

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Сигаев А.* Embedded Internet // Компоненты и технологии. – 2000. – № 2.
2. *Зубинский А.* МикроWeb // Компьютерное Обозрение. – 2000. – № 20.

Статью рекомендовал к опубликованию д.т.н., профессор А.М. Белевцев.

Тужилкин Олег Владимирович

Научно-исследовательский институт физических измерений.

E-mail: niifi@sura.ru.

440026, г. Пенза, ул. Володарского, 8/10.

Тел.: 88412591932.

Чувькин Борис Викторович

Пензенский государственный университет.

E-mail: chuvykin_bv@mail.ru.

440026, г. Пенза, ул. Красная, 40.

Тел.: 88412368238.

Tuzhilkin Oleg Vladimirovich

Research Institute of Physical Measurements.

E-mail: niifi@sura.ru

8/10, Volodarskogo Street, Penza, 440026, Russia.

Phone: +78412591932.

Chuvykin Boris Viktorovich

Penza State University.

E-mail: chuvykin_bv@mail.ru.

40, Krusnaya Street, Penza, 440026, Russia.

Phone: +78412368238.

УДК 681.327.8

М.В. Фролова

**ПРИМЕНЕНИЕ ВЕБ-ТЕХНОЛОГИЙ ПРИ РАЗРАБОТКЕ
РАСПРЕДЕЛЕННЫХ СИСТЕМ МОНИТОРИНГА**

Предложена структура построения распределенной системы мониторинга для контроля параметров технически сложных объектов. Для ее реализации предлагается использовать интерфейс Ethernet и миниатюрные веб-серверы в каждом датчике системы мониторинга или блоке сбора данных для создания удаленных измерительных систем. Описан принцип удаленного доступа к данным при помощи веб-технологий. Данное решение позволит добиться увеличения скорости работы измерительных систем, уменьшения их стоимости, размеров и времени, затрачиваемого на настройку систем, а также повышения роли программного обеспечения. Выбраны средства разработки и разработан проект программного обеспечения системы. Предложено несколько вариантов развития данного проекта.

Система мониторинга, программное обеспечение; веб-сервер; протокол связи.

M.V. Frolova

**WEB-TECHNOLOGIES APPLICATIONS FOR DEVELOPMENT
THE DISTRIBUTED MONITORING SYSTEMS**

The structure of the distributed monitoring system for control of technically difficult objects parameters is offered. For its realization it is offered to use interface Ethernet and tiny web-servers in each sensor of monitoring system or the block of data gathering for remote measuring systems creation. The principle of remote data access using web technologies is described. This decision will allow to achieve increase of work speed of measuring systems, decrease of their cost,

sizes and time for systems adjustment and increase of the software role. The development environments are chosen and the system software project is developed. Some variants of this project development are offered.

Monitoring system; software; web-server; communication protocol.

На текущем этапе развития технологии создания систем измерения, а также самих объектов измерения, все более актуальной становится проблема обеспечения одновременного контроля большого количества параметров измерения, в частности проведение контроля параметров технически сложных объектов. В результате чего возникает потребность в определенном классе систем измерения – систем мониторинга, основным отличием которых от традиционных измерительных систем является возможность использования различных типов датчиков без изменения общей структуры измерительной системы и наличие средств управления данными от этих датчиков, что позволяет системе адаптироваться к динамически изменяющимся условиям, среди которых могут быть требования к функционалу, отказоустойчивости и масштабируемости системы [1].

Очевидно, что для комплексного выполнения этих требований, а также для возможности адаптации к их изменениям, необходимо применение нового класса инструментов разработки измерительных систем, которые позволят решить основные проблемы создания подобных систем и дополнить список функций системы следующими:

- ◆ передача и управление большим объемом данных, поступающих от нескольких десятков датчиков, входящих в состав данной системы, которые необходимо обрабатывать и передавать с большой скоростью;
- ◆ хранение данных для проведения анализа в случае отказов;
- ◆ удаленный доступ к данным вне зависимости от положения системы.

В данной работе предлагается архитектура распределенной системы мониторинга, которая позволяет обеспечить выполнение перечисленных требований и описываются этапы разработки основных ее элементов, в частности программного обеспечения.

Данная система мониторинга предназначена для удаленного доступа к информации о состоянии технически сложных объектов по каналу Ethernet. Система позволяет следить в реальном времени за состоянием объекта наблюдения, анализировать причины неполадок, а также настраивать систему на выполнение специальных действий при наличии событий определенного типа. Основная идея построения распределенной системы мониторинга заключается в объединение географически распределенных объектов мониторинга и множества пользователей, имеющих доступ к информации по этим объектам через интерфейс Ethernet.

