

N. A. Zhukova

Saint-Petersburg electro technical university «LETI»

PATTERNS FOR DESIGN OBJECT-ORIENTED INTELLIGENT GEOGRAPHIC INFORMATION SYSTEMS

In the article patterns for building object-oriented descriptions of the intelligent geographic information systems focused on solving problems of data processing and analysis in applied subject domains are offered. Patterns are developed within the general concept of development of object-oriented intellectual systems according to the agile methodology of the systems design. Patterns for describing both separate objects and information models of the systems are presented.

Intelligent GIS, object-oriented approach, software design patterns

УДК 050.043.19

А. К. Большев, А. А. Лавров

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Программные средства мониторинга обработки данных гидроакустической станции на основе системы мониторинга Nagios

Рассмотрены особенности задач мониторинга состояния бортовых вычислительных комплексов обработки данных, роль и место программных средств мониторинга системы обработки, отображения данных и управления (СООДУ) в составе автоматизированной системы технического диагностирования (АСТД) гидроакустической станции. Предложена архитектура подсистемы мониторинга СООДУ, предназначенной для работы в режиме реального времени в составе АСТД гидроакустических станций подвижных автономных объектов.

Бортовые комплексы обработки гидроакустических данных, мониторинг вычислительных сетей, Nagios

СООДУ представляет собой комплекс программно-аппаратных средств, объединенных высокоскоростной сетью Ethernet. Поскольку СООДУ является ядром бортовой информационной системы, непосредственно влияющим на функционирование базовых систем подвижного объекта (в данной статье – гидроакустической станции (ГАС)), необходимо наличие средств обеспечения контроля, диагностики и мониторинга программно-аппаратного комплекса СООДУ.

Задачи диагностики СООДУ сводятся к мониторингу состояния сетевой телекоммуникационной инфраструктуры цифрового вычислительного комплекса (ЦВК), работоспособности всех входящих в СООДУ узлов и выполнения ими требуемой функциональности, целостности аппаратной конфигурации СООДУ и к уведомлению опе-

раторов комплекса в режиме реального времени об обнаруженных проблемах и неисправностях.

Специфические требования к системе мониторинга определяются спецификой ее применения и требованиями к ГАС. Отличием систем сетевого мониторинга СООДУ подвижных объектов промышленного или военного назначения от систем мониторинга стационарных корпоративных сетей и иных сетей связи являются повышенные требования по надежности, отказоустойчивости, а также требования к аппаратным ресурсам [1].

Основные функциональные требования к системам мониторинга СООДУ подвижных объектов:

- повышенная отказоустойчивость, наличие функций защиты от сбоев;
- функционирование в режиме реального времени, минимизация времени реакции на про-

исходящие в контролируемой инфраструктуре события;

- минимизация аппаратных требований, необходимость сохранения работоспособности в условиях ограниченного объема памяти и иных аппаратных ресурсов;

- масштабируемость, возможность подключения модулей для сбора данных любого рода; поддержка адаптивных алгоритмов мониторинга.

Роль и место подсистемы мониторинга в АСТД. Подсистема мониторинга СООДУ (ПМ СООДУ) предназначена для осуществления комплексного мониторинга СООДУ и обеспечивает решение следующих задач мониторинга и диагностики СООДУ:

1. Постоянное наблюдение за работоспособностью устройств и программного обеспечения комплекса посредством отслеживания ряда заданных оператором комплекса параметров составных частей СООДУ.

2. Интеграция ПМ СООДУ в состав ПО оператора комплекса для отображения информации о состоянии комплекса в режиме реального времени, а также немедленной передачи оператору (программному обеспечению оператора) уведомлений о нештатном поведении комплекса или не-

штатном состоянии того или иного (или нескольких) отслеживаемых параметров работы СООДУ.

3. Обеспечение в соответствии с требованиями к АСТД четырех режимов контроля (мониторинга): контроля начального пуска, оперативного контроля, контроля технического состояния, поиска места отказа.

4. Ведение журналов мониторинга, содержащих историю изменения отслеживаемых параметров работы комплекса, их графическая визуализация и предоставление по запросу оператора информации о состоянии комплекса, истории сбоев в работе и нештатном состоянии параметров.

5. Обеспечение информационной безопасности комплекса за счет отслеживания целостности сетевых характеристик входящих в состав комплекса узлов.

6. Выявление аномалий в поведении комплекса за счет применения методов выявления аномалий, основанных на использовании самообучающейся ИНС.

Архитектура подсистемы мониторинга СООДУ. Архитектура ПМ СООДУ и ее место в составе аппаратных и программных средств АСТД и СООДУ иллюстрируются рис. 1.

