что в [6] история переписки D после выполнения этапа I отбрасывается.

Этап II. Выбор абонентом A коэффициентов „рюкзачной схемы“ и передача их абоненту B. Отправитель A выбирает коэффициенты $e_1, ..., e_k$, где $e_i = \{0,1\}$, такие что:

$$\sum_{i=1}^{k} d_i e_i = S + \Delta . \qquad (3).$$

Здесь операция сложения по mod p, Δ — некоторый элемент из GF_p, подчиненный свойству (2). Набор битов $e_1, ..., e_k$ передается абоненту B.

Этап III. Сборка секрета абонентом B. Абонент B получает коэффициенты $e_1,...,e_k$, вычисляет значение $S+\Delta$ и передает его абоненту A по обратному каналу q. После получения сообщения от B абонент A отправляет Δ любым способом по достоверным каналам. Абонент B получает Δ и вычисляет секретное сообщение S. На этом заканчивается выполнение протокола П.

Теорема: Пусть противник P является k-активным ($k<n$), при этом не имеет доступа к обратному каналу связи q. Тогда условие

$$k < 2n+1 \tag{4}$$

необходимо для того, чтобы протокол $\Pi(A,B,D,S,P)$ был (0,0)-безопасным.

Доказательство: Представим действие протокола $\Pi(A,B,D,S,P)$ в виде композиций протоколов $\Pi(A,B,D,S,P)=\Pi_1\circ\Pi_2\circ\Pi_3(A,B,D,S,P)$, где i=1,..,3 соответствует этапу протокола П. Свойство идеальности протокола Π_1 хорошо известно [7]. Отсюда следует, что противник P может восстановить или угадать элементы множества D с вероятностью $1/|GF_p|$, где $|GF_p|$ — мощность числового поля. Если трафик прослушивается $E=\{e_1,...,e_k\}$, то $H(E\mid D)=H(D)$. Последнее равенство доказывает совершенность протокола Π_2. Свойство совершенности протокола Π_3 вытекает из (3), что завершает доказательство теоремы.

Нетрудно показать, что однократное применение схемы разделения секрета Шамира эквивалентно применению n шифров Вернама по каждому из путей $R=\{\Gamma_1,...,\Gamma_n\}$ с попарно различными ключами, определяемыми по значениям многочлена $p_n(x_j)-S$ в схеме разделения секрета. Из этого, с учетом абсолютной стойкости однократного шифрования Вернама [3], следует 0-секретность по Шеннону протокола Π_1, его композиций, а следовательно, и всего протокола $\Pi(A,B,D,S,P)=\Pi_1\circ\Pi_2\circ\Pi_3(A,B,D,S,P)$.

Ограничение на доступ противника P к обратному каналу q в теореме является необходимым. Криптоанализ протокола Π_1 [8] показывает, что в случае активного доступа противника к обратному каналу q успешно проводится криптографическая атака „человек посередине“ (“Man in the middle”). Этот факт, вообще говоря, приводит к понижению стойкости протокола Π_1, а следовательно и $\Pi(A,B,D,S,P)$, до $(0,\varepsilon)$-безопасного, где ε удовлетворяет неравенству $\frac{1}{p}<\varepsilon<\frac{5}{p}$.

СПИСОК ЛИТЕРАТУРЫ

1. *Панасенко С.* Алгоритмы шифрования. СПб: БХВ, 2008. 563 с.
2. *Черемушкин А. В.* Криптографические протоколы: основные свойства и уязвимости. М.: Изд. центр Академия, 2009. 272 с.
3. *Shannon C.* Communication theory of secrecy systems // Bell System Techn. J. 1949. Vol. 28, N 4. P. 656—715.
4. *Dolev D. D., Yao A.* // IEEE Transact. on Inform. Theory. 1983. Vol. IT-29, N 2. P. 198—208.
5. *Franklin M., Wright R.* Secure communication in minimal connectivity models // J. Cryptology. 2000. Vol. 13, N 1. P. 9—30.
6. *Shamir A.* How to share a secret // Communication of ACM. 1979. Vol. 22, N 11. P. 612—613.
7. *Dolev D., Dwork C.* Perfectly Secure Message Transmission // Proc. 31st Annu. Symp. on Found. of Comput. Sci. 1990. P. 36—45.
8. *Yang Q., Desmedt Y.* Cryptanalysis of Secure Message Transmission Protocols with Feedback // ICITS. 2009. P. 159—176.

