

**А. С. Богданов<sup>1</sup>, Е. В. Кадывкина<sup>1</sup>**

<sup>1</sup>АО «Научно-производственное предприятие «Радар ммс»

# МЕТОДЫ МОНИТОРИНГА И ДИАГНОСТИКИ РАБОТОСПОСОБНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

*Рассмотрены вопросы управления информационной инфраструктурой предприятия, где мониторинг информационных систем является неотъемлемой частью процесса непрерывного наблюдения и отслеживания динамики происходящих изменений. Предложена трехуровневая логическая структура комплексной системы мониторинга с составными элементами, реализующими мониторинг сетей, серверов и рабочих станций, приложений. Проведен сравнительный анализ принципиальных решений в области мониторинга, выявлены их достоинства и недостатки. Также определены цели инструментов мониторинга, рассмотрены положительные и отрицательные стороны готовых программных продуктов и предложена индивидуальная адаптация решений. Рассмотрены параметры оценки продукта, в числе которых: соответствие архитектуры и технологии требованиям к нагрузке системы, стоимость решений, затраты, шифрование персональных данных. Указаны принципы оценки работоспособности разработанной системы мониторинга информационной системы.*

**Ключевые слова:** мониторинг сети, мониторинг серверов, комплексная система мониторинга

## Введение

Мониторинг информационных систем является составной частью процесса управления информационной инфраструктурой предприятия. Процесс мониторинга представляет собой непрерывное наблюдение и отслеживание динамики изменений, происходящих в информационной инфраструктуре путем проведения периодического анализа ее объектов [1]. К основным задачам систем мониторинга относят получение, сохранение и анализ данных о состоянии элементов информационной инфраструктуры предприятия. Специальные программы в области мониторинга и диагностики работоспособности информационных систем направлены на оперативное реагирование при возникновении проблем в работе информационных сервисов и эффективное устранение возникших неполадок.

## Организационная структура комплексной системы мониторинга

Организация полноценного мониторинга информационных систем предусматривает использование системы, которая дает возможность отслеживать состояние аппаратных и программных составляющих. На рис. представлена логическая структура комплексной системы мониторинга [2], включающая три взаимосвязанных уровня.

Рассмотрим составные элементы комплексной системы мониторинга.

Мониторинг сетей включает следующие функции:

- мониторинг IP-сетей – построение и отображение топологии сетей;
- сбор, последующую обработку данных и формирование сообщений о проблемах;
- мониторинг производительности сетевых интерфейсов и устройств, т.е. сбор статистических данных по загрузке и числу ошибок;
- формирование отчетности и прогнозов;
- управление конфигурациями сетевого оборудования, т.е. автоматизацию управления.

Мониторинг серверов и рабочих станций включает следующие функции:

- мониторинг производительности серверов – получение данных о различных параметрах производительности, создание графических отчетов;
- мониторинг аппаратных сбоев, т.е. получение данных о сбоях в аппаратном обеспечении серверов;
- мониторинг сбоев в операционной системе – получение данных о работе операционной системы с помощью определенных параметров.

Мониторинг приложений и сервисов включает следующие функции:

- активный мониторинг программ и сетевых сервисов, т.е. получение данных об уровне их



Рисунок. Система комплексного мониторинга

доступности и производительности с помощью активных мониторов;

- мониторинг сбоев в программах – сбор и отображение сведений о работе различных приложений (с помощью использования определенных параметров);
- мониторинг производительности приложений, т. е. наблюдение за временем выполнения различных транзакций и за ресурсами приложений;
- мониторинг сервисов – создание сервисно-ресурсной модели, отражение данных в форме иерархически связанной структуры и предоставление информации о протекании данных процессов.

Современные сети состоят из физических, виртуальных и облачных серверов, а также могут включать устаревшие серверы, работающие параллельно друг с другом. Для современного рынка характерно непрерывное развитие микросервисов. Сетевая инфраструктура постоянно усложняется, при этом мониторинг сетей, серверов и приложений имеет решающее значение для обеспечения безопасности, соответствия определенным требованиям, быстроты устранения неполадок и использования разумных бизнес-решений.

### Выбор решения в области мониторинга серверов

Решения в области мониторинга серверов делятся на использующие агенты и безагентные. Агент в данном случае – это программа, которая выступает посредником между системой мониторинга и наблюдаемым объектом. В случае когда выбор одного из типов системы не может полностью решить поставленную на предприятии задачу, возможно использование обоих вариантов.

