*Игорь Афонин*

# Решение AdvantiX Intellect для обеспечения высокой доступности информационных систем

**Статья даёт общее представление о высокой доступности информационных систем, обслуживающих современные производственные процессы, о её влиянии на совокупную стоимость владения и методах достижения. Описывается отказоустойчивая система на базе решения AdvantiX Intellect, обеспечивающего её высокую доступность, приводятся основные особенности и преимущества данного решения.**

## Введение

Обеспечение высокой доступности информационной системы является одним из главных требований для непрерывности производственных процессов компаний любого масштаба и автоматизации различных уровней: систем телемеханики, SCADA и MES, диспетчерских и ERP-систем.

Выбор стратегии обеспечения высокой доступности напрямую зависит от специфики производства. Прежде всего, на выбор влияют ущерб от простоя и максимально допустимое время простоя, а также временной режим функционирования (например, 8/5 – 8 часов в день и 5 дней в неделю или 24/7 – 24 часа в день и 7 дней в неделю). Так, для точки розничной торговли и предприятия с непрерывным производственным циклом стоимость простоя может отличаться в несколько раз. Более того, отказ информационной системы на критически важных производствах влияет на безопасность технологических процессов и может привести к невосполнимым потерям.

## Основные понятия

Высокая доступность (High Availability) и отказоустойчивость (Fault Tolerance) – не одно и то же. Понятие «высокая доступность» значительно шире и более значимо, хотя понятие «отказоустойчивость» часто используется как его синоним, чтобы показать, как реализуется высокая доступность.

Отказоустойчивые решения – это аппаратно-ориентированные системы, использующие специализированные аппаратные средства для обнаружения ошибок и мгновенного переключения на резервный компонент оборудования. Применительно к информационным системам этим компонентом может быть процессор, память, системная плата, блок питания, подсистемы ввода/вывода или подсистемы хранения. Возможность перехода на дублирующий компонент обеспечивает высокий уровень отказоустойчивости.

Решения высокой доступности используют различные комбинации стандартного оборудования и программного обеспечения, сводя к минимуму время простоя (Downtime) и восстановления (Recovery), когда система или её часть выходит из строя. Достигается высокая доступность комплексным организационно-техническим подходом, в который вовлечены технологии, процессы и специалисты.

Доступность рассчитывается на основе характеристик надёжности по следующей формуле:

$$Av = MTBF / (MTBF + MTTR), \quad (1)$$

где MTBF (Mean Time Between Failures) – среднее время между сбоями (характеризует способность системы не быть подверженной сбоям);

MTTR (Mean Time To Recover) – время восстановления (характеризует способность системы восстанавливаться после сбоев).

В сфере информационных технологий мера высокой доступности определяется как процент времени, когда система доступна, и выражается количеством девяток, начиная с одной (90%). Если система работает 90% времени, то её доступность – одна девятка; если доля времени работы достигает 99%, то доступность выражается двумя девятками и т.д. Табл. 1 определяет время простоя за год при доступности, характеризуемой разным количеством девяток.

## Способы обеспечения высокой доступности

Очевидно, чтобы достичь постоянной доступности ($Av \to 1$), согласно выражению (1), необходимо уменьшать MTTR и повышать MTBF.

*Таблица 1*

**Доступность систем**

| Представление доступности количеством девяток | Доля времени работы в % | Время простоя за год |
|---|---|---|
| 3 | 99.9 | 8,76 часов |
| 4 | 99.99 | 52,56 минуты |
| 5 | 99.999 | 5,26 минуты |
| 6 | 99.9999 | 31,5 секунды |

Уменьшение MTTR обеспечивается, во-первых, сигнализацией для своевременного обнаружения неисправных компонентов и, во-вторых, использованием сменных модулей FRU (Field Replaceable Units) для всех критичных подсистем.

Высокого значения MTBF можно достичь, прежде всего, использованием высоконадёжных компонентов. Но на определённом этапе затраты становятся несоизмеримыми с достигаемым результатом, и дальнейшее повышение надёжности системы уже нецелесообразно без резервирования компонентов.

Для электронных систем в течение полезного срока эксплуатации характерно постоянство величины интенсивности отказов (λ). MTBF связано с ней следующим соотношением:

$$MTBF = 1/\lambda = 1/(\lambda_1 + \lambda_2 + ... + \lambda_i), \quad (2)$$

где $\lambda_i$ – интенсивность отказа $i$-го компонента.

