УДК 621.398
ББК 32.965.7
С 37

Симанков В.С.
Доктор технических наук, профессор, директор института информационных технологий и безопасности университетского комплекса Кубанского государственного технологического университета, Краснодар, тел. (861) 275-11-10, e-mail: vs@simankov.ru
Колодий А.С.
Аспирант кафедры компьютерных технологий и информационной безопасности Кубанского государственного технологического университета, Краснодар, e-mail: admin@comp-info.ru

Подход к построению архитектуры интеллектуальной системы обнаружения и устранения сетевых аномалий

(Рецензирована)

Аннотация
Специфика аномалий в современных распределенных сетях делает необходимым применение в системах обнаружения и противодействия как формальных, так и эвристических, адаптивных методов и алгоритмов. Использование методологии ситуационного моделирования и управления позволяет повысить уровень формализации процедур принятия решений за счет классификации возникающих ситуаций и выбора способов их обработки на основе экспертных знаний и применения формальных методов.
Ключевые слова: *сетевые аномалии, ситуационное моделирование, адаптивное управление, выявление аномалий, функциональная модель, классификация и кластеризация.*

Simankov V.S.
Doctor of Technical Sciences, Professor, Director of Institute of Information Technologies and Safety of University Complex, Kuban State University of Technology, Krasnodar, ph. (861) 275-11-10, e-mail: vs@simankov.ru
Kolodiy A.S.
Post-graduate student of Department of Computer Technologies and Information Security, Kuban State University of Technology, Krasnodar, e-mail: admin@comp-info.ru

Approach to creation of intellectual system architecture for detection and elimination of net anomalies

Abstract
Specifics of anomalies in the modern distributed nets requires application of both formal and heuristic adaptive methods and algorithms in detection and counteraction systems. Use of methodology of situational modeling and management allows us to raise level of formalization of decision making procedures at the expense of classification of arising situations and choice of ways of their processing on the basis of expert knowledge and application of formal methods.
Keywords*: network anomalies, situational modeling, adaptive management, detection of anomalies, functional model, classification and clustering.*

Проблема выявления аномалий в современных распределенных, гетерогенных сетях требует для своего решения целого комплекса мер, организационных, технических и программных, а также разработки соответствующего алгоритмического обеспечения. В настоящее время на рынке представлен ряд решений и продуктов, позволяющих реализовать необходимый функционал алгоритмического, математического и программного обеспечения [1-3].

Природа сетевых аномалий (СА), их разнообразие и характеристические признаки подробно изучены и классифицированы как отечественными, так и зарубежными исследователями. Однако до сих пор при разработке стандартов, практик и рекомендаций по управлению и обеспечению эффективности функционирования сетей недостаточное внимание уделяется принципам, алгоритмам и единым методологическим основам по-

строения архитектуры системы обнаружения и противодействия СА (особо отметим стандарты сетевой безопасности CISCO и линейку архитектур, начиная с CISCO NGN, где эти вопросы вообще начали рассматриваться с практической точки зрения).

Определим, что в качестве составных элементов разрабатываемая архитектура должна включать:

– способы обработки исходных данных (наблюдений) – т.е. принципы организации и функционирования подсистем сетевого мониторинга – для разработки адекватных математических моделей и эффективной алгоритмизации;

– методику выбора информативных показателей, характеризующих состояние сети;

– методику оценки состояния сети и аналитической обработки результатов ее мониторинга;

– модели оценки состояния, обнаружения и классификации выявляемых аномалий;

– методику адаптивного управления и принятия решений по устранению выявленных аномалий;

– модели и методы оценки эффективности предложенных решений.

Указанные методики и модели должны охватывать все этапы проектирования, развертывания и поддержания функционирования сетей с учетом их архитектуры, режимов работы и используемых видов обеспечения.

Предлагаемый подход основывается на методологии ситуационного моделирования и управления, что позволяет повысить уровень формализации процедур принятия решений за счет классификации возникающих ситуаций и выбора способов их обработки на основе экспертных знаний и применения формальных методов. Применение алгоритмических и математических моделей в системе ситуационного управления повышает точность распознавания текущих ситуаций в сети, оценки времени на их обработку в соответствии с нормативными данными по выполнению операций, формирование решений по выполнению нового технологического цикла работ на основе базы знаний.