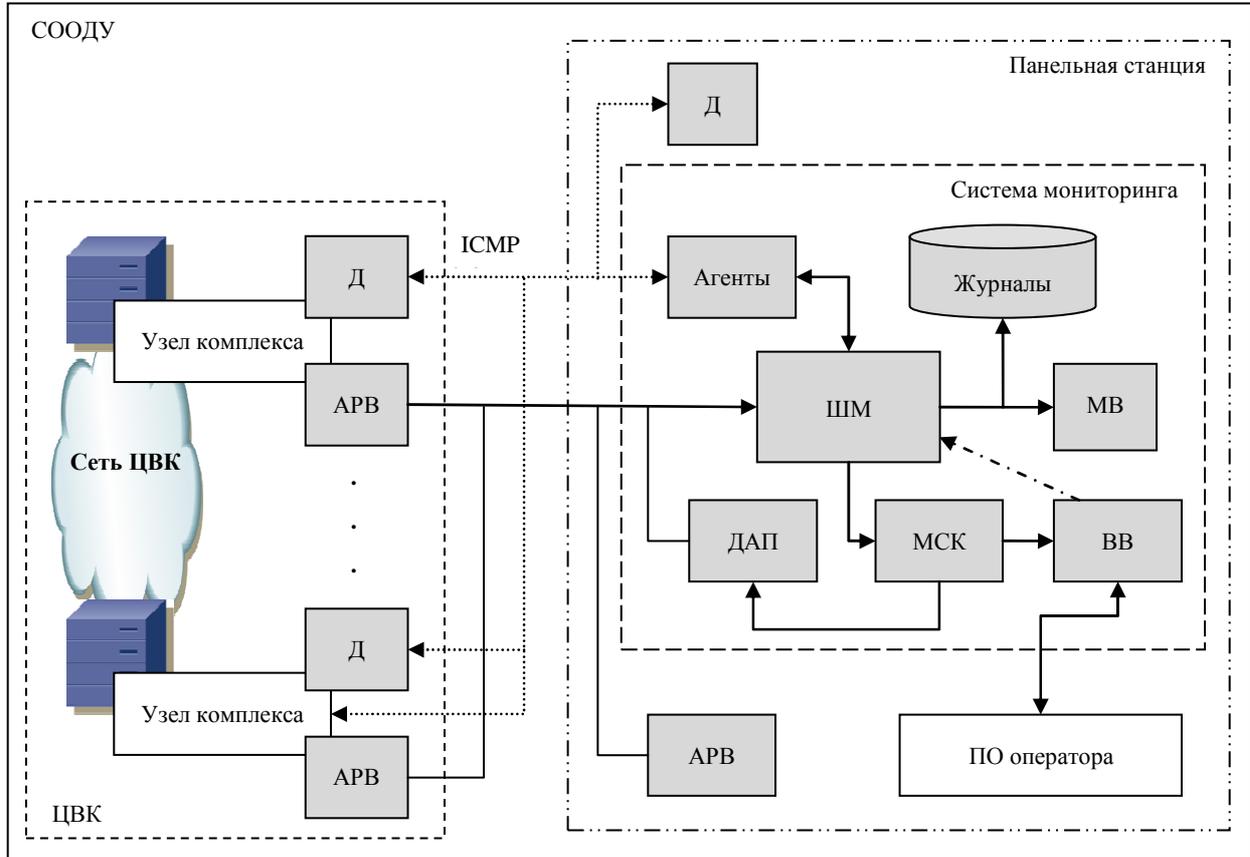


Рис. 1

В состав ПМ СООДУ входят следующие внешние и внутренние модули:

1. *Шасси мониторинга* (ШМ) – внутренний базовый модуль ПМ, который предоставляет интерфейсы для подключения агентов, обеспечивает загрузку и управление конфигурацией подсистемы, управляет модулями оповещения и журналирования и остальными компонентами ПМ.

2. *Агенты*, опрашивающие удаленные датчики или узлы напрямую (например, по протоколу ICMP для определения доступности узла СООДУ) и передающие полученную информацию блоку ШМ.

3. *Журналы*, хранящие числовую и текстовую информацию о событиях, происходящих в сети, и представляющие собой структурированный набор файлов; информация поступает в файлы журналов непосредственно от ШМ.

4. *Модуль визуализации* (МВ), отвечающий за графическое представление информации о состоянии конкретного параметра мониторинга за определенный период времени.