Для решения данных задач в этой работе предлагается использовать интерфейс Ethernet и миниатюрные веб-серверы в каждом датчике системы мониторинга или блоке сбора данных для создания удаленных измерительных систем. Данное решение позволит добиться увеличения скорости работы измерительных систем, уменьшения их стоимости, размеров и времени, затрачиваемого на настройку систем, а также повышения роли программного обеспечения (ПО). С точки зрения изменения структуры измерительной системы это влечет включение в состав системы кроме датчиков, цифровых преобразователей и других элементов – специализированный компьютер (сервер), решающий задачи по управлению данными системы, связанные с приемом, хранением, обработкой и анализом данных в режиме реального времени, а также представления их пользователем в наиболее удобном виде. При этом датчики в составе подобной системы мониторинга с Ethernet – интерфейсом могут подключаться или прямо к компьютеру через обычную сетевую карту, или к компьютерной сети.

Преимущества удаленного управления через Ethernet:

- ◆ управляющая система не привязана пространственно к исполнительным устройствам и датчикам, вследствие чего появляется возможность создания распределенной системы управления;
- ◆ в большинстве случаев отсутствует необходимость прокладки дополнительной кабельной сети для связи компонентов системы;
- ◆ отсутствие необходимости написания специального программного обеспечения (для управления системой можно использовать веб-браузер) [2].

Коммуникация по интерфейсу Ethernet осуществляется со скоростью 10/100 Мбит/с через ТСР/ІР-протокол. Благодаря этому представляется возможным взаимодействовать с датчиками из любой операционной системы с помощью подходящей программы или с помощью обычных текстовых команд. ІР-адрес, как и другие параметры (параметры настройки датчиков), записаны в flash-память датчика и позволяют себя легко изменять. Таким образом, предоставляется возможность с помощью одного стандартного браузера из любой точки получать данные о контролируемом объекте и настраивать, и программировать датчики системы мониторинга, а применение обычных сетевых карт и отсутствие необходимости в сложном ПО, снижает затраты на проектирование и интеграцию оборудования при разработке.

При разработке концепции построения системы мониторинга было выделено 3 основных объекта:

1. Объект мониторинга – фактически это часть системы, которая представляет основной интерес в задаче мониторинга. Объект задается несколькими динамическими параметрами, характеризующими его состояние. Для регистрации значений этих параметров на объекте мониторинга распределена удаленная измерительная система, состоящая из разных типов датчиков. Датчики в системе могут быть управляемыми, в этом случае возможна настройка датчиков системе удаленным пользователем.

2 Ядро системы мониторинга (сервер) – это некоторая программно-аппаратная часть системы, обеспечивающая хранение информации мониторинга, а также взаимодействие клиентов и объектов мониторинга.

3. Клиент системы – часть системы, которая является конечным получателем информации по мониторингу. Клиенты могут выполнять также удаленную настройку системы.

Таким образом, основываясь на данной идеи построения, можно предложить структуру системы мониторинга технически сложных объектов (рис. 1), основными элементами которой являются:

- ◆ датчики;
- ◆ блок сбора данных с микро-веб-сервером, предназначенный для сбора данных и преобразования в пакеты в соответствии с протоколом ТСР/ІР или коммутатор (для случая установки микро-веб-сервера в датчике);
- ◆ сервер системы мониторинга, обеспечивающий хранение данных и взаимодействие пользователя системы с данными;
- ◆ веб-ресурс системы мониторинга, позволяющий получить доступ к данным о контролируемом объекте, о настройках самой системы и настройках датчиков, входящих в состав данной системы.

В системе можно выделить 3 уровня иерархии:

1. Уровень объекта. Уровень объекта представляет собой удаленную измерительную систему, состоящую из нескольких десятков датчиков, распределенных по объекту измерения – технически сложному объекту. Функциями данного уровня являются регистрация данных датчиками, первоначальная их обработка, сжатие и передача по высокоскоростному каналу передачи данных.

