МЕТОДОЛОГИИ ОБЕСПЕЧЕНИЯ КАТАСТРОФОУСТОЙЧИВОСТИ В ВИРТУАЛИЗИРОВАННЫХ ИНФРАСТРУКТУРАХ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОДХОДОВ

Буцкевич Е. М., Кравченко Е. Д., Белоусова Е. С.
Кафедра защиты информации,
Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: {lbutskevich, ekat25163}@gmail.com, belousova@bsuir.by

Проведён сравнительный анализ современных методологий обеспечения катастрофоустойчивости в виртуализированных IT-инфраструктурах. Особое внимание уделено роли резервного центра обработки данных (ЦОД) и механизмам синхронизации. В работе предложена концептуальная модель автоматизированной системы аварийного восстановления, основанная на политиках, управляемых бизнес-метриками (RTO/RPO). Данная модель обеспечивает адаптивный выбор сценария переключения и минимизирует влияние человеческого фактора в процессе реагирования на инциденты.

Введение

В эпоху цифровизации и активного внедрения технологий виртуализации обеспечение непрерывности бизнес-процессов становится одной из ключевых задач управления IT-инфраструктурами. Нарушение доступности сервисов вследствие техногенных или природных катастроф может привести к значительным финансовым и репутационным потерям. Для минимизации таких рисков организации внедряют стратегии аварийного восстановления (Disaster Recovery Plan, DRP), базирующиеся на создании географически удалённого резервного ЦОД. Эффективность любой стратегии оценивается по двум ключевым бизнес-метрикам: RTO (Recovery Time Objective) – целевое время восстановления, и RPO (Recovery Point Objective) – целевая точка восстановления. Целью настоящей работы является сравнительный анализ основных подходов к обеспечению катастрофоустойчивости, их оценка по критериям RTO/RPO, и обоснование необходимости разработки автоматизированной системы, способной адаптивно выбирать механизм переключения при сбое.

I. Анализ базовых методологий катастрофоустойчивости

Фундаментом катастрофоустойчивой инфраструктуры является резервный ЦОД. Существуют четыре базовых подхода, отличающихся по принципу действия, стоимости и достигаемым показателям RTO и RPO.

Восстановление из резервных копий (Backup and Restore). Данная методология основана на периодическом (как правило, ежесуточном) создании образов виртуальных машин. Принцип действия заключается в развертывании инфраструктуры «с нуля» из последней копии в резервном ЦОД. Из-за периодического характера и необходимости ручного вмешательства данный подход характеризуется высокими RTO и RPO, измеряемыми в часах или днях.

Репликация виртуальных машин. Технология обеспечивает непрерывное копирование данных ВМ на резервную площадку в асинхронном режиме. Принцип действия состоит в том, что на резервной площадке поддерживаются актуальные копии ВМ, готовые к запуску. Это позволяет достичь низкого RPO (минуты), однако сам процесс переключения (failover) часто требует ручного или автоматизированного запуска.

Географически распределённый кластер (Metro Cluster). Этот подход объединяет два ЦОД в единую отказоустойчивую систему с синхронной репликацией данных. Принцип действия заключается в том, что система хранения данных обрабатывает обе площадки как единое целое. Это позволяет автоматически переключать нагрузку при сбое, обеспечивая RPO, близкий к нулю, и RTO в пределах минут.

Бесшовная отказоустойчивость (Fault Tolerance, FT). Технология создает полную, синхронно работающую копию ВМ. Принцип действия основан на технологии lockstep, когда каждая операция выполняется одновременно на основной и теневой ВМ. Это обеспечивает мгновенное переключение без простоя и потерь данных (RTO=0, RPO=0), являясь самым дорогостоящим решением.

Сводная сравнительная характеристика рассмотренных подходов приведена в таблице 1.

II. Архитектура системы автоматизации аварийного восстановления на основе политик

Анализ существующих подходов показывает, что их ключевым недостатком является зависимость от человеческого фактора на этапе принятия решения. Для устранения этого недостатка предлагается концептуальная модель автоматизированной системы, реализующей адаптивный,

управляемый политиками выбор сценария восстановления.