5. *Модуль состояния комплекса* (МСК), хранящий текущее состояние всех отслеживаемых параметров составных частей СООДУ и обеспечивающий взаимодействие с виджетом визуализации по специальному протоколу. Через регулярные промежутки времени модуль состояния передает виджету визуализации информацию о состоянии всех отслеживаемых параметров СООДУ. При возникновении нештатной ситуации МСК уведомляет виджет визуализации о произошедшем событии.

6. *Датчики* (Д), которые устанавливаются на узлах СООДУ и предоставляют агентам информацию о состоянии отслеживаемых параметров работы СООДУ. Датчики используются для получения информации о состоянии только тех параметров, период опроса которых (время реакции на изменение состояния со стороны ПМ) составляет более 1 с. Для отслеживания состояния параметров, период опроса которых должен составлять менее 1 с, используются агенты реального времени.

7. *Агенты реального времени* (АРВ), устанавливаемые на узлах СООДУ для опроса параметров, время реакции на изменение состояния которых со стороны подсистемы мониторинга должно быть минимальным.

8. *Датчик аномального поведения* (ДАП), определяющий аномалии в текущем состоянии СООДУ посредством эвристических предполо-

жений о штатном поведении комплекса. Эвристики вырабатываются в процессе мониторинга с использованием самообучающейся ИНС.

9. *Виджет визуализации* (ВВ), осуществляющий связь между программным обеспечением управления и отображения информации и подсистемой мониторинга. Виджет визуализации обеспечивает отображение всей поступающей от системы мониторинга информации, а также возможность передачи подсистеме мониторинга команд, связанных с отображением поступающей информации и управлением процессом опроса узлов СООДУ.

Общие принципы функционирования ПМ. Основные положения, касающиеся принципов работы ПМ СООДУ, формулируются следующим образом:

1. При запуске системы осуществляется *контроль начального пуска* – последовательный опрос всех параметров составных частей СООДУ. По окончании опроса виджет визуализации получает информацию о состоянии комплекса.

2. Для каждого параметра с периодом опроса более 1 с вырабатывается специальный график опроса для избежания пересечения одновременно опроса двух или более параметров.

3. Агенты периодически опрашивают датчики параметров. Полученные численные данные записываются в журналы и передаются МВ.

4. АРВ, установленные на узлах СООДУ, передают шасси данные о состоянии отслеживаемых параметров каждые 50 мс.

5. Информация о состоянии отслеживаемых узлов и параметров функционирования СООДУ передается виджету визуализации и отображается на дисплее оператора в режиме реального времени.

6. С ПО оператора можно запросить выполнение *контроля технического состояния* – последовательный опрос всех параметров составных частей СООДУ или нескольких заданных параметров.

7. Каждые 60 с состояние всех параметров мониторинга передается на ДАП для определения вероятности аномального поведения СООДУ в данный момент времени. При обнаружении аномальностей в состоянии СООДУ информация об этом немедленно передается ВВ.

Рассмотрим архитектуру основных компонентов ПМ СООДУ. Архитектура *шасси мониторинга* представлена на рис. 2.

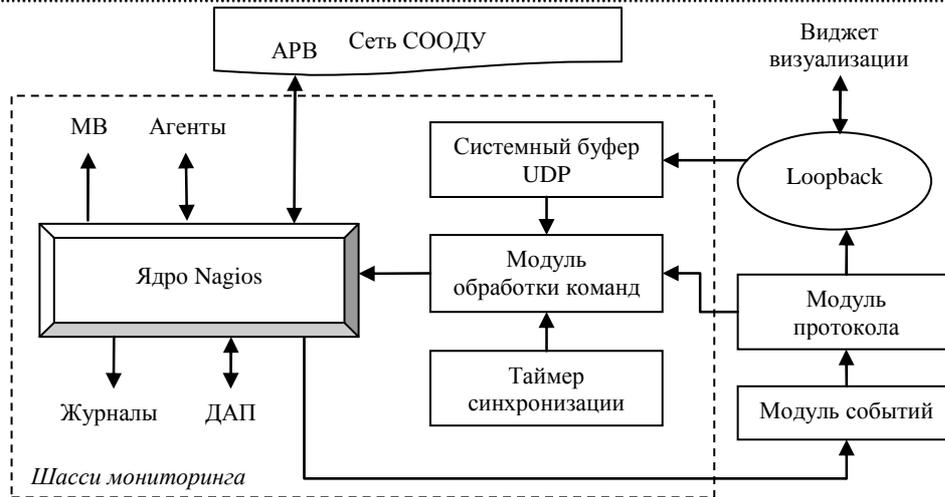


Рис. 2

Программным ядром шасси мониторинга является Nagios. Nagios – приложение с открытым кодом, предназначенное для комплексного всестороннего мониторинга компьютерных систем и сетей.