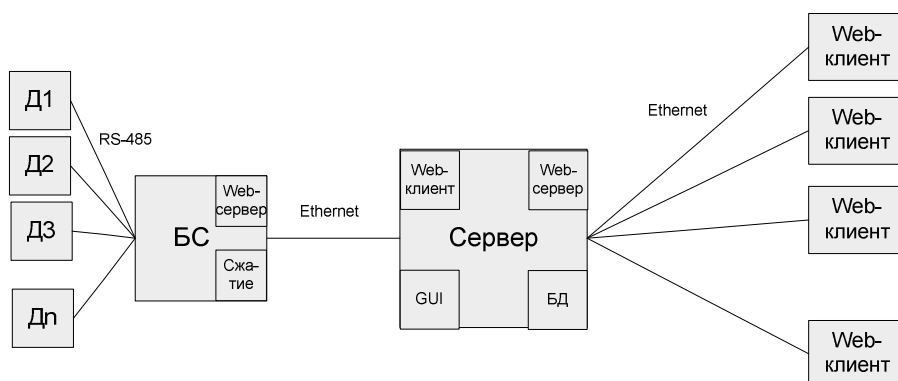


Рис. 1. Структура системы

Основной проблемой данного уровня является объединение данных от нескольких датчиков в один высокоскоростной цифровой информационный поток. В качестве варианта ее решения может быть использован блок сбора данных, представляющий собой многоканальный вторичный преобразователь сигналов датчиков, который осуществляет прием нескольких аналоговых сигналов, их преобразование в цифровую форму, сжатие и объединение в один информационный поток согласно выходному интерфейсу. В рамках данной работы был проведен анализ этой проблемы и разработана модель в среде Simulink(Matlab), имитирующая работу блока сбора данных от датчиков и формирование Ethernet-пакетов (рис. 2).

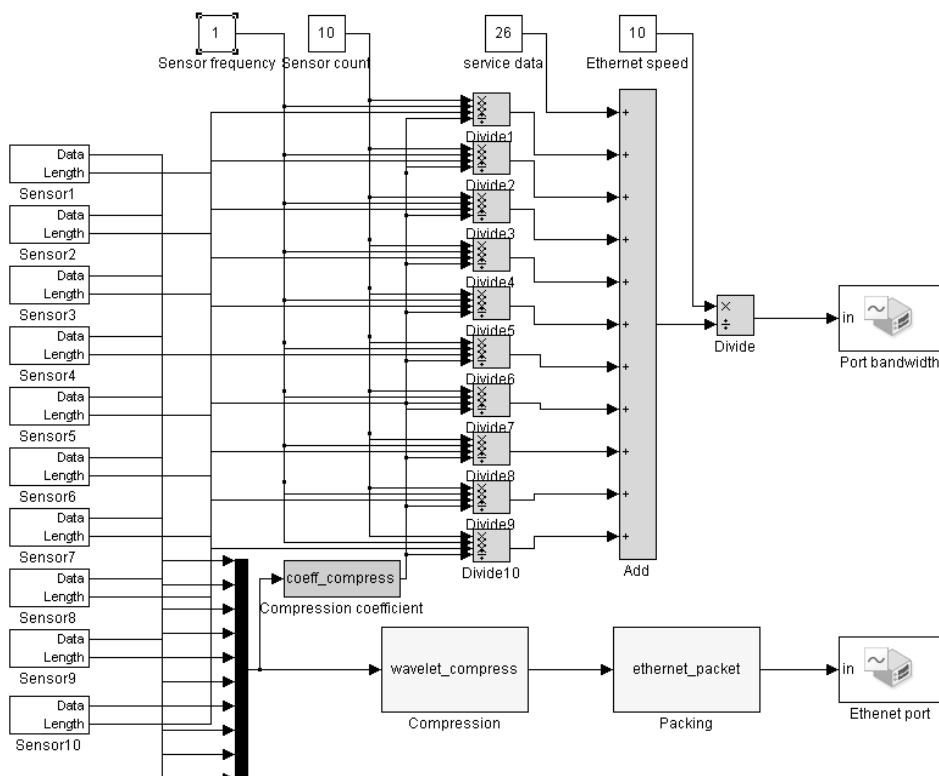


Рис. 2. Модель блока сбора данных системы мониторинга

В результате проведенного исследования была получена зависимость полезной пропускной способности блока сбора от количества датчиков в системе и частоте их опроса (рис. 3), была математически обоснована необходимость применения сжатия данных в блоке сбора данных системы.

