УДК 004.652.4

05.00.00 Технические науки

СИСТЕМЫ УСТРАНЕНИЯ СЕТЕВЫХ АНОМАЛИЙ И МЕТОДИКИ ПОСТРОЕНИЯ ИХ АРХИТЕКТУРЫ

Кучер Виктор Алексеевич
к.т.н

Магомадов Алексей Сайпудинович
д.т.н.

Чигликова Надежда Дмитриевна
к.т.н.

Дьяченко Роман Александрович
д.т.н.
Кубанский государственный технологический университет, Краснодар, Россия

В статье анализируются различные этапы проектирования архитектуры систем обнаружения и противодействия сетевым аномалиям. Указывается, что для определения ситуаций состояния сети возможна их обобщенно-признаковая классификация: «нормальные», «критические» и «аварийные». Предлагаются основы технологий для построения архитектуры систем обнаружения и устранения аномалий

Ключевые слова: СЕТЕВЫЕ АНОМАЛИИ, БАЗА ДАННЫХ, СОСТОЯНИЕ СЕТИ, УСТРАНЕНИЕ АНОМАЛИЙ

UDC 004.652.4

Technical sciences

SYSTEMS OF REMOVING NETWORK ANOMALIES AND METHODS OF CREATION THEIR ARCHITECTURE

Kucher Viktor Alekseevich
Cand.Tech.Sci.

Magomadov Aleksey Saipudinovich
Dr.Sci.Tech.

Chiglikova Nadezhda Dmitrievna
Cand.Tech.Sci.

Dyachenko Roman Aleksandrovich
Dr.Sci.Tech.
Kuban State Technological University, Krasnodar, Russia

Different stages of designing architecture of detection systems and opposition to network anomalies are analyzed in this article. It is pointed that common classification can be to determine state of network: “normal”, “critical”, “faulted”. Bases for building architecture of detection and removing anomalies are offered

Keywords: NETWORK ANOMALIES, DATA BASES, STATE OF NETWORK, REMOVING ANOMALIES

Введение

Задача обнаружения 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 [3, 4, 6].

Разнообразие сетевых аномалий (СА), их природа 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 построения 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).

Укажем, 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.

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

Разрабатываемый в данной работе 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.

Использование 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 [2].

Для формального описания системы управления сетью используем кортеж, описывающий подсистему, характеризующую сеть как объект управления (рисунок 1):

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

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.

Разнообразие архитектуры и режимов функционирования современных сетей (гетерогенность, распределенность и т.д.) обуславливают необходимость использования в системе обнаружения и устранения аномалий ряда математических моделей [3,5,6], позволяющих учесть имеющиеся неопределенности и неточности знаний относительно предполагаемых аномалий.