Сведения об авторе

Алексей Викторович Александров — канд. физ.-мат. наук, доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: alex_izi@mail.ru

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.

УДК 519.6

М. В. Белоусов, А. В. Александров

ОСОБЕННОСТИ РЕАЛИЗАЦИИ SMT-ПРОТОКОЛА НА БАЗЕ ЯЗЫКА PYTHON 3

Описана реализация SMT-протокола на основе схемы разделения секретного сообщения Шамира, исследованы характеристики протокола, такие как алгоритмическая сложность, скорость работы и надежность.

Ключевые слова: *SMT-протокол, схема разделения секрета, модель Долева—Яо.*

Рассмотрим реализацию SMT-протокола (Secure Message Transmission), принадлежащего к группе 0-секретных протоколов передачи сообщений [1], в обобщенном канале связи.

Под обобщенным каналом связи понимается ориентированный граф с множеством вершин и путей (каналов), таких что:

1) все пути C_i $(i = 1, ..., n)$ попарно не пересекаются, за исключением оконечных точек A и B, задающих направление передачи данных в канале связи;

2) $\Pi(A, B, C, S)$ — протокол обмена сообщениями между вершинами A и B. В рамках протокола секретное сообщение (секрет) S должен быть передан в точку B по обобщенному каналу $C = \{C_1, ..., C_n\}$.

3) секрет S является элементом числового поля GF_p (p—большое простое число), изначально находящимся в точке A;

4) подчиненный модели безопасности Долева—Яо [2] протокол предусматривает противодействие противника на протяжении всей работы.

В классических вариациях SMT-протокола всегда можно выделить два этапа: разделение сообщения S на криптографические части — тени $Share_1(S)$, ..., $Share_n(S)$ с отправкой $Share_i(S)$ по каналам C_i, и сборка сообщения S из необходимого набора теней в другой точке сетевого графа.

Свойства конфиденциальности SMT-протоколов изучены в работах [1, 3, 4] для различных реализаций схем разделения и сборки секрета из теней. В частности, в статье [1] вводится понятие надежности. Надежность работы протокола $\Pi(A, B, C, S)$ определяется вероятностью P того, что по окончании работы протокола переданное и полученное сообщения одинаковы:

$$S^A = S^B, \quad P \sim 1. \tag{1}$$

В работе [4] для контроля надежности $\Pi(A, B, C, S)$ предлагается дополнительно использовать обратный канал связи (feedback).

В рамках нашей реализации протокола схема разделения секрета представляет собой классическую (n,n)-пороговую схему, позволяющую вычислять теневые копии для больших

значений n. Схема разделения секрета Шамира использует многочлены степени n–1 над полем GF_p [5]:

$$p_{n-1}(x) = a_{n-1}x^{n-1} + ... + a_1 x + a_0, \;\; a_0 = S, \tag{2}$$

$$a_{n-1}a_1 \in \text{rand}GF_p; \;\; x \in GF_p.$$

Долей секрета $Share_i(S)$ является упорядоченная пара:

$$Share_i(S) = (i, p_{n-1}(i)), \;\; i \neq 0.$$

Теорема о полиномиальной интерполяции для многочленов (2) над полем GF_p сохраняет свою силу, поэтому при наличии совокупности попарно различных теней мощности n секрет S восстанавливается по интерполяционной формуле Лагранжа:

$$p_n(x) = \prod_{i=1, j\neq i}^{n-1} \frac{x - x_i}{x_i - x_i}.$$

Обратимся к деталям реализации протокола $\Pi(A, B, C, S)$ на базе языка Python.

Для генерации и хранения теней секрета применяется тип dictionary, позволяющий использовать индексы на всем диапазоне bigint. Это позволяет фактически ограничивать количество генерируемых теней лишь объемом оперативной памяти [6] и достигать n~500 при приемлемых значениях времени работы протокола.

В протоколе используются основные математические операции над полем GF_p, реализованные в рамках языка Python, такие как сложение, умножение Карацубы и быстрое возведение в степень. Анализ быстродействия данных операций на числах различной длины позволил определить оптимальные по скорости выполнения реализации. Для качественной генерации случайных коэффициентов в выражении (2) использован алгоритм Mersenne twister (MT19937), его период равен 2^{19937}–1. Алгоритм обладает достаточно высокими показателями времени генерации, например, время генерации a_i $(i = n-1, ..., 1)$ в (2) относительно линейных конгруэнтных генераторов меньше приблизительно в 2—2,5 раза.