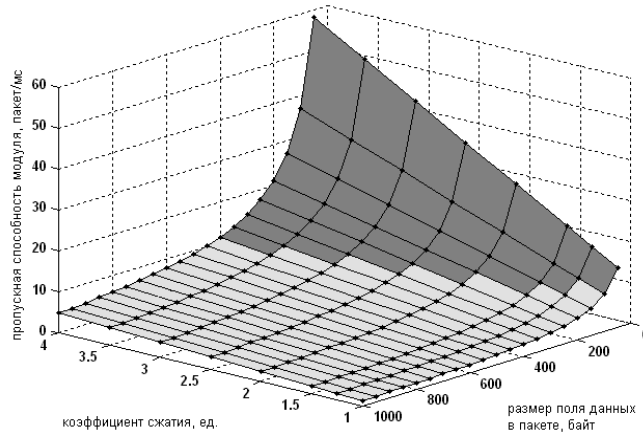


Рис. 3. Результаты моделирования

В качестве средства взаимодействия по интерфейсу Ethernet на уровне объекта предлагается использовать встроенные в датчик или блок сбора данных микро-веб-сервер, функциями которого являются прием запроса от сервера по TCP/IP (HTTP) и отсылка данных на сервер по TCP/IP (HTTP).

2. Уровень сервера. Основной компонент сервера системы мониторинга – это серверное ПО, позволяющее объединять множество удаленных объектов мониторинга и конечных пользователей в единую информационную сеть. ПО включает сервер приложений, веб-сервер (для обращения клиентов к системе) и базу данных.

Основными функциями данного уровня являются прием данных с удаленной измерительной системы, расположенной непосредственно на объекте; архивирование данных – ведение баз данных регистрируемых датчиками данных; обработка и анализ принимаемых данных согласно требованиям; выборка и предоставление данных удаленным клиентам.

3. Уровень удаленного клиента. В качестве удаленного клиента может выступать пользователь удаленного компьютера, который при помощи стандартного веб-браузера через сеть Intranet/Internet желает получить доступ и выборку данных на сервере системы мониторинга, или удаленный АРМ (автоматизированное рабочее место) подсистемы мониторинга для получения данных конкретной подсистемы мониторинга. Пользователь системы мониторинга имеет возможность доступа при помощи веб-браузера ко всей информации по мониторингу объектов доступной этому пользователю.

На каждом из перечисленных уровней основные функции системы мониторинга, которые отличают ее от традиционной измерительной системы, реализуются при помощи программного обеспечения. При этом основная сложность состоит в реализации серверного ПО и ПО блока сбора данных, так как на них возложена большая часть выполнения данных функций. В заключительной части данной работы предложен один из вариантов реализации программного обеспечения для распределенной системы мониторинга (рис. 4).

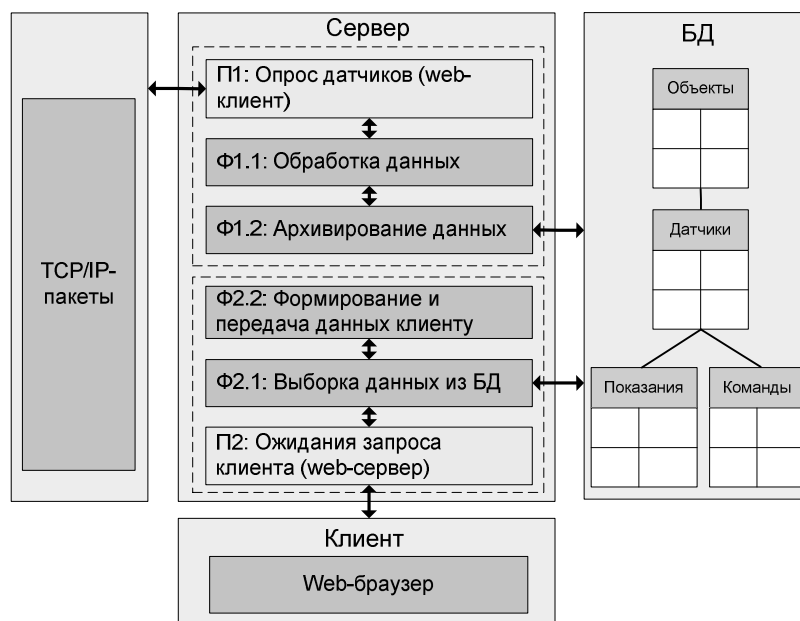


Рис.4. Структура и функции ПО системы мониторинга

ПО блока сбора данных должно обеспечивать прием и преобразование данных от датчиков в TCP/IP-пакеты, а также прием команд настройки датчиков от сервера. Для их реализации было решено использовать интегрированный микро-веб-сервер, предоставляющий для приемопередачи пакетов два TCP/IP-сокета [3]. Частота считывания информации из датчиков зависит от ширины полосы пропускания и загруженности сети. Также интегрированный микро-веб-сервер, базируясь на TCP/IP-протоколе, может также представляет привычные и удобные HTML-веб-страницы взаимодействовать через HTTP-Protocol с ПО сервера.