Согласно выражению (2), если существует компонент, интенсивность отказов которого много больше, чем у остальных, то именно он определяет среднее время наработки на отказ всей системы. Это является теоретическим обоснованием принципа резервирования так называемого слабого звена. К этим звеньям обычно относятся высоконагруженные компоненты, такие как блоки питания, диски и вентиляторы. Необходимость их резервирования влечёт за собой некоторую избыточность, что также повышает стоимость системы. Но в связи с тем, что при этом возможно использование менее дорогостоящих компонентов, эффективность данного решения значительно выше предыдущего.

Можно резервировать не только компоненты системы, но и саму систему с помощью специального программного обеспечения, позволяющего объединить в отказоустойчивый комплекс (кластер) стандартные серверы, которые становятся узлами кластера. Узлов может быть более двух. При отказе одного из узлов приложение автоматически запускается на другом, за счёт чего повышается доступность системы, хотя часть данных, находящихся в оперативной памяти, будет потеряна.

И, наконец, для систем, где необходим наивысший уровень готовности и недопустимы потери данных и даже минимальный простой, применяют специальные технические решения, которые обеспечивают непрерывную доступность (Continuous Availability) за счёт дублирования и синхронизации всех компонентов до уровня процессорных тактов и блоков памяти.

Следует отметить, что, условно говоря, каждая девятка значительно повышает стоимость решения (рис. 1).

## Решение AdvantiX Intellect

Построение эффективной и качественной системы высокой доступности представляет собой достаточно сложную задачу, решение которой требует глубоких знаний, опыта и существенных затрат. Самым распространённым способом обеспечения высокой доступности информационных систем является использование отказоустойчивого кластера. Применение данной технологии требует использования высоконадёжной системы хранения данных, создания дополнительной сетевой инфраструктуры и привлечения специалистов высокой квалификации для развёртывания и эксплуатации системы. В качестве альтернативы для широкого круга ответственных применений компания ПРОСОФТ предлагает готовое отказоустойчивое решение нового поколения – AdvantiX Intellect. Решение рассчитано прежде всего на использование в информационных системах автоматизации производственных процессов предприятий любого размера и требует минимальных затрат на обслуживание.

Следует отметить, что в данном решении используются несколько методов повышения доступности, позволяющих системе достичь уровня 99,99+, который раньше могли обеспечить только более дорогие решения:

- во-первых, использование качественных серверных компонентов, отличающихся высокой надёжностью, имеющих высокое значение MTBF и предназначенных для работы в режиме 24/7/365 со 100-процентной нагрузкой;
- во-вторых, резервирование и обеспечение возможности «горячей» замены критически важных компонентов, таких как блоки питания, диски (RAID) и вентиляторы системы охлаждения;
- в-третьих, использование двух серверов стандартной архитектуры Intel x86 с поддержкой IPMI (Intelligent Platform Management Interface), объединённых в двухузловой кластер;
- в-четвёртых, применение виртуализации (Embedded Hypervisor) и специального программного обеспечения мониторинга и управления системой Avance Policy Engine.

Функциональная схема решения приведена на рис. 2. По служебному каналу передаются пакеты, обеспечивающие синхронизацию данных и использующиеся для обнаружения сбоев и управления ресурсами. Данные и приложения непрерывно синхронизируются в реальном масштабе времени между узлами системы. BMC (Baseboard Management Controller) контролирует со-

