

ПО «ГиперСфера»: обеспечение отказоустойчивости прикладных серверов в системах физической безопасности объектов

Системы физической безопасности объектов, такие как системы противопожарной защиты, охранной сигнализации, видеонаблюдения, контроля доступа, а также смежные, являются неотъемлемой частью любого современного объекта вне зависимости от его размеров и отрасли. Большинство этих систем создаются, проектируются и строятся таким образом, чтобы возможные отказы их ИТ-компонентов (программного и аппаратного обеспечения серверов и АРМ, сетевой инфраструктуры) не приводили к отказу системы в целом. Однако часть функциональности некоторых систем физической безопасности, в частности, систем контроля и управления доступом (СКУД), систем видеонаблюдения, не может быть реализована без бесперебойной работы прикладных серверов этих систем. Технический директор компании «СТР» [Антон Душко](#) рассказывает об этих проблемах и о программном обеспечении «ГиперСфера», предназначенном для создания отказоустойчивости прикладных серверов, об аппаратном обеспечении и компетенциях персонала, требующихся для развертывания отказоустойчивого кластера. ■■■■■

ЦИТАТА: При использовании встроенной или дополнительно реализованной заказной функциональности СКУД, которая не может работать только на полевых контроллерах системы, без участия ПО, отказоустойчивость сервера системы выходит на первый план.

Антон Александрович! В каких случаях в системах контроля и управления доступом (СКУД) необходимо обеспечить отказоустойчивость прикладных серверов?

Обычно к отказоустойчивости сервера СКУД не предъявляется особых требований: полевые контроллеры системы в норме способны самостоятельно принимать решения о разрешении или запрете доступа. В большинстве систем отказ сервера не приводит к отказу СКУД в целом,

а наличие в контроллерах буфера для записи произошедших событий позволяет не терять события при своевременном восстановлении работоспособности сервера.

Но при использовании встроенной или дополнительно реализованной заказной функциональности СКУД, которая не может работать только на полевых контроллерах системы, без участия ПО, отказоустойчивость сервера системы выходит на первый план.

Приведите, пожалуйста, примеры таких дополнительных функций.

Построение точек доступа в особо ответственные зоны объекта зачастую требует дополнительных проверок, которые невозможно осуществить внутри СКУД, потому что необходимо участие персонала службы безопасности или интеграция с дополнительными подсистемами. Например, это может быть точка доступа с дежурным сотрудником службы безопасности, который сверяет фотографию

и данные владельца идентификатора, отображаемые АРМ фотоверификации СКУД, с человеком, фактически использующим идентификатор. Или те же точки прохода, в которых вместо дежурного персонала внедрена дополнительная подсистема видеоверификации, построенная на программном комплексе распознавания лиц. Такие точки доступа не могут полноценно работать при отказе сервера СКУД: АРМ и интеграция с программным комплексом распознавания лиц зависят от сервера системы и не будут работать при его отказе.

Аналогичная ситуация возникает и с программными интеграциями СКУД. Так, если на предприятии сменный график и сотрудники имеют возможность обмениваться сменами, для корректной работы СКУД требуется интеграция с системой управления персоналом, в которую вносятся все сменные графики и их изменения. Зачастую временные зоны получаются слишком сложными для загрузки в полые контроллеры и требуют регулярной коррекции со стороны сервера. А он, в свою очередь, может получить последние изменения в графиках из системы управления персоналом за считанные минуты до начала смены.

Таким образом, для надежной работы СКУД крупных объектов или объектов с повышенными требованиями

к безопасности необходимо обеспечить отказоустойчивость серверной инфраструктуры системы.

Какие из современных систем безопасности объекта наиболее зависимы от отказоустойчивости серверов?

Системы видеонаблюдения. Пожалуй, они являются самыми компьютеризированными из всех систем физической безопасности объекта. В сколь-нибудь крупных системах используются IP-видеокамеры, подключаемые непосредственно к локальной вычислительной сети, и видеорегистраторы, построенные на базе серверных или настольных ПК. Эти системы зависимы от ИТ-инфраструктуры, и ее отказы могут приводить к частичным отказам системы. Проблема зависимости систем видеонаблюдения от ИТ-инфраструктуры хорошо известна производителям этих систем.

