УДК 004.272.3

В.А. Мартовицкий, И.В. Рубан

*Харьковский национальный университет радиоэлектроники, Харьков*

# МОДЕЛЬ МУЛЬТИАГЕНТНОЙ СИСТЕМЫ СБОРА И ХРАНЕНИЯ ИНФОРМАЦИИ

*Статья посвящена проблеме создания подсистем, предназначенных для решения задач сбора и хранения параметров в системах мониторинга сетевой инфраструктуры. Рассмотрена модель мультиагентной системы сбора и хранения информации. Целью агентов данной системы является представление пользователю или информационной системе более высокого уровня информации о состоянии наблюдаемой сетевой инфраструктурой, полученной в результате сбора и интеллектуальной обработки параметров.*

***Ключевые слова:*** *сбор и хранение информации, мультиагентная система, агент, Big Data.*

## Введение

В системах мониторинга сетевой инфраструктуры происходят радикальные перемены, вызванные обострением конкуренции на рынке, ростом требований к качеству обеспечения безопасности, техническим перевооружением сетей связи, изменением характера распределения трафика. Все это приводит к необходимости осуществления контроля большого количества параметров функционирования сетей различных технологий.

Для этих целей в системе мониторинга сетей применяется подсистема сбора и хранения данных. Она не только меняет представления о системе эксплуатации, переходя от сбора данных параметров отдельных станций к параметрам эксплуатации всей сети, а также автоматизирует многие рутинные процессы по сбору и обработке сетевых данных.

— Анализ этой информации дает возможность выявления разнообразных случаев угроз и нарушений, таких как:

— несанкционированное проникновение в сеть, пропущенное классическими средствами защиты периметра (IPS/IDS);

— распространение вирусов, «червей» и шпионского ПО, не обнаруженных штатными антивирусными средствами.

— неправильные действия пользователей (например, масштабные загрузки с торрент-трекеров, обращение к сегментам сети, к которым нет доступа, попытка доступа к конфиденциальной информации и т.п.);

— появление в сети новых устройств и их поведение;

— ошибки в работе оборудования;

— возникновение в сети «узких» мест и другие возможные нарушения.

Архитектура подсистем предназначенных для решения задач сбора и хранения параметров полученных от датчиков, характеризуются не только их целевыми функциями, но и функциональными возможностями, обеспечивающими реализацию целевых функций, иерархией и степенью параллелизма решения задач, однородностью либо разнородностью модульной структуры, организацией сбора информации в режиме реального времени, обработки данных и сетевого обмена информацией с абонентами [1].

При этом должны обеспечиваться:

— невмешательство в работу сетевого оборудования;

— постоянный сбор статистической информации, который позволяет создавать крупномасштабные базы данных, необходимые для проведения псевдооперативного и статистического анализа сети;

— обеспечение высокой скорости обработки запросов на предоставление требуемых информационных ресурсов и сервисов;

— выполнение сбора, обработки, хранения полной информации о состоянии всех компонентов телекоммуникационной и информационной инфраструктуры сети в реальном времени независимо от архитектуры сети, типа коммутатора и поставщика;

— создание единого стандартизованого информационного центра хранения данных о состоянии систем и сети.

Учитывая большой объем событий, сопутствующих процессу диагностического мониторинга, многообразие типов событий и устройств в открытой диагностической системе и необходимость функционирования в режиме реального времени с учетом высокой изменчивости внешней среды, задачу построения диагностической сенсорной сети следует отнести к проблематике обработки больших данных (Big Data) [2].

Решение указанной проблемы сопряжено с реализацией новых парадигм программирования,



© В.А. Мартовицкий, И.В. Рубан

поддерживающих возможность распределенного взаимодействия автономных активных устройств в процессе решения конкретной оперативной задачи [3].

Для решения выше указанных проблем наиболее подходящей технологией является реализация мультиагентной системы с использованием автономных программных агентов.

**Целью данной статьи** является описание мультиагентной модели системы сбора и хранения информации, представляющею собой построенную на основе агентов.

Целью данных агентов является представление пользователю или информационной системе более высокого уровня информации о состоянии наблюдаемой сетевой инфраструктурой, полученной в результате сбора и интеллектуальной обработки параметров.

## Основная часть

Для выявления разнообразных случаев угроз и нарушений система мониторинга должна осуществлять контроль большого количества параметров состояния компонентов сети, который реализуется на разных уровнях [4].