Возможность использования в автоматизированной системе как формальных, так и эвристических, адаптивных методов и алгоритмов обнаружения создает предпосылки для повышения точности принимаемых решений в текущих ситуациях, что способствует снижению непроизводственных затрат на выполнение последующих циклов работ [4].

Для формального описания системы управления сетью используем кортеж, описывающий подсистему, характеризующую сеть как объект управления [5] (рис. 1):

$$S = \{I_t,\ I_m,\ I_c,\ I_x\}, \quad Z;\ K;\ W;\ R;\ U > \tag{1}$$

где I_t – массив используемой технологической (протоколы, технологии) информации о сети,

I_m – управленческая информация, набор сетевых политик;

I_c – коммуникационная (топология, инфраструктура) информации;

I_x – информация о внешних и управляющих воздействиях;

Z – формальное описание целей управления;

K – набор характеристик информационных ресурсов сети;

W – возмущающие воздействия (внешние);

R – множество отношений между элементами сети (схемы и реализации политик);

U – управляющие воздействия.

Особенности архитектуры и режимов функционирования современных сетей (гетерогенность, распределенность и т.д.) обуславливают необходимость использования в системе обнаружения и устранения аномалий ряда математических моделей [1, 3, 6], позволяющих учесть имеющиеся неопределенности и неточности знаний относительно предполагаемых аномалий.

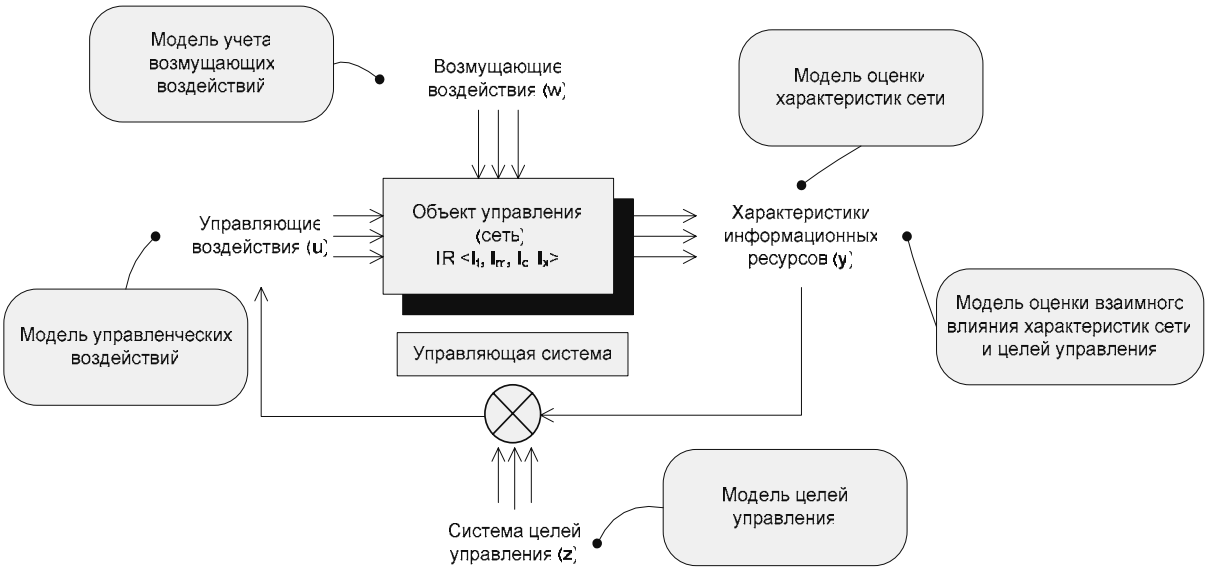

Рис. 1. Общая схема системы обнаружения и выявления аномалий в сети

Высокую неоднородность информационных ресурсов сети также необходимо учитывать при выборе используемых в системе управления математических моделей, которые должны иметь универсальный характер, не зависящий от конкретных особенностей того или иного вида данных ресурсов.