Какие методы производители применяют для повышения их отказоустойчивости?

Для нейтрализации последствий отказов инфраструктуры в продвинутых системах видеонаблюдения используются различные методы, такие как запись видеопотока на локальное хранилище IP-видеокамеры при обрыве связи с видеорегистратором с последующей загрузкой этих записей на

видеорегистратор при восстановлении связи и резервирование видеорегистраторов по схеме N + m (N + 1, N + 2 и т.д.). В этом случае сервер управления контролирует работоспособность видеорегистраторов и, в случае отказа одного из них, поручает резервному видеорегистратору взять на себя запись и трансляцию видеопотоков с видеокамер, которые ранее обслуживались отказавшим видеорегистратором.

Более того, во многих системах видеонаблюдения сервер управления системой является единой точкой входа для всех АРМ системы, и его отказ приведет к невозможности использования системы, несмотря на то что видеокамеры продолжают съемку, а видеорегистраторы — запись. Так что сервер управления системой видеонаблюдения (при его наличии в системе) — это компонент, отказ которого наиболее критичен, а обеспечение его отказоустойчивости — первоочередная задача.

Насколько эффективны применяемые методы повышения отказоустойчивости сервера?

Не все методы можно применить во всех случаях. Инфраструктура систем физической безопасности объектов, как сетевая, так и серверная, зачастую строится параллельно и неза-