— Канальный уровень. Данный уровень определяет методы доступа к среде передачи данных и обеспечивает передачу кадра данных между любыми узлами в сетях с типовой топологией по физическому адресу сетевого устройства. Адреса, используемые на канальном уровне в локальных сетях, часто называют MAC-адресами (MAC media access control, управление доступом к среде передачи данных).

— Сетевой уровень. Обеспечивает доставку данных между любыми двумя узлами в сети с произвольной топологией, при этом не гарантируется надежная доставка данных от узла-отправителя к узлу-получателю.

На этом уровне выполняются такие функции:

маршрутизация логических адресов сетевых узлов,

создание и ведение таблиц маршрутизации,

фрагментация и сборка данных.

— Сеансовый уровень. Реализует средства управления сессией, диалогом, а также предоставляет средства синхронизации в рамках процедуры обмена сообщениями, контроля над ошибками, обработки транзакций, поддержки вызова удаленных процедур RPC.

— Прикладной уровень. Набор сетевых сервисов, предоставляемых конечным пользователям и приложениям. Примеры таких сервисов — обмен сообщениями электронной почты, передача файлов между узлами сети, приложения управления сетевыми узлами.

Контроль параметров на каждом из этих уровней позволяет выявлять угрозы направление на объекты сетевой инфраструктуры, которые условно можно разделить на такие классы:

Первый класс угроз — это нарушение функционирования сетевой инфраструктуры. Для реализации угрозы возможны следующие типы атак:

переполнение CAM–таблицы,

VLAN Hopping,

атака на STP,

MAC-снуфинг,

атака на PVLAN,

атака на DHCP.

Второй класс угроз направленный на маршрутизаторы и их алгоритмы маршрутизации. Для данного класса угроз характерны следующие типы атак:

подмена маршрута RIP,

атака BGP Router Masquerading,

атаки на MD5 для BGP,

«Слепые» DoS-атаки на BGP-маршрутизаторы.

Третий класс угроз направленный на взаимодействие со стеком протоколов TCP/IP. Примерами данного класса угроз являются: сканирование сети, атака Teardrop, атака на TCP, атака на UDP [5].

Исходя из модели мониторинга рассмотренной в статье [6] по техническим и другим причинам логически связанные данные сохраняются в различных форматах под управлением различных систем хранения и обработки данных. Очевидно, что для изучения и анализа информации требуется открытый доступ к локальным и удаленным информационным источникам.

С другой стороны, встает проблема интеграции данных.

Различные коллекции параметров состояния компонентов сети, даже расположенные на одном физическом узле, зачастую имеют различные логические входы и не предоставляют возможности сквозного связывания данных из разных источников.

Необходимость учета всей имеющейся информации по определенному вопросу требует от системы сбора и хранения данных обеспечения прозрачных для пользователей средств доступа к распределенной информации.

Одним из решений данной задачи является реструктуризация разнородных данных. Для реструктуризации данных мониторинга потребуется гармонизация сопоставимой информации к единому представлению, либо расширение структур данных путем добавления уникальных признаков, позволяющих сопоставлять данные из различных источников.

Так или иначе, эта задача весьма трудоемкая, особенно для удаленных друг от друга хранилищ,

так как требует и технического, и организационного взаимодействия от источников. Кроме того, после реструктуризации данных потребуется качественная модификация средств доступа к информации с учетом новых структур данных.

В связи с этим предлагается модель системы сбора и хранения данных, обеспечивающая работу с множеством разнородных источников, путем их интегрирования с целью получения более полного сбора связной информации. Система основана на мультиагентном подходе и позволяет не прекращать обработку запросов при выполнении модификаций набора и структур используемых баз данных.

В зависимости от решаемой задачи реализация мультиагентной системы может кардинально меняться, однако при этом программные агенты сохраняют свойства посреднической деятельности: агенты постоянно взаимодействуют с пользователями или другими программами.

Для взаимодействия между всеми агентами предлагается использовать группу интеллектуальных агентов запроса, целью которых является:

координация агентов сбора информации,

реструктуризация полученной информации;

реализация протоколов и механизмов передачи сообщений между всеми агентами модели.

Функции каждого агента-сбора информации следующие:

— сбор и накопление данных в промежуточном хранилище небольшого объема;

— предварительная обработка данных в реальном времени;

— корректировка интервалов дискретизации;

— обращение к агентам запроса для проведения дополнительных измерений и осуществления комплексного анализа ситуации;

Модель системы сбора и хранения информации представлена на рис. 1.