При разработке математического и алгоритмического обеспечений такой системы обнаружения следует обращать внимание на следующие архитектурные особенности программно-аппаратной реализации решения в условиях разнородной и территориально распределенной сети:

– множество источников и большой объем данных по мониторингу;

– используются программируемые математические модели для оценки текущей ситуации, прогнозирования ее развития с учетом сделанных предположений, анализа «что, если…» (такой функционал, например, представляет платформа CISCO MARS и архитектуры TRUST SEC);

– информация по мониторингу часто представляется в агрегированном виде, но необходимо иметь возможность детализации до требуемого уровня – т.е. знать о том, из каких источников и на основе каких преобразований она получена;

– большой объем подготовительной работы с анализом всех доступных данных и моделированием ситуаций.

Система ситуационного управления обнаружения аномалий сети строится на основе набора математических моделей. Все множество ситуаций разбивается на иерархически вложенное множество классов ситуаций. Структура классификатора ситуаций соответствует уровням полномочий по принятию решений в структуре сети. Таким образом, например, для определенных ситуаций состояния сети возможна их обобщенно-признаковая классификация: «нормальные», «критические», «аварийные» [1, 2].

В ситуациях класса «нормальные» управляющее воздействие определяется в соответствии с принятой схемой управления, являющейся неотъемлемой частью проектных данных сети. За реализацию управляющего воздействия в таком режиме отвечает контур программного управления.

В ситуациях класса «критические» и «аварийные» управляющее воздействие интерактивно определяется системным администратором сети или администратором безопасности [7]. Для этого нештатная ситуация должна быть отнесена к определенно-

му классу ситуаций, проанализированы рекомендации, при необходимости проведен сбор дополнительной информации и на основе полученных данных принята схема управляющего воздействия.

Для выбора управляющего воздействия целесообразно использование формируемой и подключаемой базы знаний прецедентов, для оценки допустимости воздействия используется его экстраполяция на последующие фазы в соответствии с математической моделью объекта и проверкой соответствия системе ограничений. Эта процедура позволяет снизить количество неэффективных решений, выявляемых на заключительных этапах.

Разрабатываемая автоматизированная система обнаружения аномалий представляет собой интерактивный человеко-машинный программный комплекс, исходными моделями которого являются математические, структурно-функциональные, имитационные и иные модели сети. Свойства формальной ситуационной модели определяются функциональными свойствами механизмов преобразования в формальные математические модели [8] (рис. 2).