Шасси системы Nagios представляет собой сервис, автоматически запускающийся при старте узла, на котором развернута система мониторинга.

Nagios является модульной системой. Само шасси не выполняет функции мониторинга, а лишь опрашивает агентов и датчики и обрабатывает поступающую информацию.

Принцип функционирования шасси мониторинга в ПМ СООДУ:

1. Ядро Nagios, взаимодействуя с агентами и датчиком аномального поведения, получает информацию о состоянии узлов сети, параметров их текущей работы и состоянии всей сети в целом.

2. Полученные данные передаются модулю визуализации и журналам, а также модулю событий. Модуль событий проводит предварительную обработку данных, после чего передает их модулю протокола для отправки виджету визуализации и отображения оператору.

3. Взаимодействие между шасси мониторинга, виджетом визуализации и модулем протокола осуществляется по протоколу UDP по локальной петле loorback. При поступлении команды от оператора они отправляются в локальную петлю, после чего сохраняются в приемном буфере UDP операционной системы. По сигналу от таймера синхронизации, совершающего 2 тика в секунду, модуль обработки команд считывает имеющиеся в буфере UDP данные, обрабатывает их и отправляет ядру Nagios.

Все модули, входящие в состав шасси мониторинга, за исключением ядра Nagios и системного буфера UDP, разработаны в рамках работы специально для ПМ СООДУ.

Ядро Nagios в целях применения в составе АСТД ГАС оптимизировано для обеспечения возможности работы с системами реального времени, что потребовало изменения конфигурации ядра посредством наложения ряда специально разработанных патчей.

Агенты. Опрос состояния узлов СООДУ осуществляется с использованием агентов. Агент представляет собой модуль опроса или получения

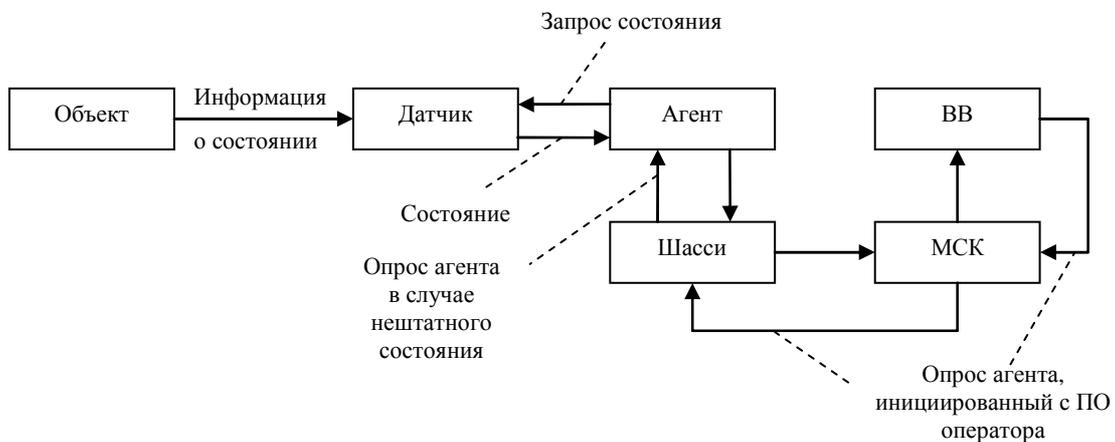


Рис. 3

информации от удаленных датчиков или напрямую от удаленных сервисов и устройств. Агенты принимают сообщения или опрашивают датчики, после чего шасси синхронизирует информацию и принимает решение о состоянии системы или сети. Датчики устанавливаются на удаленных узлах и предоставляют необходимую информацию по запросам агентов или самостоятельно посылают ее на узел с шасси.

На рис. 3 представлена диаграмма взаимодействия между агентами и шасси мониторинга.

В ПМ СООДУ используются 3 вида агентов:

1. *Стандартные агенты*, функционирующие в связке с соответствующими датчиками. Используются для отслеживания параметров узлов СООДУ, время реакции на изменение состояния которых может превышать 1 с. Функционируют следующим образом: по команде от шасси опрашивается связанный датчик, полученная информация передается шасси.

2. *АРВ*, используемые для отслеживания в режиме реального времени критических параметров узлов СООДУ. АРВ в режиме реального времени постоянно отправляют напрямую ШМ информацию о состоянии наблюдаемых параметров.