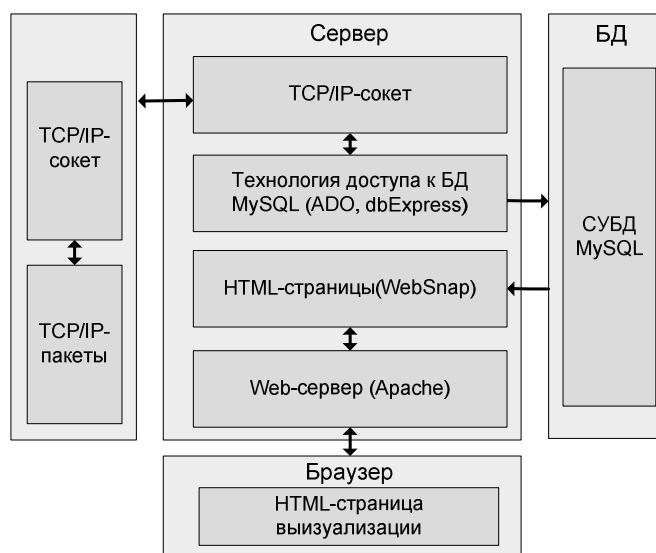


Рис. 5. Средства реализации ПО системы мониторинга

ПО сервера реализует в отличие от ПО блока сбора данных сразу несколько функций: обмена пакетами с блоком сбора данных при помощи TCP/IP-сокета (прием данных и настройка датчиков), хранение данных в БД (в качестве СУБД была выбрана MySQL и технология доступа dbExpress), формирование HTML-страниц (технология WebSnap) и предоставление их удаленному клиенту (веб-браузер). Связь с веб-браузером организована через стандартный веб-сервер Apache.

Таким образом, в результате проведенной работы с целью проверки гипотезы о практической возможности создания распределенной системы мониторинга, была предложена структура системы мониторинга, разработана ее модель в среде Simulink(Matlab), выбраны средства ее разработки и разработан программный комплекс, реализующий проект рассмотренной архитектуры. Опытные результаты эксплуатации прототипа показали его работоспособность и эффективность.

Можно выделить несколько путей развития данного проекта: полнофункциональная реализация предложенной архитектуры распределенной системы мониторинга или реализация данного подхода и прикладного интерфейса программирования для создания отдельных датчиков с веб-интерфейсом, каждое из которых является весьма перспективным.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Таненбаум Э., Ван Стеен М. Распределенные системы. Принципы и парадигмы. – СПб.: Питер, 2003. – 877 с.
2. Сигаев А. Embedded Internet // Компоненты и технологии. – 2000. – № 2.
3. Зубинский А. МикроWeb // Компьютерное обозрение. – 2000. – № 20.

Статью рекомендовал к опубликованию д.т.н., профессор В.В. Тютиков.

Фролова Марина Владимировна

Научно-исследовательский институт физических измерений.

E-mail: niifi@sura.ru, fro-mi2@yandex.ru.

440026, г. Пенза, ул. Володарского, 8/10.

Тел.: 88412591932.

Frolova Marina Vladimirovna

Research Institute of Physical Measurements.

E-mail: niifi@sura.ru, fro-mi2@yandex.ru.

8/10, Volodarskogo Street, Penza, 440026, Russia.

Phone: +78412591932.

УДК 004.021

Р.Н. Селин, С.А. Чурилов

МОДЕЛЬ СЕТЕВЫХ ПРОЦЕССОВ И АЛГОРИТМ ОБНАРУЖЕНИЯ УГРОЗ В КОМПЬЮТЕРНОЙ СЕТИ

Представлена модель сетевых процессов и алгоритм обнаружения угроз в компьютерной сети, предназначенные для прогнозирования изменения уровня информационной безопасности в зависимости от происходящих сетевых событий. Авторы предлагают новый способ моделирования механизма угроз информационной безопасности, который позволяет предугадывать различные варианты развития компьютерных атак. С помощью приведенной модели решаются задачи прогнозирования компьютерных атак с целью их предотвращения.

Информационная безопасность; модель; сетевой процесс; уязвимость; обнаружение угроз.