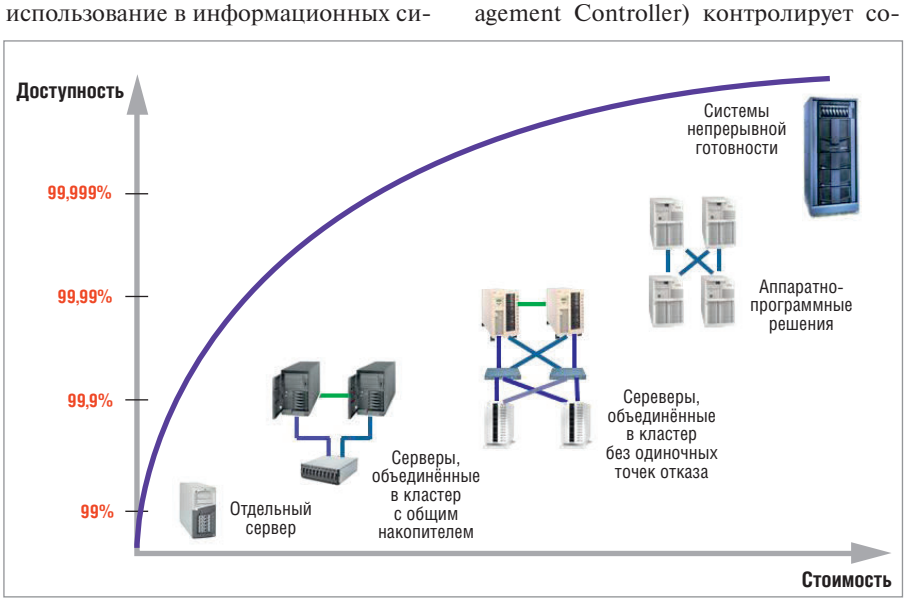
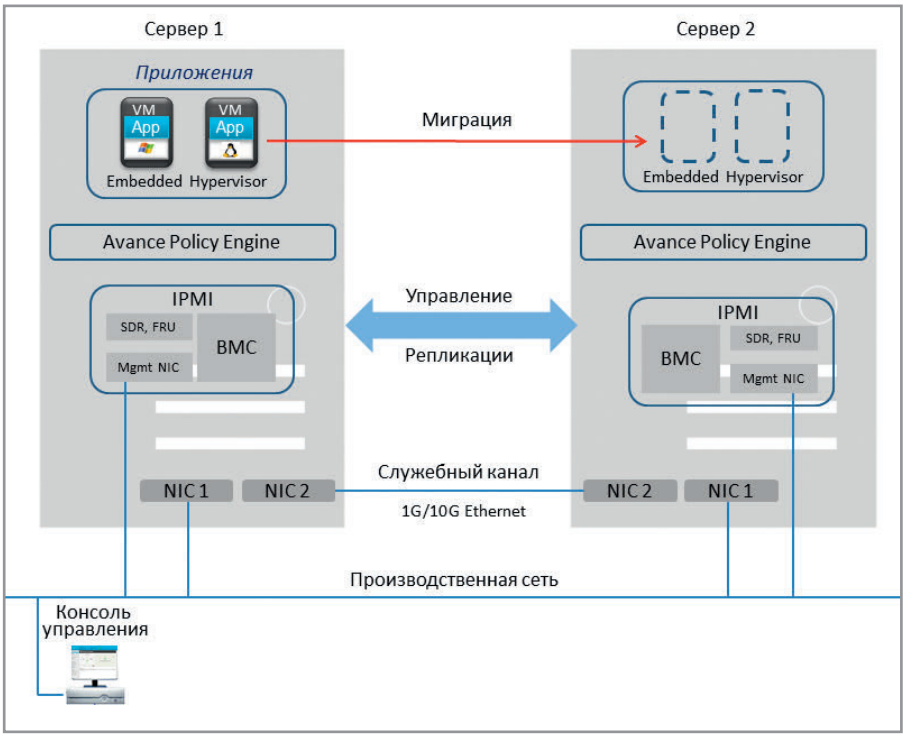



**Рис. 1. Типы серверных систем с разной стоимостью и доступностью**




**Условные обозначения:** BMC (Baseboard Management Controller) – интегрированный контроллер управления; NIC (Network Interface Controller) – сетевой контроллер; Mgmt NIC – сетевой контроллер модуля управления; SDR (Sensor Data Record) – запись о параметрах и состоянии датчика (сенсора); FRU (Field Replaceable Unit) – сменный элемент/модуль.