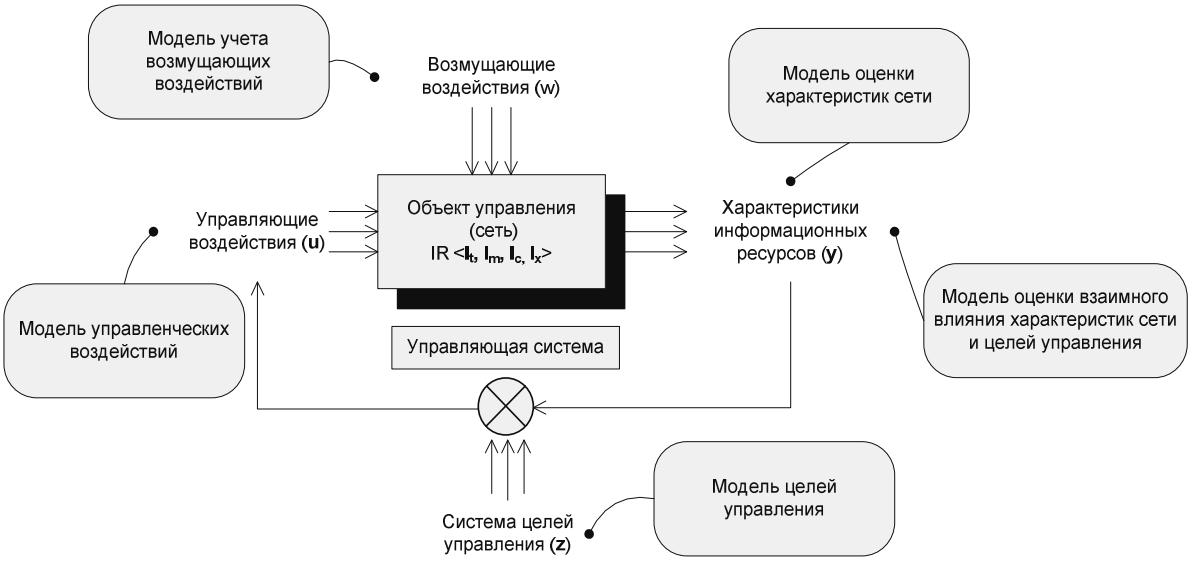

Рисунок 1 - Общая схема системы обнаружения и выявления аномалий в сети

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.

Разработки математического и алгоритмического обеспечений такой системы обнаружения требует обращение внимания 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» [3,4].

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. Для этого нештатная ситуация должна быть отнесена к определенному классу ситуаций, проанализированы рекомендации, при необходимости проведен сбор дополнительной

информации и на основе полученных данных принята схема управляющего воздействия.

При отборе 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 имитационные, структурно-функциональные, математические и иные модели сети. Свойства формальной ситуационной модели определяются функциональными свойствами механизмов преобразования в формальные математические модели (рисунок 2).