Преимуществом безагентного решения является уменьшение накладных расходов, однако, такая реализация технически не может получать данные с целевых серверов с интервалом в одну секунду. В некоторых случаях такая скорость получения данных является необходимым условием, например, в приложении для торговли акциями, где учитываются все пики центрального процессора (ЦП), памяти и дискового ввода-вывода.

Краткое сравнение решений для мониторинга серверов на основе агентов и безагентных представлено в табл.

Оба подхода имеют свои достоинства и недостатки. Развертывание системы мониторинга на основе агента не требует значительных инвестиций в ресурсы или затрат по сравнению с развертыванием самого агента. Возможны трудности с получением прав доступа для установки агента. В правительственной или крупномасштабной системе развертывание на основе агентов может занять много времени, если требуется реализовывать большое число разрешений и испытаний. Для обслуживания агентов также потребуется дополнительное время. Кроме того, затруднения возможны, если развертывание, подключение, управление и администрирование охватывают большое количество клиентов и серверов.

Окончательное решение о выборе подхода должно зависеть от потребностей клиента. Сочетание мониторинга сетей с агентами и без таковых зачастую может обеспечить реализацию наилучшего баланса функций и затрат.

В последнем отчете по мониторингу сети от Markets & Markets говорится, что рынок мониторинга сети вырастет с 1,82 млрд долл. США в 2018 г. до 2,93 млрд долл. США к 2023 г. при CAGR 9,9% с 2018-го по 2023 г. [3]. Рынок сетевого

Таблица. Сравнение решений для мониторинга серверов на основе агентов и безагентных

Параметр	Мониторинг на основе агентов	Безагентный мониторинг
Простота развертывания	Агент должен быть развернут на каждом сервере	Простое развертывание, так как программное обеспечение устанавливается только на удаленный сборщик данных
Продолжительность цикла опроса данных	1 с (может использоваться для чувствительных серверов ввода-вывода и компонентов приложений)	Не менее 60 с (большая вероятность потери любого критического скачка, который может произойти в течение 60-секундного окна цикла опроса)
Технология мониторинга	.Net (PowerShell / WMI) / Python / Java / Go агенты	SNMP / PowerShell / WMI / SSH и т. д.
Безопасность	Высокая безопасность. Связь между агентом и приложением/ операционной системой обрабатывается внутри сервера, следовательно, нет необходимости настраивать дополнительные правила брандмауэра	Менее безопасный, потому что удаленному сборщику данных должно быть разрешено обмениваться данными с целевой системой через разные порты. Может возникнуть необходимость установки коллектора данных с правами администратора домена, чтобы иметь возможность доступа к удаленным системам
Сетевые ресурсы	Очень эффективная полоса пропускания, поскольку данные собираются локально, и только обработанные конечные результаты передаются на консоль	Возникает дополнительный сетевой трафик, поскольку необработанные данные о производительности передаются на удаленный сборщик данных. Реализуется двустороннее общение
Серверные ресурсы	Агент развертывается на целевом сервере – при сборе локальных данных он будет использовать ЦП, а также малый объем памяти. Затраты ресурсов зависят от настроек частоты сбора данных	Нет постоянных затрат ресурсов на целевом сервере. ЦП сервера используется по мере поступления запросов
Затраты на внедрение	Косвенные затраты на инфраструктуру, необходимую для поддержки агента	Отсутствие дополнительных прямых или косвенных затрат
Мониторинг покрытия	Обеспечивается глубокий и широкий мониторинг	Может быть ограничен, потому что не все приложения и системы имеют встроенные возможности мониторинга

мониторинга развивается благодаря наличию множества решений, которые предлагают широкий спектр возможностей. В этих условиях понимание и сопоставление этих возможностей с потребностями предприятия, оценка лучших из доступных инструментов нишевого рынка имеют первостепенное значение.

Цель инструментов мониторинга сети состоит не только в том, чтобы предупреждать и уведомлять IT-администраторов о возникновении проблем в сети, но и в том, чтобы показать тенденции изменения производительности IT-сети и помочь им в достижении SLA (Service Level Agreement).

#### Особенности сетевого мониторинга

Построение и функционирование систем мониторинга имеют ряд особенностей.