**Рис. 2. Функциональная схема решения**

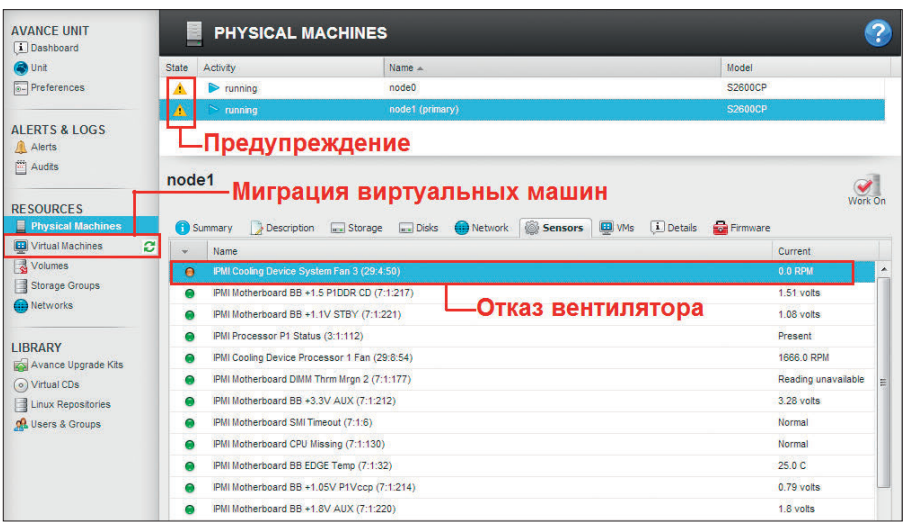



**Рис. 3. Скриншот консоли управления во время обнаружения сбоя на одном из серверов**

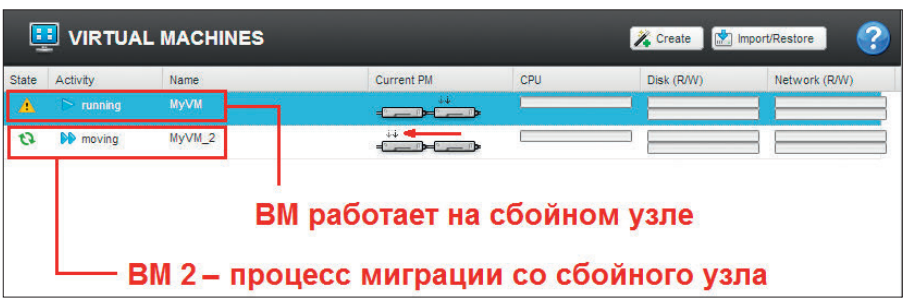



**Рис. 4. Перенос приложений**

стояние системы, сверяя информацию от датчиков с данными SDR (Sensor Data Record), находящимися в его ПЗУ. При возникновении неполадки на одном сервере его функции берёт на себя второй. Всё это происходит автоматически и не требует участия оператора. BMC имеет свой сетевой контроллер, что позволяет управлять сервером без загрузки операционной системы. Предусмотрены удалённое управление через Web-консоль с использованием обычного браузера и поддержка оповещений по электронной почте и протоколу SNMP.

Отличительной особенностью этого решения является не просто автоматическое восстановление системы после сбоя, а предотвращение сбоев, реализуемое проактивным мониторингом.

Традиционные решения по обеспечению высокой доступности контролируют компоненты системы только на наличие обратной связи, и неисправность распознаётся только в том случае, когда они выходят из строя. Взаимодействуя с интегрированным контроллером управления сервера BMC, специальное программное обеспечение выявляет потенциальные неполадки и переносит приложения и данные на неповреждённый сервер. Всё это происходит совершенно незаметно для пользователей. На рис. 3 показан скриншот консоли управления физическими машинами во время обнаружения сбоя на одном из серверов (node 1): отказ вентилятора (System Fan 3) и процесса переноса приложения (миграции виртуальных машин – VM) на второй сервер (node 0). На рис. 4 более подробно изображён процесс миграции виртуальных машин. Виртуальные машины перемещаются поочерёдно. Одна машина находится в процессе переноса (MyVM_2), а вторая (MyVM) пока работает на узле, на котором обнаружен отказ.

Мониторинг производится более чем по 150 параметрам сервера, таким как напряжение питания и температура компонентов, скорость вращения вентиляторов, ошибки чтения/записи памяти и дисковой подсистемы и многим другим. Распознаются даже минимальные отклонения от заданных значений, и происходит быстрое реагирование на них. Наряду с мониторингом всех текущих процессов ведётся база данных прошлых событий и ошибок. Можно отследить любые произошедшие изменения и проанализировать их. Непрерывный контроль выполняемых приложений и аппаратного обеспечения позволяет выявить назревающие проблемы прежде, чем они приведут к сбою (табл. 2).

Для обеспечения защиты от серьёзных внешних воздействий, таких как пожар, вандализм и т.д., предусмотрена возможность раздельной установки серверов – Split Site. Два рабочих сервера

могут находиться на удалении друг от друга, поддерживая связь по сети Ethernet. Для функционирования системы задержки в канале связи не должны превышать 10 мс. Без особых проблем можно обеспечить расстояние между узлами до 5 км.