Ядром предложенной концептуальной модели является модуль принятия решений (Policy Engine). Работа системы, как показано на рис. 1, инициируется событием от модуля мониторинга, которое передается в модуль анализа для классификации инцидента. Получив классифицированный инцидент (например, «отказ хоста» (физического сервера, на котором работают виртуальные машины) или «полный отказ ЦОД»), модуль принятия решений обращается к внешней матрице политик (Базе знаний). В данной матрице заранее определены правила, сопоставляющие тип инцидента и уровень критичности сервиса (определяемый его RTO/RPO) с конкретным сценарием восстановления (Recovery Workflow). На основе этого сопоставления система делает адаптивный выбор: для некритичного сервиса при отказе одного хоста может быть выбран сценарий перезапуска средствами HA, тогда как для критичного сервиса при полном отказе ЦОД будет инициирована активация Metro Cluster. Выбранный сценарий передается на исполнение, где запускаются соответствующие технические процедуры и отправляются уведомления администраторам.

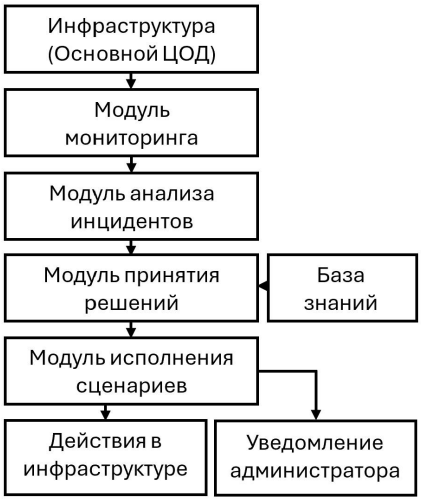

Рис. 1 – Архитектура системы адаптивного восстановления

Такая архитектура позволяет системе не просто реагировать на сбой, а адаптивно выбирать наиболее релевантный и экономически оправданный способ восстановления, минимизируя как время простоя, так и избыточные затраты.

III. Выводы

Катастрофоустойчивость является критически важным аспектом функционирования современных виртуализированных IT-инфраструктур. Проведенный сравнительный анализ показал, что, хотя выбор технологии аварийного восстановления и должен определяться метриками RTO/RPO, эффективность существующих решений ограничена зависимостью от человеческого фактора.

Для решения этой проблемы предложена концептуальная модель автоматизированной системы, управляемая политиками. Она устраняет задержки и ошибки, связанные с ручным вмешательством, путем автоматического выбора оптимального сценария восстановления на основе критичности сервиса. Такой подход трансформирует процесс реагирования на инциденты, позволяя перейти от реактивного к проактивному управлению. Это повышает адаптивность системы, сокращает время реакции при переключении между ЦОДами и минимизирует риски для бизнеса.

IV. Список литературы

1. Катастрофоустойчивость корпоративного датацентра как услуга [Электронный ресурс] / Хабр – Режим доступа: `https://habr.com/ru/companies/safedata/articles/273947/`. – Дата доступа: 24.12.2015.
2. Как сделать ИТ-инфраструктуру VMware катастрофоустойчивой? [Электронный ресурс] / OBLAKO – Режим доступа: `https://oblako.kz/iaas-blog/kak-sdelat-it-infrastrukturu-vmware-katastrofoustojchivoj`. – Дата доступа: 19.03.2018.
3. Microsoft StorSimple – автоматическое аварийное восстановление [Электронный ресурс] / Хабр – Режим доступа: `https://habr.com/ru/companies/comparex/articles/312064/`. – Дата доступа: 07.10.2016.

Таблица 1 – Сравнительная характеристика подходов

Критерий	Резервное копирование	Репликация	Metro Cluster	Fault Tolerance
RTO	от 4 до 48 часов	от 15 мин до 1 часа	от 1 до 5 минут	Ноль (мгновенно)
RPO	от 12 до 24 часов (зависит от частоты копирования)	от 15 сек до 5 минут (зависит от канала связи)	Ноль (синхронная репликация)	Ноль (без потерь данных)
Сложность	Низкая	Средняя	Высокая	Высокая