Во-первых, некоторые решения для мониторинга сети предлагают базовые функции отчетности, в то время как другие поставляются с заранее определенными, простыми в использовании шаблонами. Задача IT-администратора в каждом конкретном случае состоит в том, чтобы сделать выбранный инструмент полезным. При этом необходимо настроить или отрегулировать решение для мониторинга на основе IT-процессов и сетевой архитектуры конкретной организации. Важной составляющей этого процесса является понимание того, как устройства разных производителей или разных типов интегрируются с инструментом мониторинга сети.

Во-вторых, инструменты должны сообщать о проблемах, с которыми может столкнуться устройство, а также о его состоянии и производительности. Для каждого отслеживаемого сетевого

устройства уровень уведомлений может достигать точки, в которой важные сообщения теряются в потоке бесполезного шума. Это делает практически невозможным точно определять важные проблемы и передавать значимую информацию пользователю. В этом случае необходимо найти решение, которое поддерживает устройства разных производителей и несколько протоколов.

В-третьих, IT-администраторы должны быть знакомы с функционалом, включенным в пакет. Обычно инструменты обрабатывают, а затем архивируют IT-данные, собранные с разных устройств. Многие решения могут оценивать состояние сетевого устройства в режиме реального времени, одновременно поддерживая архив данных. В некоторых случаях в режиме реального времени можно отслеживать только часть элементов, что приводит к необходимости выбора того, какие элементы являются критически важными с расстановкой приоритетов. Инструменты, которые в основном формируют предупреждения и уведомления о состоянии сети, обычно архивируют машинные данные.

Индивидуальная адаптация решения в соответствии с инфраструктурой и потребностями клиента обеспечит лучший результат и оптимальную производительность сети.

В настоящее время мониторинг сети стал основой любой организации, ключом к обеспечению требуемого времени безотказной работы, улучшению контроля ИТ-инфраструктуры, анализу событий в области безопасности и уменьшению простоев в будущем.

Решения для мониторинга и диагностики информационных систем предприятия можно создать силами штатных или привлекаемых под проект разработчиков. Также можно приобрести готовое решение, настроив его с использованием встроенного инструментария и подключаемых модулей, либо выбрать доработанный сторонними разработчиками API, хотя такой подход требует дополнительных финансовых затрат.

Преимущества готовых программных продуктов обусловлены их быстрым включением в бизнес-процессы предприятия, использованием готового пользовательского интерфейса и интеграцией с различными сервисами, а также экономией на аналитической фазе и фазе проектирования базовых сущностей системы. Недостатки связаны с неполным соответствием требованиям, продиктованным конкретным бизнесом, и, как следствие,

необходимостью доработки, а также наличием абонентской платы.

Самым эффективным, но дорогостоящим способом реализации и внедрения комплекса мониторинга и диагностики информационных систем предприятия является создание собственного отдела разработчиков. Для получения максимальной отдачи от такого отдела необходимо грамотно его структурировать, контролировать ключевые процессы разработки (анализ, проектирование, программирование, документирование, тестирование), выбрать методологию разработки (Agile, RUP, OpenUP). Самостоятельная разработка системы мониторинга и диагностики работоспособности требует высокой квалификации сотрудников.

При выборе готового продукта оценке подлежат не только функциональность, но и другие параметры:

- соответствие архитектуры и технологии требованиям к нагрузке на систему (высоконагруженные системы нуждаются в индивидуальных решениях);
- стоимость решения с учетом абонентской платы. Например, для малого и среднего бизнеса на рынке представлены решения стоимостью от 140 тыс. руб. (абонентская плата от 30 тыс. руб. в год). Для крупного бизнеса (банкинг, оптовая торговля и т.д.) актуальны коробочные решения стоимостью от 6 млн руб. (абонентская плата от 1 млн руб. в год плюс стоимость подключаемых модулей);
- затраты, обусловленные применением той или иной технологии (например, стоимость разработки, внедрения, дальнейшей поддержки и развития системы);
- наличие шифрования персональных данных (особенно актуально для облачных решений), открытого кода и возможности доработки решения.

### Выводы

За последнее десятилетие создано множество программных продуктов в области мониторинга и диагностики работоспособности автоматизированных систем управления предприятием, однако единого подхода к выбору соответствующего решения пока не выработано. Причиной этому является уникальность каждой информационной системы, обусловленная уникальностью каждого объекта автоматизации.