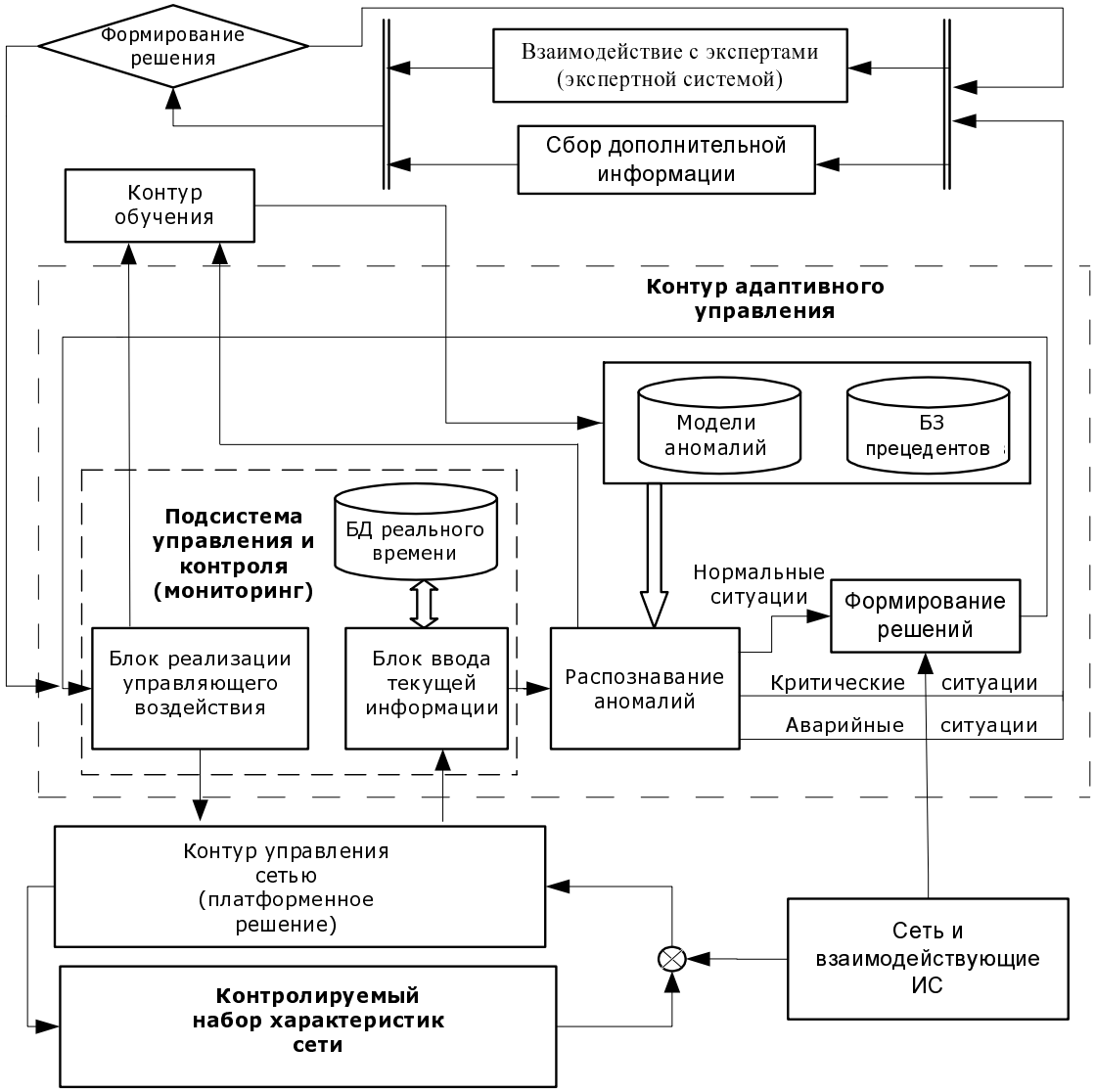

Рис. 2. Функциональная модель обнаружения аномалий
на множестве классификационных признаков

Реализация предлагаемых подходов к обнаружению и противодействию сетевым аномалиям подразумевает включение в состав системы баз данных и знаний, содержащих как характеристические описания прецедентов (аналог сигнатур), так и БД моделей и мониторинга состояния сети. Таким образом, контур адаптивного ситуационного управления на основе результатов мониторинга состояния сети в режиме реального времени определяет (формирует) и реализует механизмы и решения эффективного противодействия.

Как мы видим, в комплексе значительная роль отведена взаимодействию с экспертами (лицами, принимающими решения) о тех или иных мероприятиях и управляющих воздействиях в тех случаях, когда это невозможно или нецелесообразно автоматизировать.

Целесообразным представляется использование методики формализации на основе вероятностного подхода, повышающая надежность и достоверность результатов математического моделирования [8]. Учитывая модель (1) формального описания системы управления сетью, запишем интегральный показатель оценки эффективности обнаружения аномалии следующим образом:

$$J = F_1(x, y, w, u), \tag{2}$$

где $x = (x_1, x_2, ..., x_m)$ – совокупность входных параметров, $x \in X$;

$y = (y_1, y_2, ..., y_n)$ – совокупность выходных параметров, $y \in Y$;

$w = (w_1, w_2, ..., w_k)$ – совокупность неконтролируемых внешних воздействий, $w \in W$;

$u = (u_1, u_2, ..., u_l)$ – совокупность управляющих воздействий, $u \in U$.

Задача выбора закона управления для противодействия обнаруженной и классифицированной аномалии заключается в определении $u = F_2(x, y, w)$, приводящего при существующих значениях $x \in X$, $y \in Y$, $w \in W$ к оптимальному значению J. При этом состояние сети (т.е. характеристика предполагаемой аномалии) характеризуется совокупностью контролируемых параметров x, где X – область возможных значений вектора x.

На этапе практической реализации (алгоритмизации) в сети математической модели закона управления модель интегрируется в сетевую политику (например, противодействия аномалиям) путем введения $P = (p_1, p_2, ..., p_N)$ – конечной совокупностью меток, индексирующих множество возможных методов противодействия.