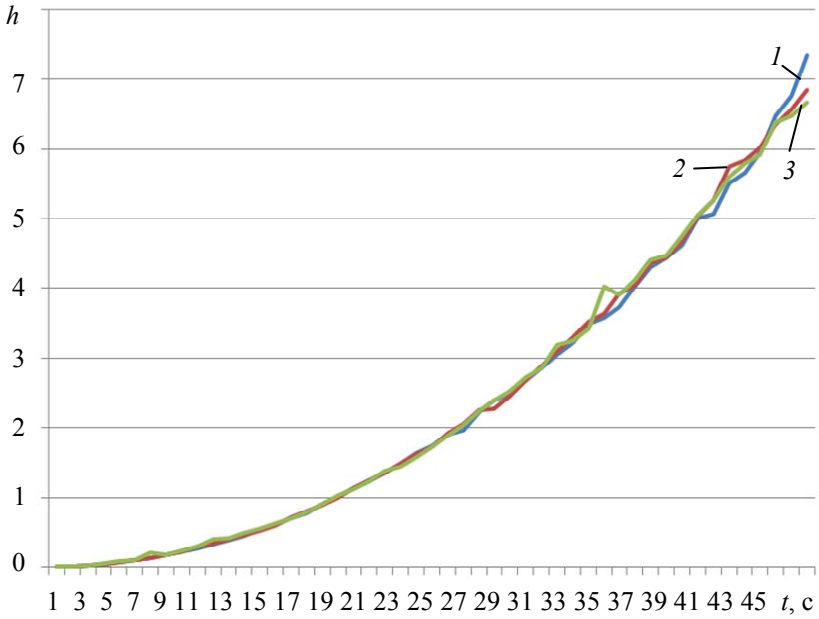
Функциональность реализованного базового SMT-протокола фактически ограничена предоставленными ресурсами оперативной памяти для хранения теней и элементов поля GF_p в процессе вычислений, а также вычислительными ресурсами процессора.

Поскольку основная часть протокола сводится к операциям разделения и сборки секретного сообщения, основные показатели быстродействия алгоритма в целом зависят от этих операций. Теоретические оценки вычислительной сложности операций разделения и сборки в нашем случае — $O(\log_2 n)$ и $O(n^2)$ соответственно.

Рассмотрим надежность работы протокола. Введение обратного канала для контроля надежности может существенно понижать конфиденциальные свойства протокола [4]. Поэтому нами предложено использовать хеш-функции как для контроля целостности теней секрета, так и для контроля сборки значения S в точке B. В частности, протокол $\Pi(A, B, C, S)$ завершает свою работу пересылкой значения хеш-функции секрета $h(S)$ по всем доступным каналам C_i либо пересылкой значений секрета и тени S+$Share_i$ по соответствующим каналам передачи теней C_i. При этом, очевидно, вероятность P в (1) зависит от криптографических свойств применяемой хеш-функции:

$$P\left[\left(h(S^A) = h(S^B)\right) \rightarrow \left(S^A = S^B\right)\right] = 1 - P(h).$$

В правой части равенства $P(h)$ — вероятность появления коллизии для выбранной криптографической хеш-функции $h(S)$.



Для вариации протокола получены значения времени (см. рисунок, кривая *1*; кривая *2* — $h(S_i)$, *3* — $h(S)$) и алгоритмической сложности сборки секрета в зависимости от значения n, соответствующие указанным выше теоретическим оценкам, представленны на рисунке.

СПИСОК ЛИТЕРАТУРЫ

1. *Dolev D., Dwork C.* Perfectly Secure Message Transmission // Proc. 31st Annu. Symp. on Found. of Comput. Sci. 1990. P. 36—45.

2. *Dolev D., Yao A.* On the Security of Public Key Protocols // IEEE Transact. on Inform. Theory. 1983. Vol. 29, N 2. P. 198—208.

3. *Kurosawa K.* General Error Decodable Secret Sharing Scheme and Its Application. Cryptology ePrint Archive Report/ 2009. P. 263.

4. *Yang Q., Desmedt Y.* Cryptanalysis of Secure Message Transmission Protocols with Feedback // ICITS. 2009. P. 159—176.

5. *Shamir A.* How to share a secret // Communication of ACM. 1979. Vol. 22, N 11. P. 612—613.

6. Python Core Development [Электронный ресурс]: <http://www.python.org/dev/peps/pep-0237/>.

Сведения об авторах

Максим Васильевич Белоусов — аспирант; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: lib.bmw@gmail.com

Алексей Викторович Александров — канд. физ.-мат. наук, доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: alex_izi@mail.ru

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.