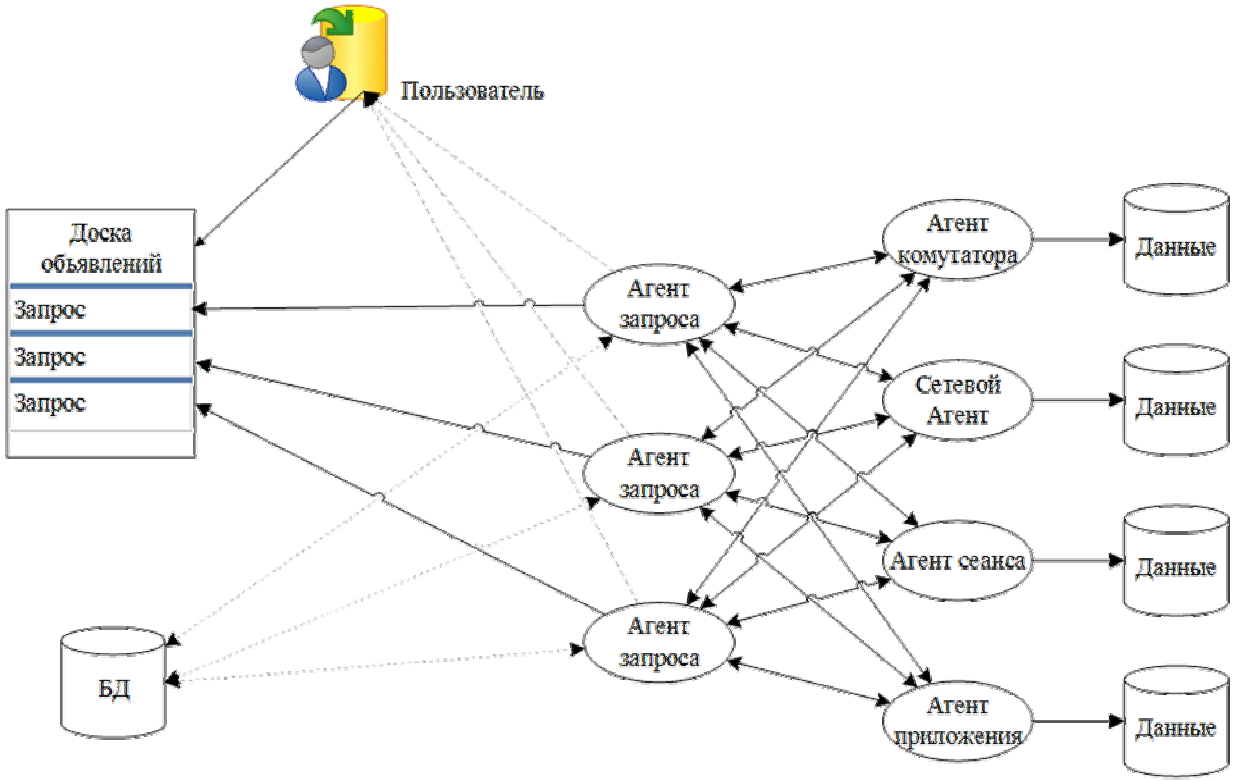


Рис. 1. Модель системы сбора и хранения информации

Модель сбора и хранения информации включает в себя следующие элементы:

— Агент коммутатора и сетевой агент, которые обеспечивают сбор данных с первых двух уровней, описанных выше. Поскольку функционирование канального и сетевого уровня, обеспечивается, в основном, активным сетевым оборудованием и, как правило, реализуются следующими компонентами: сетевыми адаптерами, репитерами, мостами, концентраторами, коммутаторами, маршрутизаторами, для минимизации вмешательства в работу сетевого оборудования данные агенты будут работать на основе протокола SNMP. В качестве промежуточного хранилища данных будет использоваться MIB-файлы. Задачей этих агентов является стандартизация данных из файлов для дальнейшей передачи их агентам запросов. Также на агентов возложена задача по управлению доставкой аварийных сообщений, поскольку протокол SNMP работает через ненадежный протокол UDP [7].

— Агент сеанса, который обеспечивает сбор информации про имя пользователя, имя терминаль-

ной линии, астрономическое время начала сеанса, продолжительность бездействия терминальной линии с момента последнего обмена, идентификатор процесса интерпретатора команд shell для каждого из пользователей, работающих в системе. В зависимости от операционной системы промежуточные хранилища могут отличаться.