Система предусматривает удалённое администрирование из любой точки через Web-консоль. С помощью консоли можно управлять физическими и виртуальными машинами, дисковой подсистемой, делать Backup, Snapshot и импорт виртуальных машин, настраивать параметры системы, выводить физические и виртуальные машины на обслуживание, проводить модернизацию системы без её остановки. Простая и интуитивно понятная консоль позволяет избежать многих ошибок операторов и работать, не требуя глубоких знаний в области ИТ-технологий.

Ключевые моменты решения AdvantiX Intellect:

- используются только два стандартных сервера x86, дополнительное аппаратное и программное обеспечение не нужны;
- проактивная диагностика неполадок позволяет предотвратить проблемы и сбои до того, как они повлияют на производственный процесс;
- программное обеспечение ведёт автоматический мониторинг и полное протоколирование событий, происходящих в системе, что позволяет не только постоянно контролировать работоспособность, но и анализировать состояние, прогнозировать и предотвращать сбои;
- система самостоятельно действует при возникновении ошибок и сразу же оповещает ответственных лиц компании и службу поддержки по электронной почте или по протоколу SNMP.

*Таблица 2*

**Примеры неполадок, которые устраняются системой**

| | |
|---|---|
| **Сеть** | Отказ/ошибки сетевого адаптера |
| | Отказ/ошибки сетевого соединения |
| **Дисковая подсистема** | Отказ /ошибки жёсткого диска |
| | Износ жёсткого диска |
| | Отказ/ошибки RAID-массива |
| | Отказ/ошибки RAID-контроллера |
| | Отказ аккумулятора RAID-контроллера |
| **Система охлаждения** | Отказ вентилятора |
| | Выход числа оборотов вентиляторов за допустимые пределы |
| | Нестабильность числа оборотов вентиляторов |
| **Электропитание** | Отказ блока питания |
| | Сбой питания |
| | Провалы/колебания напряжения |
| | Выход значений напряжения за заданные пределы |
| **Температура** | Повышение температуры компонентов системы |
| | Выход за допустимые пределы температуры компонентов системы |
| **Память** | Отказ |
| | Повторяющиеся ошибки памяти |
| **Системная плата** | Одиночные и повторяющиеся ошибки высокоскоростных интерфейсов |
| | Отказ/ошибки контроллера управления |
| **Процессор** | Выход за допустимые пределы напряжения питания и температуры |

## Совокупная стоимость владения

Необходимо остановиться на таком немаловажном и даже во многом определяющем критерии при выборе решения (в данном случае – информационной системы), как совокупная стоимость владения (Total Cost of Ownership – TCO). Этот критерий позволяет оценить затраты, связанные с использованием информационной системы за период её жизненного цикла.

В общем затраты можно разделить на:

- прямые (бюджетные), включающие в себя стоимость аппаратного и программного обеспечения, аренды каналов связи, стоимость электроэнергии и т.д.;
- косвенные, или внебюджетные, получаемые в результате расчётов на основе усреднённых показателей по отрасли и прогнозов (эти затраты, как правило, связаны с конечными пользователями информационных систем, и сюда можно отнести простои, непродуктивную работу и т.д.).

По оценке Gartner Group, первая категория расходов составляет около 20% от общей стоимости затрат на использование информационной системы, то есть обслуживание и поддержка системы в рабочем состоянии обходятся в несколько раз дороже её приобретения. И это – не учитывая затрат на ликвидацию возможных последствий после аварийных сбоев технологических процессов.

Решение AdvantiX Intellect, которое обеспечивает высокую доступность без особых затрат на оборудование, подготовку персонала и поддержание системы в рабочем состоянии, позволяет значительно снизить TCO. Если сравнивать стоимость одного часа простоя предприятия среднего класса с затратами на обеспечение бесперебойной работы, то данное решение является оптимальным выбором.

## Заключение

Всё более усложняющиеся производственные процессы предъявляют самые высокие требования по надёжности к информационным системам, обеспечивающим их реализацию. Цена сбоя и ликвидации его возможных последствий очень высока, поэтому главный принцип развития современных технологий – проактивность, предполагающая необходимость действовать для предотвращения проблем, а не реагировать на их возникновение. Решение AvantiX Intellect полностью соответствует этому принципу. Оно обеспечивает высокую отказоустойчивость при минимальных инвестициях и значительно снижает совокупную стоимость владения.

Данное решение подходит для компаний любого масштаба и с различным уровнем автоматизации производственных процессов.●

**Автор – сотрудник фирмы ПРОСОФТ**
**Телефон: (495) 234-0636**
**E-mail: info@prosoft.ru**