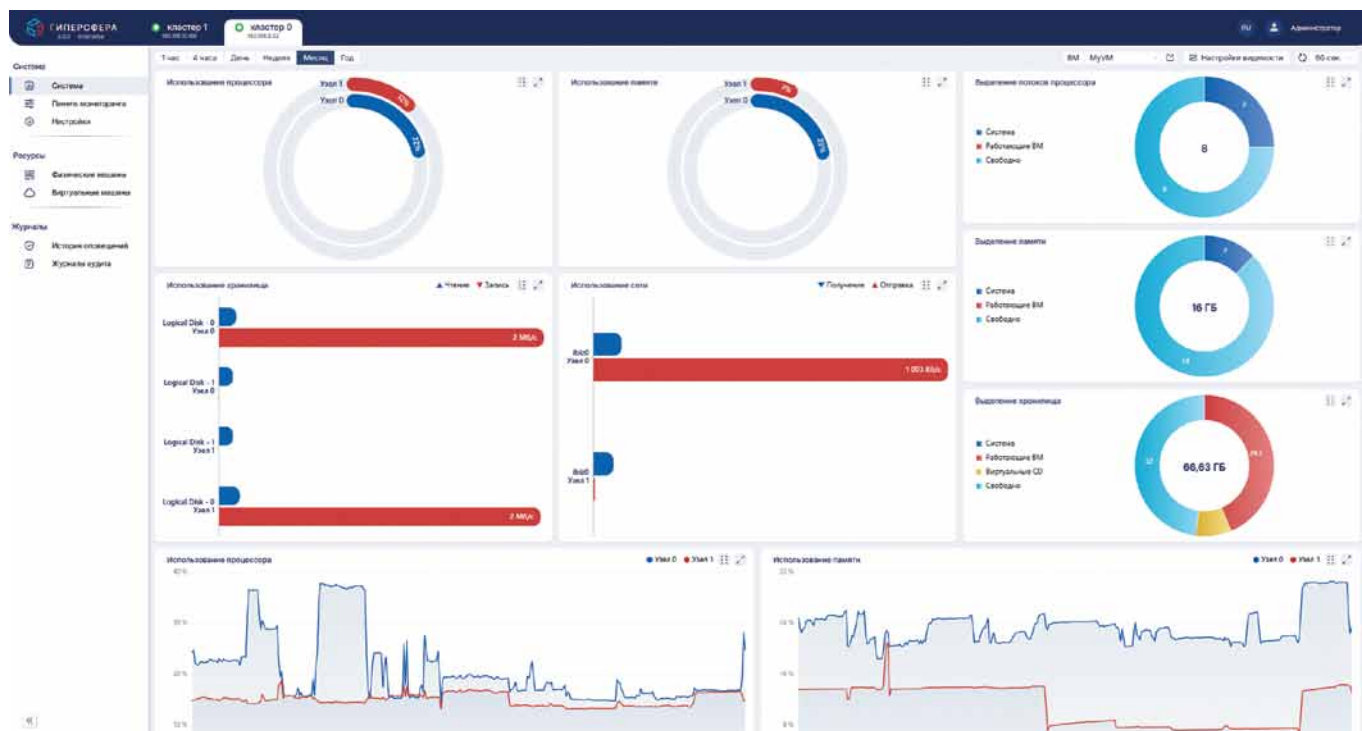


Рис. 1. ПО «ГиперСфера»: пример рабочего окна

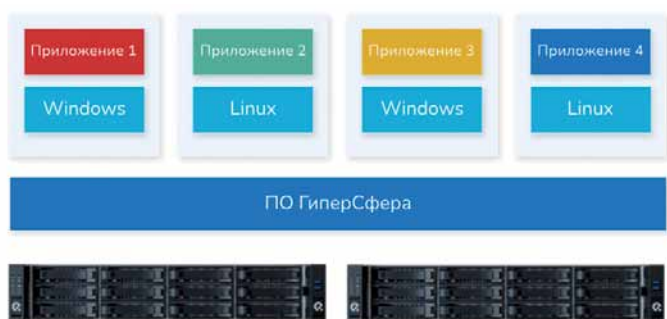


Рис. 2. Виртуальная машина работает одновременно на двух серверах: если один сервер выйдет из строя, виртуальная машина продолжит работать на резервном сервере

висимо от общей ИТ-инфраструктуры объекта. Более того, часто бывает, что поддержка инфраструктуры систем безопасности находится вне зоны ответственности ИТ-службы объекта. Это ограничивает выбор решений: для обеспечения отказоустойчивости прикладных серверов не подойдут сложные решения, требующие активной поддержки со стороны ИТ-службы.

Какие возможности дает ПО «ГиперСфера» для обеспечения отказоустойчивости серверов систем безопасности?

ПО «ГиперСфера» (рис. 1) идеально подходит для выполнения этой задачи, так как это решение «всё в одном». Для развертывания и поддержки системы достаточно компетенций компаний-партнеров и не требуется привлекать ИТ-службу заказчика. «ГиперСфера» обеспечивает отказоустойчивость полезной нагрузки, в данном случае — прикладных серверов систем физической безопасности объекта, пу-

тем создания непрерывной или, по выбору, высокой доступности виртуальных машин, в которых выполняются соответствующие прикладные сервера.

Поддержка в качестве гостевых операционных систем разнообразных версий Windows и Linux, включая отечественные ОС, позволяет использовать «ГиперСферу» для обеспечения отказоустойчивости практически любых прикладных серверов систем физической безопасности объектов и вспомогательных серверов контура безопасности (контроллеров домена и т. п.).

А что можно сказать о доступности виртуальных машин?

Непрерывная или высокая доступность виртуальных машин реализуется в ПО «ГиперСфера» путем поддержания на двух физических серверах синхронизированных копий виртуальных машин. Если один из серверов откажет, выполнение виртуальных машин продолжится на другом физическом

сервере без перерыва (для виртуальных машин с непрерывной доступностью, виртуальные машины с высокой доступностью будут перезапущены) и потери данных (рис. 2).

Какое аппаратное обеспечение требуется для построения такой системы?

Для построения отказоустойчивого кластера достаточно двух обычных серверных ПК схожей конфигурации с сетевыми адаптерами 10 Гбит/с для сети синхронизации узлов кластера. Наличие общего для узлов кластера хранилища, такого как отдельная система хранения данных, не требуется.

Решение на базе ПО «ГиперСфера» позволяет обеспечить требуемую отказоустойчивость прикладных серверов систем безопасности объекта вне контура, обслуживаемого ИТ-службой объекта, с минимальными затратами на аппаратное обеспечение кластера и без высоких требований к компетенциям, требующимся для развертывания и поддержки кластера.

Беседовали: С. В. Бодрышев, главный редактор журнала «ИСУП»,



ГИПЕРСФЕРА

А. А. Душко, технический директор, ООО «СТР», г. Москва, тел.: +7 (495) 646-8511, e-mail: info@str-technologies.com, сайты: str-technologies.com, отказоустойчивость.рф