SUMMARY

P. 7—11.

RESEARCH INTO POSSIBILITIES OF DIGITAL RADIO STATION CREATION ON THE BASIS OF COHERENT RECEPTION OF GMSK-SIGNALS

An investigation on noise immunity of digital demodulator with bearing and clock frequencies tuning out is performed with the use of ADS. A prototype of radio station for the VHF range is developed, and possibilities of its application as a part of radio communication system equipment operated in frequency slot pitch of 6,25 or 3,125 kHz are tested experimentally.

Keywords: VHF radio station, GMSK, narrow-band reception, coherent demodulator.

Data on authors

Alexander S. Merkutov — Cand. Techn. Sci.; Vladimir State University, Department of Computer Engineering; E-mail: merkutov@yandex.ru

Denis V. Krutin — Vladimir State University, Department of Computer Engineering; Engineer; E-mail: krutin.denis@gmail.com

Andrey N. Tsyslav — Vladimir State University, Department of Computer Engineering; Scientist; E-mail: cislav@yandex.ru

Alexander A. Pletnev — Vladimir State University, Department of Computer Engineering; Scientist; E-mail: Alexandr.Pletnerv@gmail.com

P. 12—15.

METHODS OF EVALUATION OF THE COMMUNICATION LINK QUALITY. WCDMA TECHNOLOGY

The problem of monitoring of exchange service station capacity of cellular system using code channel separation on the base of signal-to-noise ratio assessment is considered. Methods for signal-to-noise ratio determination with the use of WCDMA technology are proposed.

Keywords: WCDMA, code channel separation, signal-to-noise ratio.

Data on authors

Denis V. Krutin — Vladimir State University, Department of Computer Engineering; Engineer; E-mail: krutin.denis@gmail.com

Maxim A. Kislyakov — Vladimir State University, Department of Computer Engineering; Junior Scientist; E-mail: kislyakov.maxim@gmail.com

Sergey G. Mosin — Cand. Techn. Sci.; Vladimir State University, Department of Computer Engineering; E-mail: smosin@vlsu.ru

P. 15—19.

DESIGN OF WIRELESS SENSOR NETWORKS

Theoretical problems in wireless sensor networks design are considered. Separate stages of the design route are described. The networks classification of as topological structures is presented.

Keywords: wireless sensor network, design route, static topology.

Data on author

Maxim A. Kislyakov — Vladimir State University, Department of Computer Engineering; Junior Scientist; E-mail: kislyakov.maxim@gmail.com

Sergey G. Mosin — Cand. Techn. Sci.; Vladimir State University, Department of Computer Engineering; E-mail: smosin@vlsu.ru

Veronika V. Savenkova — Vladimir State University, Department of Computer Engineering; Engineer; E-mail: savenkova.nika@gmail.com

P. 19—23.

METHODOLOGY OF TEST-ORIENTED DESIGN OF MIXED-SIGNAL CIRCUITS

Methodology of test-oriented design of mixed-signal circuits where parallel design procedures are executed at multicores or multiprocessors computer systems is proposed. The choice between methods of in-circuit and external testing is provided.

Keywords: design-for-testability, in-circuit testing, mixed-signal integrated circuits, design automation, parallelism.

Data on author

Sergey G. Mosin — Cand. Techn. Sci.; Vladimir State University, Department of Computer Engineering; E-mail: smosin@vlsu.ru

P. 24—28.

A DISTRIBUTED MECHANISM OF OVERLOADS MANAGEMENT IN DATA COMMUNICATION NETWORKS

An analysis of equilibrium states of the TCP traffic control system is presented. A new method of congestion control in TCP/IP networks is proposed. Distinguishing features of the method are incorporation of slow adaptation algorithms and allowing for selective packet removal.

Keywords: TCP/IP, computer network, congestion, AQM, control.

Data on author

Yury M. Monakhov — Cand. Techn. Sci.; Vladimir State University, Department of Informatics and Information Security; E-mail: unclefck@gmail.com

P. 28—32.

ON ORGANIZATION OF DISTRIBUTED INFORMATION ENVIRONMENT FOR INTEGRATED PROTECTION AND SAFETY SYSTEMS

Evaluation criteria and methods of organization of information exchange in a distributed information environment of integrated protection and safety systems by various manufacturers are presented.