Так, например, для UNIX систем такими хранилищами будут системные файлы /etc/utmp, /etc/wtmp, /etc/inittab.

— Агент приложения отвечает за сбор данных от разных приложений специфических для той или иной информационно-вычислительной системы.

— Агенты запроса цель которых является обработка запросов на выборку данных от пользователей системы сбора, координация других агентов для сбора необходимой информации, а также реструктуризация полученной информации для хранения статистический данных о системе в целом.

## Заключение

В статье представлена модель мультиагентной системы сбора и хранения информации. Предлагаемое решение имеет следующие преимущества:

— ориентирована на одновременную работу с множеством запросов и разнородных информационных источников;

— создание единого стандартизованого информационного центра хранения данных о состоянии систем и сети;

— уменьшение нагрузки на сеть за счет использования промежуточных хранилищ и регулировки обмена информацией между агентами.

На основе предложенного подхода ведется разработка и реализация мониторинга кластерных суперкомпьютеров.

Дальнейшее развитие системы направлено на разработку оптимальной структуры реляционной базы данных для создания единого стандартизованного информационного центра хранения данных о состоянии систем и сети.

Другим направлением развития является использования методов машинного обучения для корректной обработки неполных или отсутствующих данных в детектировании аномальных состояний информационно-вычислительной системы.

## Список литературы


*1. Петров, Назар Сергеевич. "Архитектура кластерной системы сбора и обработки информации датчиков динамических объектов." Известия Южного федерального университета. Технические науки 11 (148) (2013).*

*2. Sahandi, Reza, et al. "Wireless technology in the evolution of patient monitoring on general hospital wards." Journal of medical engineering & technology 34.1 (2010): 51-63.*

*3. Иващенко, А. В., А. А. Минаев, and М. Ю. Сподобаев. "Шаблон агента-медиатора для программного обеспечения сенсорных сетей." Программные продукты и системы 3 (111) (2015).*

*4. Капустин, С. П., and В. Е. Дементьев. "Информационно-вычислительные сети: учебное пособие." Ульяновск: УлГТУ, 2011.–141 с (2011).*

*5. Мартовицький В.О. Критерии обнаружения угроз безопасности по цели сетевого воздействия // Інформаційна безпека та комп'ютерні технології: Збірник тез доповідей II міжнародної науково-практичної конференції, 20-22 квітня 2017 року, м. Кропивницький:, 2017- с. 60.*

*6. Ruban, I., V. Martovytskyi, and N. Lukova-Chuiko. "Разработка модели мониторинга кластерных суперкомпьютеров." Восточно-Европейский журнал передовых технологий 6.2 (2016): 32-37.*

*7. Кенин, Александр Михайлович. Самоучитель системного администратора. 3-е изд. БХВ-Петербург, 2012.*



*Надійшла до редколегії 15.10.2017*

**Рецензент**: д-р техн. наук, проф. Г.В. Худов, Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків.


### МОДЕЛЬ МУЛЬТИАГЕНТНОЇ СИСТЕМИ ЗБОРУ ТА ЗБЕРІГАННЯ ІНФОРМАЦІЇ


В.О. Мартовицький, І.В. Рубан



*Стаття присвячена проблемі створення підсистем, призначених для вирішення завдань збору та зберігання параметрів в системах моніторингу мережевої інфраструктури. Розглянуто модель мультиагентної системи збору і зберігання інформації. Метою представників цієї системи є уявлення користувачеві або інформаційній системі більш високого рівня інформації про стан спостерігається мережевою інфраструктурою, отриманої в результаті збору та інтелектуальної обробки параметрів.*



***Ключові слова:*** *collection and storage of information. multiagent system, agent, Big Data.*


### MODEL OF MULTIAGENT SYSTEM OF INFORMATION COLLECTION AND STORAGE


V.A. Martovytskyi, I.V. Ruban



*The article is devoted to the problem of creating subsystems intended for solving tasks of collection and storage of parameters in network infrastructure monitoring systems. The model of a multi-agent system of information collection and storage is considered. The goal of the agents of this system is to provide the user or information system with a higher level of information about the status of the monitored network infrastructure obtained as a result of the collection and intelligent processing of parameters.*



***Keywords:*** *collection and storage of information. multiagent system, agent, Big Data.*