В предлагаемом подходе к обнаружению аномалий режимы работы сети $\{u_k\}$, характеристики решаемых задач $\{x_j\}$ и выходные параметры, результаты $\{y_i\}$ могут быть описаны нечеткими переменными на множествах U, X, Y. Необходимо выбрать управление $u' \subset F(U)$, которое переводит процесс из заданного состояния $x' = \{x_j'\} \subset F(X_j)$ в состояние, соответствующее требуемому выходному показателю y'.

При выборе стратегии противодействия аномалиям мы остановились на принципе ситуационного управления, который сводится к формированию однородных классов состояний (т.е. классов аномалий), требующих одного и того же метода противодействия. Таким образом, предлагаемая методика обнаружения и противодействия аномалиям в ходе своей практической реализации в рамках распределенной сети строится на двух группах алгоритмов:

– сбора, обработки и анализа информации о состоянии сети, т.е. характеристик той или иной аномалии в моменты времени. Результаты мониторинга и анализа (выявленные аномалии) группируются оптимальным образом в классы исходных ситуаций. Формируется приближенное представление классификационной модели;

– алгоритмы управления: ситуация, наблюдаемая в момент времени или относится к классу наиболее близких к ней ситуаций (для которых установлена стратегия управления с помощью отображения), или «дает начало» образованию нового класса ситуаций, стратегия управления для которых не совпадает ни с одной из стратегий, идентифицированных на предыдущем этапе [1, 2, 7].

Сравнительный анализ результатов практического использования при выявлении аномалий в разнородной сети, полученных на основе методик с применением аналитических и статистических моделей, показал эффективность предлагаемой методики даже в условиях недостаточной и нечеткой информации относительно классификационных признаков предполагаемых аномалий при работе в распределенных гетерогенных сетях.

В качестве вывода отметим, что практическое применение описанных технологий, построенных на алгоритмах ситуационного анализа и моделирования, «эвристического» обнаружения аномалий и использовании баз данных и знаний (классификационные признаки, ретроспективный анализ, БД/БЗ ситуаций и моделей и т.д.) совместно с экспертными знаниями позволяет существенно повысить качество процессов выявления и управления уязвимостями в распределенных сетях и, следовательно, предлагаемые технологии могут являться основой построения архитектуры системы обнаружения и устранения аномалий.

Примечания:

1. Clemm A. Network Management Fundamentals. Cisco Press, 2011. 510 pp.
2. Rattner D. «Risk Assessments». Security Management. Lecture. Northeastern University, Boston, 2010.
3. Дымарский Я.С., Крутякова Н.П., Яновский Г.Г. Управление сетями связи: принципы, протоколы, прикладные задачи. М., 2010. 384 с.
4. Симанков В.С., Шпехт И.А. Автоматизация системных исследований на основе неформальных процедур: монография. М.: БиномПресс, 2012. 358 с.
5. Симанков В.С. Автоматизация системных исследований: монография. Краснодар, 2002. 376 с.
6. Гребешков А.Ю. Стандарты и технологии управления сетями связи. М.: Эко-Трендз, 2009. 288 с.
7. Клиланд Д., Книг В. Системный анализ и целевое управление. М.: Сов. радио, 1984. 280 с.
8. Мелихов А.Н., Бернштейн Л.С., Коровин С.Я. Ситуационные советующие системы с нечеткой логикой. М.: Наука, 1990. 272 с.

References:

1. Clemm A. Network Management Fundamentals. Cisco Press, 2011. 510 pp.
2. Rattner D. «Risk Assessments». Security Management. Lecture. Northeastern University, Boston, 2010.
3. Dymarskiy Ya.S., Krutyakova N.P., Yanovskiy G.G. Management of communication networks: principles, protocols, applied tasks. M., 2010. 384 pp.
4. Simankov V.S., Shpekht I.A. Automation of system researches on the basis of informal procedures: a monograph. M.: BinomPress, 2012. 358 pp.
5. Simankov V.S. Automation of system researches: a monograph. Krasnodar, 2002. 376 pp.
6. Grebeshkov A.Yu. Standarts and technologies of communication networks management. M.: Eko-Trendz, 2009. 288 pp.
7. Kliland D., King B. System analysis and venture management. M.: Sov. radio, 1984. 280 pp.
8. Melikhov A.N., Bernstein L.S., Korovin S.Ya. Situational advising systems with fuzzy logic. M:. Nauka, 1990. 272 pp.