Keywords: integrated security systems, SCADA systems.

Data on authors

Andrey V. Telniy — Cand. Techn. Sci.; Vladimir State University, Department of Informatics and Information Security; E-mail: andre.izi@mail.ru

Oleg R. Nikitin — Dr. Techn. Sci., Professor; Vladimir State University, Department of Informatics and Information Security; E-mail: olnikitin@mail.ru

Igor V. Khrapov — Cand. Techn. Sci.; Tambov State Technical University, Analytical Center for Economic Development; Director; E-mail: igor@tambov.ru

P. 33—35.

ANALYSIS OF WIRELESS CHANNELS QUALITY IN DISTRIBUTED TELECOMMUNICATION DATA TRANSFER ENVIRONMENT IN DENSELY BUILT-UP CITY AREA

An experimental study of quality of data transfer link organized with the use of wireless communication technologies between a mobile vehicle moving around the city and a central office is carrier out. An analysis of the results is presented.

Keywords: wireless link of communication, mobile vehicle, UMTS/HSDPA, GSM/GPRS/EDGE.

Data on authors

Aleksey V. Goryachev — Post-Graduate Student; Vladimir State University, Department of Informatics and Information Security; E-mail: a.goryachev@rfc-cfa.ru

Mikhail Yu. Monakhov — Dr. Techn. Sci., Professor; Vladimir State University, Department of Informatics and Information Security; Head of the Department; E-mail: mmonakhov@vlsu.ru

P. 35—39.

INVENTORY OF INFORMATION RESOURCES AS A BASIS FOR SAFE OPERATION OF AUTOMATIC CONTROL SYSTEM

A universal list of information resources of automatic control system (ACS) is compiled on the basis of a resource involvement into information processing. The critical characteristics of information resources are determined from the standpoint of safe operation of the ACS. A method of information resources inventory is proposed, peculiarities of the method application are analyzed.

Keywords: inventory, information resources, business-processes, information security.

Data on authors

Mikhail Yu. Monakhov — Dr. Techn. Sci., Professor; Vladimir State University, Department of Informatics and Information Security; Head of the Department; E-mail: mmonakhov@vlsu.ru

Olga I. Fayman — Vladimir State University, Department of Informatics and Information Security; Assistant; E-mail: Olich06@inbox.ru

P. 39—43.

A MODEL FOR ASSESSMENT OF FACTORS OF INFORMATION RELIABILITY CHANGE IN CORPORATE DATA COMMUNICATION NETWORKS

The problem of reliability of information resources in corporate data communication networks is considered. Dependence of the information reliability on a row of difficult to formalize characteristics and factors is determined. A model for reliability assessment of information resource and prediction of its changes is proposed.

Keywords: reliability of data, information resource, corporate data communication networks, destabilizing factor, expert assessment.

Data on authors

Dmitry A. Polyansky — Cand. Techn. Sci.; Vladimir State University, Department of Informatics and Information Security; E-mail: polyansk@rambler.ru

Mikhail Yu. Monakhov — Dr. Techn. Sci., Professor; Vladimir State University, Department of Informatics and Information Security; Head of the Department; E-mail: mmonakhov@vlsu.ru

P. 43—45.

A TOOLSET FOR PROVIDING INFORMATION AUTHENTICITY IN CORPORATE NETWORKS SUPPORTING DATA COMMUNICATION IN AUTOMATIC CONTROL SYSTEMS

A structure and composition of a set of tools for providing authenticity of the data circulating in corporate networks are examined. The features and peculiarities of the toolset using are analyzed.

Keywords: authenticity of data, informative resource, corporate networks, destabilizing factor, expert estimation.

Data on authors

Dmitry A. Polyansky — Cand. Techn. Sci.; Vladimir State University, Department of Informatics and Information Security; E-mail: polyansk@rambler.ru

Olga I. Fayman — Vladimir State University, Department of Informatics and Information Security; Assistant; E-mail: Olich06@inbox.ru

Svetlana Yu. Kirillova — Cand. Techn. Sci.; Vladimir State University, Department of Information Systems and Information Management; Head of the Department; E-mail: sv-kir@mail.ru

P. 46—49.

ON AUTOMATION OF PROCESSES PROVIDING FUNCTIONAL STABILITY OF INFORMATION-TECHNOLOGICAL INFRASTRUCTURE OF AN ENTERPRISE RESOURCE PLANNING SYSTEM

Proposed are tools for automation of processes of administration of information-technological infrastructure of an enterprise resource planning (ERP) system used in search and recovery tasks caused by destructive actions on its components

Keywords: administration of a corporate data networks, automated administration system, administrator.