3. *Агенты «прямого действия»* (АПД), аналогичные стандартным агентам, но функционирующие без использования датчиков. Применяются для контроля параметров функционирования узлов, не требующих установки на узлах специальных датчиков (например, проверка доступности узла по ICMP).

В составе ПМ СООДУ используются 17 агентов, отслеживающих следующие характеристики работы комплекса (входящих в его состав узлов): сетевую доступность узла по ICMP; загрузку CPU узлов; температуру чипсета узлов; состояние подсистем хранения данных; загрузку GPU; состояние оперативной памяти; состояния служб

mpdboot, ntp, proftpd, ssh; состояние процессов обработки данных; состояние службы HTTP; количество запущенных процессов; целостность сетевой инфраструктуры СООДУ; аномальность поведения СООДУ.

Журналы. В составе ПМ СООДУ используются 2 типа журналов:

1. *Журнал состояний* – хранит информацию о состоянии отслеживаемых параметров, ведется ядром Nagios в текстовом формате.

2. *Журнал численной информации* – хранит исторические данные для численных значений отслеживаемых параметров, используемые для визуализации состояния параметров.

Модуль визуализации предназначен для визуализации исторического изменения состояния отслеживаемых численных параметров функционирования узлов СООДУ. МВ включает в себя скрипт предварительной обработки данных журнала численной информации и модуль NagVis для построения графиков.

Алгоритм работы модуля визуализации заключается в следующем:

1. По команде от ШМ скрипт предварительной обработки данных запрашивает информацию о значениях заданного параметра в заданный период времени у журнала численной информации и проводит их предварительную обработку.

2. Данные передаются в NagVis, который на основе полученной информации формирует график.

3. График передается в виджет визуализации по протоколу HTTP и выводится оператору.

Ключевой компонент модуля визуализации – NagVis, являющийся плагином Nagios, предназначенным для визуализации состояния узлов и сервисов.

Процедура начального пуска. Общий вид временной диаграммы процедуры начального пуска показан на рис. 4.

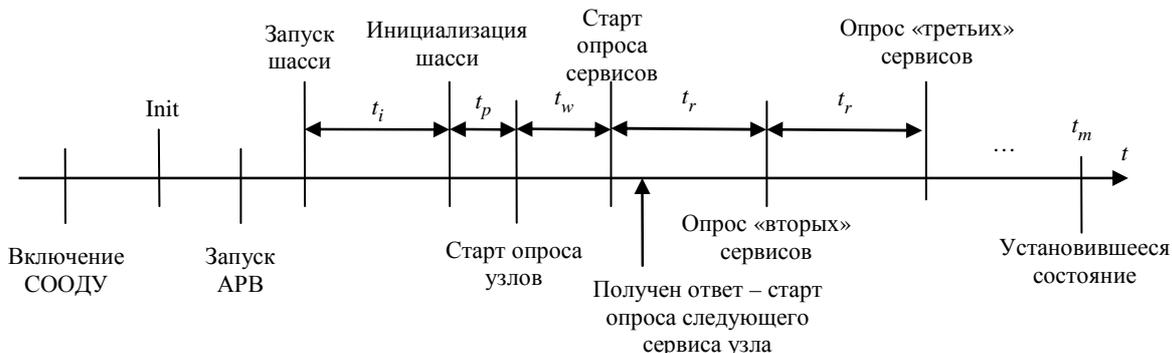


Рис. 4

После включения системы, инициализации ядра Linux и процедуры init происходит запуск АРВ и шасси мониторинга. Шасси требуется время t_i на процедуру инициализации, загрузки конфигурации и определения состояния сервера. Далее по истечении паузы t_p шасси начинает опрос узлов СООДУ на предмет доступности. Через время t_w шасси отправляет первый запрос сервисам доступных узлов. Опрашивается первый сервис каждого узла, выбираемый случайным образом из списка сервисов узла. После получения ответа от сервиса или по истечении времени t_r начинается опрос следующего сервиса узла. Узлы опрашиваются параллельно, сервисы на каждом из узлов во время процедуры начального пуска – последовательно.

Датчик аномального поведения предназначен для выявления аномалий в текущем состоянии СООДУ посредством эвристических предположений о штатном поведении комплекса с использованием самообучающейся ИНС. Реализован на языке C с использованием математических библиотек GSL и FANN [2], [3].