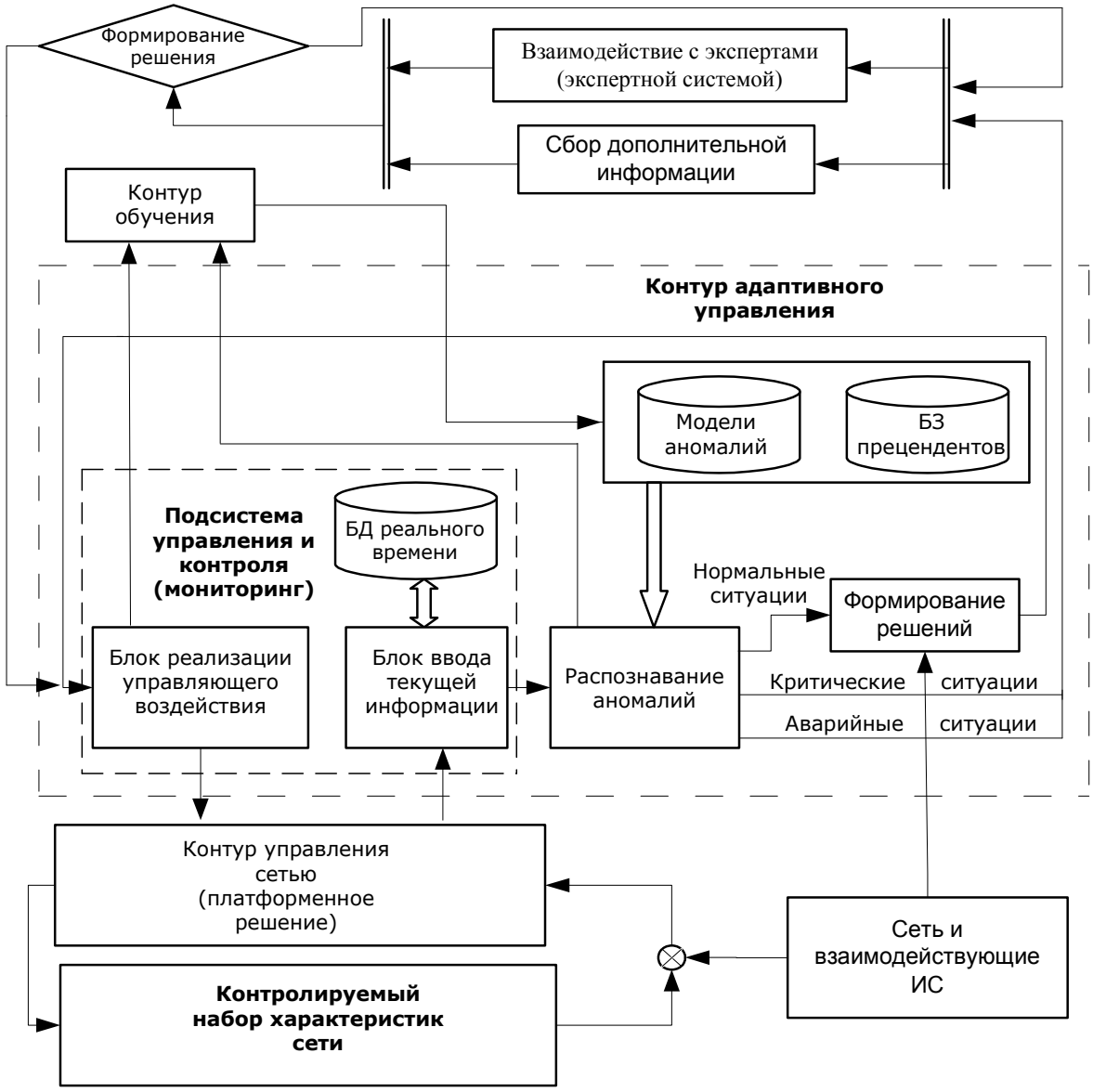

Рисунок 2 - Функциональная модель обнаружения аномалий на множестве классификационных признаков

Внедрение на практике 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.

Отметим ещё раз, что 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.

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

$$J = F_1(x,y,w,u), \quad (2)$$

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 совокупность меток, индексирующих множество возможных методов противодействия.

В разработанном подходе обнаружения аномалий режимов 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.

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.

Заключение

В заключении 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 распределённых сетях и, следовательно, предлагаемые технологии могут являться основой построения архитектуры системы обнаружения и устранения аномалий.

Литература

1. Симанков В.С. Автоматизация системных исследований: Монография (научное издание). Кубанский государственный технологический университет. – Краснодар, 2002. – 376 с.
2. Симанков В.С., Шпехт И.А. Автоматизация системных исследований на основе неформальных процедур: Монография.–М.: БиномПресс, 2012. 358 с
3. *A. Clemm: Network Management Fundamentals*. *CiscoPress*, 2011
4. Д. Раттнер. "Анализ рисков в управлении сетевой безопасностью.". *Northeastern University*, 2010.
5. А. Ю. Гребешков. Стандарты и технологии управления сетями связи, Эко-Трендз, 2009
6. Я.С. Дымарский, Н.П. Крутякова, Г.Г. Яновский. Управление сетями связи: принципы, протоколы, прикладные задачи, Москва, 2010

References

1. Simankov V.S. Avtomatizacija sistemnyh issledovanij: Monografija (nauchnoe izdanie). Kubanskij gosudarstvennyj tehnologicheskij universitet. – Krasnodar, 2002. – 376 s.

2. Simankov V.S., Shpeht I.A. Avtomatizacija sistemnyh issledovanij na osnove neformal'nyh procedur: Monografija.–M.: BinomPress, 2012. 358 s

3. A. Clemm: Network Management Fundamentals. CiscoPress, 2011

4. D. Rattner. "Analiz riskov v upravlenii setevoj bezopasnost'ju.". Northeastern University, 2010.

5. A. Ju. Grebeshkov. Standarty i tehnologii upravlenija setjami svjazi, Jeko-Trendz, 2009

6. Ja.S. Dymarskij, N.P. Krutjakova, G.G. Janovskij. Upravlenie setjami svjazi: principy, protokoly, prikladnye zadachi, Moskva, 2010