Data on authors

Denis V. Mishin — Post-Graduate Student; Vladimir State University, Department of Informatics and Information Security; E-mail: mishin.izi@gmail.com

Mikhail Yu. Monakhov — Dr. Techn. Sci., Professor; Vladimir State University, Department of Informatics and Information Security; Head of the Department; E-mail: mmonakhov@vlsu.ru

P. 50—52.

SYSTEM OF ADMINISTRATION OF CORPORATE DATA TRANSMISSION NETWORK SERVING AN AUTOMATIC CONTROL SYSTEM OF INDUSTRIAL ENTERPRISE

A model of automated control system of corporate area network is presented. The mechanisms of the system efficiency improvement and the problems of its integration into automated control system of industrial enterprise are analyzed.

Keywords: administration of corporate networks, automatic control system of industrial enterprise, administrator.

Data on authors

Denis V. Mishin — Post-Graduate Student; Vladimir State University, Department of Informatics and Information Security; E-mail: mishin.izi@gmail.com

Maria M. Monakhova — Vladimir State University, Department of Informatics and Information Security; Engineer; E-mail: monakhova_mariya@bk.ru

Arkady A. Petrov — Post-Graduate Student; Vladimir State University, Department of Informatics and Information Security; E-mail: petrov@avo.ru

P. 53—56.

INCREASE IN PRODUCTIVITY OF CORPORATE NETWORKS SUBJECTED TO INFORMATION SECURITY THREAT

The problem of increase in productivity of corporate networks experiencing information security threats is formulated as a task of building of a protection system ensuring maximum possible efficiency at guaranteed detection and effective counteraction to the information security threats.

Keywords: corporate data communication networks, productivity, information protection system, threat to information security.

Data on authors

Ludmila M. Gruzdeva — Cand. Techn. Sci.; Vladimir State University, Department of Informatics and Information Security; E-mail: glm@vlsu.ru

Mikhail Yu. Monakhov — Dr. Techn. Sci., Professor; Vladimir State University, Department of Informatics and Information Security; Head of the Department; E-mail: mmonakhov@vlsu.ru

P. 57—59.

EXPERIMENTAL STUDY OF CORPORATE TELECOMMUNICATION NETWORK WITH ADAPTIVE INFORMATION SECURITY SYSTEM

Analysis of experimental studies of productivity of a corporate data communication network under operation of information protection system which quickly changes its parameters in response to information attacks is presented.

Keywords: telecommunication network, productivity, system of information protection, information attacks.

Data on authors

Ludmila M. Gruzdeva — Cand. Techn. Sci.; Vladimir State University, Department of Informatics and Information Security; E-mail: glm@vlsu.ru

Konstantin G. Abramov — Post-Graduate Student; Vladimir State University, Department of Informatics and Information Security; E-mail: abramovk@vlsu.ru

Yury M. Monakhov — Cand. Techn. Sci.; Vladimir State University, Department of Informatics and Information Security; E-mail: unclefck@gmail.com

P. 60—64.

STABILITY OF SMT-PROTOCOL TOWARDS ENEMY ATTACK IN DOLEV—YAO SAFETY MODEL

Confidentiality properties of Secure Message Transmission (SMT) protocols with shared memory are determined. The confidentiality is understood as stability of the transmission protocol towards active and passive enemy attacks in a generalized communication channel described by the Dolev—Yao model.

Keywords: cryptographic protocols, privacy, secret sharing schemes, Dolev—Yao security model.

Data on author

Aleksey V. Aleksandrov — Cand. Techn. Sci.; Vladimir State University, Department of Informatics and Information Security; E-mail: alex_izi@mail.ru

P. 64—66.

FEATURES OF THE SMT-PROTOCOL IMPLEMENTATION BASED ON PYTHON 3

Implementation of the SMT-protocol on the base of Shamir secret sharing scheme is described. Several characteristics of the protocol, such as algorithmic complexity, speed, and safety are studied.

Keywords: SMT-protocol, secret division diagram, Dolev—Yao model.

Data on authors

Maxim V. Belousov — Student; Vladimir State University, Department of Informatics and Information Security; E-mail: lib.bmw@gmail.com

Aleksey V. Aleksandrov — Cand. Techn. Sci.; Vladimir State University, Department of Informatics and Information Security; E-mail: alex_izi@mail.ru