Агент контроля целостности сетевых характеристик СООДУ. Процедура контроля целостности сетевой инфраструктуры СООДУ реализуется соответствующим агентом, входящим в состав ПМ СООДУ в виде программного модуля контроля целостности сетевых характеристик (МКЦ). Процедура обеспечивает контроль за целостностью СООДУ с точки зрения аппаратной и программной структур входящих в состав СООДУ сетевых узлов, возможность выявления фактов несанкционированного подключения к инфраструктуре СООДУ посторонних узлов или изменения аппаратной и/или программной конфигурации существующих узлов.

Под целостностью СООДУ подразумевается состояние доступности всех входящих в СООДУ сетевых узлов и отсутствие в системе СООДУ посторонних аппаратных средств, не соответствующих архитектуре комплекса, а также соответствие аппаратной и программной конфигураций входящих в СООДУ сетевых узлов требованиям к аппаратно-программному составу комплекса. Процедура отслеживания указанного параметра основана на использовании методов сбора информации об удаленных сетевых узлах, и в частности, методов идентификации версии системного ПО удаленного узла на основе анализа временных характеристик сетевого взаимодействия [4], [5].

Для реализации МКЦ используется метод TCP-FTA2 [4], [6]. МКЦ реализован в виде отдельного демона Linux. Схема связей МКЦ с другими компонентами комплекса приведена на рис. 5.

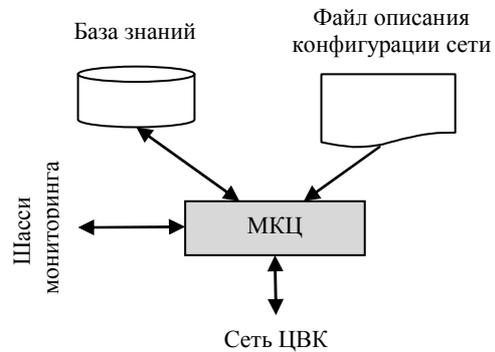


Рис. 5

Механизм функционирования МКЦ заключается в следующем:

1. При запуске считывается конфигурационный файл с параметрами сети, содержащий эталонные сигнатуры узлов сети, входящих в состав СООДУ, а также прочие параметры функционирования МКЦ.

2. На основании информации о количестве узлов, входящих в состав СООДУ, и заданного периода опроса формируется расписание опроса узлов.

3. Каждый узел, входящий в состав СООДУ, регулярно опрашивается МКЦ в соответствии с расписанием.

4. При обнаружении различий между сигнатурой, полученной от узла, и эталонной ядру мониторинга отправляется соответствующее уведомление. При этом предусмотрена возможность настройки «чувствительности» к изменению сигнатур узлов с целью устранения ложных срабатываний, вызванных случайными искажениями сигнатур.

Для функционирования алгоритма контроля целостности сетевых характеристик СООДУ необходима специальная настройка встроенного межсетевого экрана в связи с необходимостью запрета исходящих TCP-пакетов с флагом RST в адрес узлов, перечисленных в файле конфигурации МКЦ.

Модуль состояния комплекса реализуется модулем протокола (см. рис. 2) и обеспечивает формирование UDP-пакетов, отправляемых вidgetу визуализации для отображения информации о состоянии комплекса и отслеживаемых параметров.

Для уведомления виджета визуализации о состоянии каждого из отслеживаемых параметров генерируется отдельный пакет данных, содержащий следующие поля: идентификатор пакета, идентификатор отправителя, команда (признак того, что пакет содержит команду от виджета визуализации), тип (код команды для пакетов, содержащих команды от виджета визуализации), длина пакета в байтах, время получения данных (время получения информации о состоянии параметра), время проверки (время начала проверки состояния параметра), время получения данных (значение в миллисекундах для времени получения данных), время проверки (значение в миллисекундах для времени проверки), предыдущее состояние параметра (код состояния), текущее состояние параметра (код состояния), данные (информация о принадлежности параметра).

Протокол взаимодействия шасси мониторинга с модулем состояния комплекса. Взаимодействие между ШМ и МСК ведется по двум каналам: каналу событий и каналу команд. По каналу событий происходит отправка пакетов, содержащих сведения о событиях, на порт МСК.

Событие в терминах ПМ возникает в следующих случаях:

- в ШМ поступили результаты опроса состояния объекта или сервиса;
- изменилось состояние объекта или сервиса.

По каналу команд передаются команды от МСК к ШМ.

Получение пакетов с информацией о событиях и пакетов команд подтверждается получателем отправкой пакета-подтверждения.

Виджет визуализации представляет собой подключаемый модуль, реализованный на языке Qt. Виджет визуализации принимает от модуля состояния комплекса пакеты с информацией о состоянии отслеживаемых параметров и отображает полученную информацию в структурированном виде на дисплее оператора. Функции ВВ:

1. Визуализация поступающих данных от модуля состояния комплекса.
2. Вывод графиков изменения заданного параметра в заданном интервале времени.
3. Прием от пользователя команд по управлению процессом визуализации данных и процессом опроса узлов сети и их передача шасси мониторинга.