## СПИСОК ЛИТЕРАТУРЫ

1. Комплексные системы мониторинга работоспособности ИТ-систем. ИТ-консалтинг [Электронный ресурс]. URL: [http://www.topsbi.ru/services/sistemy\\_upravleniya\\_it-resursami\\_i\\_it-uslugami/monitoring\\_i\\_upravlenie\\_komponentami\\_it-infrastruktury](http://www.topsbi.ru/services/sistemy_upravleniya_it-resursami_i_it-uslugami/monitoring_i_upravlenie_komponentami_it-infrastruktury) (дата обращения: 21.05.2019).

2. Шевченко А.Л. Организации мониторинга функционирования корпоративных информационных систем // Молодой ученый. 2010. № 4. С. 109–113 [Электронный ресурс]. URL: <https://moluch.ru/archive/15/1415> (дата обращения: 27.05.2019).
3. Network Monitoring: Expectation vs Reality [Электронный ресурс]. URL: <https://www.motadata.com/blog/network-monitoring-expectation-vs-reality> (дата обращения: 27.05.2019).

## ИНФОРМАЦИЯ ОБ АВТОРАХ

**Богданов Александр Сергеевич**, магистр, АО «Научно-производственное предприятие «Радар ммс», Российская Федерация, 197375, Санкт-Петербург, ул. Новосельковская, д. 37, лит. А, тел.: 8 (921) 877-10-24, e-mail: [vrontm@gmail.com](mailto:vrontm@gmail.com).  
**Кадывкина Екатерина Валерьевна**, главный специалист, АО «Научно-производственное предприятие «Радар ммс», Российская Федерация, 197375, Санкт-Петербург, ул. Новосельковская, д. 37, лит. А, тел.: 8 (921) 567-89-26, e-mail: [kadyvkina@radar-mms.com](mailto:kadyvkina@radar-mms.com).

---

*For citation: Bogdanov A. S., Kadyvkina E. V. Methods of monitoring and diagnostics of information systems workability. Voprosy radioelektroniki, 2019, no. 9, pp. 42–46. DOI 10.21778/2218-5453-2019-9-42-46*

A. S. Bogdanov, E. V. Kadyvkina

## METHODS OF MONITORING AND DIAGNOSTICS OF INFORMATION SYSTEMS WORKABILITY

There are considered the matters information infrastructure control at the enterprise, where the procedure of information system monitoring is an indivisible part of the process of continuous observation and tracking of current changes. It is proposed a three-level logic structure of complex monitoring system. As the parts of this system there are considered monitoring of nets, servers and working stations, applications and servers. The comparative analysis of principle decisions in the sphere of monitoring is performed, advantages and disadvantages are revealed. The monitoring instruments tasks are defined, positive and negative aspects of complete SW products are considered, individual approach for decision adaptation is proposed. The parameters of product estimation are considered, including: correspondence of architecture and technology to requirements for system load, decisions cost, expenses, personal data encryption, estimation of information system efficiency diagnostics procedure and developed monitoring system is realized.

**Keywords:** net monitoring, servers monitoring, integrated monitoring system

## REFERENCES

1. Integrated systems for monitoring the health of IT systems. IT consulting. (In Russian). Available at: [http://www.topsbi.ru/services/sistemy\\_upravleniya\\_it-resursami\\_i\\_it-uslugami/monitoring\\_i\\_upravlenie\\_komponentami\\_it-infrastruktury](http://www.topsbi.ru/services/sistemy_upravleniya_it-resursami_i_it-uslugami/monitoring_i_upravlenie_komponentami_it-infrastruktury) (accessed 21.05.2019).
2. Shevchenko A. L. Organization for monitoring the functioning of corporate information systems. *Molodoi uchenyi*, 2010, no. 4, pp. 109–113. (In Russian). Available at: <https://moluch.ru/archive/15/1415> (accessed 27.05.2019).
3. Network Monitoring: Expectation vs Reality. Available at: <https://www.motadata.com/blog/network-monitoring-expectation-vs-reality> (accessed 27.05.2019).

## AUTHORS

**Bogdanov Alexander**, master, «NPP «Radar mms» JSC, 37A, Novoselkovskaya St., Saint-Petersburg, 197375, Russian Federation, tel.: +7 (921) 877-10-24, e-mail: [vrontm@gmail.com](mailto:vrontm@gmail.com).

**Kadyvkina Ekaterina**, chief specialist, «NPP «Radar mms» JSC, 37A, Novoselkovskaya St., Saint-Petersburg, 197375, Russian Federation, tel.: +7 (921) 567-89-26, e-mail: [kadyvkina@radar-mms.com](mailto:kadyvkina@radar-mms.com).