ВВ является связующим звеном между интерфейсом оператора СООДУ и подсистемой мониторинга. Подключение ВВ к программному обеспечению управления и отображения информации,

используемому панельной станцией СООДУ, осуществляется программным образом стандартными средствами языка C++. В случае необходимости отображения интерфейса, предоставляемого виджетом визуализации, ПО управления и отображения информации вызывает ВВ.

Интерфейс виджета визуализации адаптирован для использования на сенсорных панелях.

Виджет визуализации позволяет отправлять ШМ следующие команды от оператора:

1. Обновить информацию обо всех узлах и их параметрах – запрашивает последовательный переопрос всех отслеживаемых параметров СООДУ.

2. Обновить информацию о всех параметрах конкретного узла.

3. Переопрос конкретного параметра конкретного узла.

Отправка команд оператора выполняется посредством UDP-дейтаграмм по протоколу, соответствующему протоколу передачи данных о состоянии узлов СООДУ и отслеживаемых параметров от шасси к виджету визуализации.

В заключение приведем оценки требований к аппаратно-программным средствам, необходимым для развертывания и эксплуатации ПМ СООДУ.

Требования к программному окружению. ПМ СООДУ предназначена для выполнения в среде Linux и использует в своей работе следующее ПО сторонних производителей, распространяющееся по лицензии GNU:

1. Nagios (ШМ) с наложенными авторскими патчами для обеспечения режима реального времени.
2. Nagiosgraph и веб-сервер Apache версии 2 для реализации модуля визуализации.
3. Dis (виртуальная машина inferno-os) для реализации APB.

Требования к аппаратным вычислительным средствам. Рассмотрим оценки уровня потребления ПМ СООДУ аппаратных ресурсов узла мониторинга (узла, на базе которого развернута ПМ СООДУ). Рассматриваемые оценки представляют собой верхний предел уровня потребления того или иного ресурса.

Загрузка CPU и потребление ресурсов оперативной памяти. В случае использования процессора Core 2 Duo 3 GHz, на базе которого функционирует панельная станция, расчетная загрузка ядер процессора подсистемой мониторинга составит:

– для основного ядра: 10 % – максимум, 1 % – в штатном режиме;

– для второго ядра: 0–1 % – в штатном режиме, 1 % – при выполнении опросов.

В моменты генерации графиков для отчетов нагрузка на первом ядре возрастает в среднем на 15 %, т. е. составит 16–18 %.

Максимальное значение уровня потребления ресурсов оперативной памяти составляет 256 Мбайт.

Количество процессорного времени, потребляемого АРВ, составляет менее 1 %.

Потребление ресурсов дисковой подсистемы хранения данных. Объем потребляемого дискового пространства напрямую зависит от числа анализируемых параметров и типа их обработки.

Для параметров без визуализации *верхняя* граница для размера отчета в сутки (в байтах) вычисляется по следующей формуле:

$$P = 64(N_p + N_n) \frac{86400}{t_{ov}},$$

где N_p – количество параметров; N_n – количество узлов; t_{ov} – среднее время опроса.

Для параметров с визуализацией *верхняя* граница размера отчета в сутки увеличивается в среднем в 4 раза.

Графики анализируемых параметров генерируются и обрабатываются подсистемой мониторинга только при обращении к ним пользователя. При запросе графика оператором график временно загружается на диск, после просмотра удаляется. Для хранения одного графика требуется в среднем 202 Кбайт дискового пространства.

Время реакции системы определяется следующим образом:

$$t_r = t_d + t_a + t_n,$$

где t_d – время опроса датчика; t_a – время обработки информации агентом; t_n – время нотификации.

Время опроса датчика зависит от типа параметра. В частности, для проверки доступности узла оно составляет 200 мс, для определения уровня загруженности процессора – максимум 40 мс.

Время обработки информации агентом для всех параметров, кроме комплексных (обнаружение аномалий и вторжений), составляет менее 20 мс. В рамках этого процесса фактически выполняются 10–20 тактов арифметических операций, а также формирование и отправка UDP-пакета.

Время нотификации определяется исключительно загруженностью сети и временем реакции ПО оператора на получение пакета по протоколу взаимодействия с системой мониторинга.

Интенсивность обмена трафиком.

Агентский трафик (в среднем в секунду), байт:

$$T_a = \sum_{j=1}^{N_n} \sum_{i=1}^{N_j} \frac{110}{t_i},$$

где N_n – количество узлов; N_j – количество анализируемых параметров узла j ; t_i – время опроса параметра i .

График уведомлений:

– 1500 байт при каждом событии, когда происходит уведомление ПО оператора;

– 1500 байт · N · N_n – при выполнении полного опроса узлов СООДУ.

Трафик загрузки отчетов (графиков): 1 Мбайт на страницу с графиками.

Таким образом, в данной статье описана архитектура подсистемы мониторинга бортового вычислительного комплекса гидроакустических станций подвижных объектов, разработанная на базе ядра Nagios и оптимизированная для эксплуатации в режиме реального времени. Подробно рассмотрены архитектурные особенности основных компонентов предложенной ПМ СООДУ, представлены оценки потребления аппаратных ресурсов. Особенностью предложенной ПМ является контроль дополнительных характеристик функционирования СООДУ: отслеживание аномального поведения комплекса и контроль целостности сетевой инфраструктуры.

Работа выполнена в СПбГЭТУ при финансовой поддержке Министерства образования и науки Российской Федерации в рамках договора № 02.G25.31.0058 от 12.02.2013 г.

СПИСОК ЛИТЕРАТУРЫ

1. Иванов А. И. Отказоустойчивый программно-аппаратный комплекс мониторинга для подвижных морских объектов // Подводные исследования и робототехника. 2007. № 4 (6). С. 40–46.

2. Большев А. К., Яновский В. В. Применение нейронных сетей для обнаружения вторжений в компьютерные сети // Вестн. С.-Петербург. ун-та. 2009. Вып. 4. С. 128–134.

3. Большев А. К., Яновский В. В. Подход к обнаружению аномального трафика в компьютерных сетях с использованием методов кластерного анализа // Изв. СПбГЭТУ «ЛЭТИ». 2006. № 3. С. 38–45.

4. Большев А. К., Лавров А. А. Метод идентификации версии системного программного обеспечения удаленного сетевого узла, основанный на комплексном анализе характеристик TCP/IP // Изв. СПбГЭТУ «ЛЭТИ». 2012. № 1. С. 45–51.

5. Лавров А. А., Яновский В. В. Идентификация операционной системы удаленного хоста методами анализа временных характеристик // Изв. СПбГЭТУ «ЛЭТИ». 2011. № 3. С. 34–39.

6. Лавров А. А., Лисс А. Р. Метод опорных векторов в задаче идентификации версии операционной системы удаленного узла // Изв. СПбГЭТУ «ЛЭТИ». 2013. № 10. С. 11–15.

A. K. Bolshev, A. A. Lavrov

Saint-Petersburg state electro technical university «LETI»

THE SOFTWARE FOR MONITORING DATA PROCESSING DIGITAL COMPUTING SYSTEM OF HYDROACOUSTIC STATION BASED ON NAGIOS

The features of monitoring board digital computing systems and role of software for monitoring computing systems of hydroacoustic stations is examined. The real time software for monitoring data processing digital computing system of hydroacoustic station is proposed.

Hydroacoustic data processing digital computing systems, network monitoring, Nagios

УДК: 20.53.19, 28.23.13

И. И. Холод

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Архитектура «облака» интеллектуального анализа данных на основе библиотеки алгоритмов с блочной структурой

Описывается архитектура платформы, интегрирующая в себе технологии интеллектуального анализа данных и облачных вычислений. Предлагается построение «облака» интеллектуального анализа данных на базе библиотеки алгоритмов интеллектуального анализа данных, построенных на принципах функционально-блочной структуры.

Облако интеллектуального анализа данных, интеллектуальный анализ данных, облачные вычисления, интеллектуальный анализ распределенных данных

За последние десятилетия в результате повсеместного использования информационных технологий у человечества накоплены огромные объемы данных. Эти данные содержат множество полезной информации, анализ которой позволяет переосмысливать пройденный путь и правильно выбирать дорогу в будущем. Неудивительно, что в последнее время бурно развивается технология интеллектуального анализа данных. Основным преимуществом данной технологии является извлечение из данных более сложных (по сравнению

с математической статистикой) видов закономерностей, скрытых в данных, но при этом более понятных человеку. Наибольший эффект от методов интеллектуального анализа достигается при их применении к большим объемам данным. Это требует больших объемов памяти хранилищ и высокой производительности аппаратной составляющей, на которой хранятся и обрабатываются данные. Наиболее эффективным способом решения этой проблемы является распараллеливание алгоритмов интеллектуального анализа и выпол-