

Федеральное государственное автономное
образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт космических и информационных технологий

Системы автоматики, автоматизированного управления и проектирования

УТВЕРЖДАЮ
Заведующий кафедрой

_____ С. В. Ченцов

« ____ » июня 2017 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

**ПРОЕКТИРОВАНИЕ ЦЕНТРОВ СБОРА И ОБРАБОТКИ ДАННЫХ ДЛЯ
ПРЕДПРИЯТИЙ ЭЛЕКТРОЭНЕРГЕТИКИ НА ОСНОВЕ ТЕХНОЛОГИИ
ВИРТУАЛИЗАЦИИ**

27.04.04 Управление в технических системах

27.04.04.03 Автоматизация управления технологическими процессами в энергетике

Научный руководитель	_____	____.06.2017	доцент, канд. техн. наук С. А. Темербаев
Выпускник	_____	____.06.2017	А. А. Потерайло
Рецензент	_____	____.06.2017	доцент, канд. пед. наук С. А. Виденин
Нормоконтролер	_____	____.06.2017	Т. А. Грудинова

Красноярск 2017

В работе исследуются различные способы и подходы к построению ЦСОД в электроэнергетике: классический подход, подход с применением технологий виртуализации и подход с применением технологий кластеризации. Выделены основные достоинства и недостатки каждого подхода с учетом особенностей, которые необходимо учитывать при проектировании ЦСОД в электроэнергетике. Продемонстрировано влияние используемых технологий на снижение себестоимости тепловой и электрической энергии, путем снижения затрат на ИТ-инфраструктуру.

Используя методы имитационного моделирования, в программной среде AnyLogic были построены упрощенные модели ЦСОД и проведены исследования при различных режимах работы. На основании полученных результатов сформулированы рекомендации по построению ЦСОД в энергетике.

Результаты исследования были апробированы в работе одного из генерирующих предприятий Красноярского края - Красноярской ТЭЦ-1.

Ключевые слова: виртуализация, кластеризация, гипервизор, ЦСОД, ЦОД, энергетика.

СОДЕРЖАНИЕ

Введение	4
1 ЦСОД и технологии виртуализации	6
1.1 Классические методы проектирования ЦСОД, основные компоненты и архитектуры.....	6
1.2 Обзор подходов к построению ЦСОД	21
1.2.1 Классический подход	21
1.2.2 Виртуализация.....	24
1.2.3 Кластеризация	27
1.3 Особенности ЦСОД предприятий энергетического комплекса	30
2 Исследование технологии виртуализации.....	32
2.1 Обзор наиболее популярных гипервизоров.....	32
2.2 Сравнение параметров гипервизоров.....	38
2.3 Моделирование центров сбора и обработки данных в программной среде AnyLogic.	42
2.4 Выводы и рекомендации по использованию технологий виртуализации ЦСОД в энергетике.	61
3 Апробация результатов.....	65
3.1 Описание текущей ситуации и структуры ЦСОД СГК.....	65
3.2 Результаты внедрения предложенного типового решения для ЦСОД на основе технологий виртуализации	66
Заключение.....	72
Список использованных источников	73
Приложение А	73
Приложение Б.....	73
Приложение В	73
Приложение Г.....	80
Приложение Д	81

ВВЕДЕНИЕ

В условиях постоянного удорожания энергоресурсов и соответствующей политике государства по сдерживанию роста тарифов, стимулированию к энергосбережению и энергоэффективности, для всех предприятий энергетического сектора важнейшими задачами является:

- повышение эффективности управления выработкой тепловой, электрической и других видов энергий,
- оптимизация затрат на передачу энергоресурса до конечного потребителя
- улучшение основных показателей производственной деятельности,
- улучшение технико-экономических показателей производства электрической и тепловой энергии.

Решение этих задач невозможно без консолидации данных о производственных показателях по всем территориально-распределенным энергоактивам компании в одном месте. Поэтому важным этапом в построении системы планирования и организации производственной деятельности становится создание единой инфраструктуры – центра сбора и обработки данных (далее ЦСОД). При проектировании ЦСОД возникает проблема, какой подход применить для построения ЦСОД.

Целью данной работы является развитие методов построения центров сбора и обработки данных для предприятий энергетического сектора на основе технологий виртуализации и кластеризации.

В главе 1 рассматривается состав ЦСОД, обзор его основных компонент. Определены особенности, преимущества и недостатки различных подходов к построению ЦСОД, а также особенности построения ЦСОД в энергетической отрасли.

В главе 2 представлены результаты исследования технологий виртуализации и кластеризации. Был осуществлен обзор и аналитическое сравнение гипервизоров, построены модели ЦСОД в программной среде имитационного мо-

делирования AnyLogic. В результате исследования были сформулированы рекомендации для построения ЦСОД в энергетике.

В главе 3 представлены результаты апробации работы на Красноярской ТЭЦ-1. Рассмотрено состояние ИТ-инфраструктуры до и после внедрения технологий виртуализации и кластеризации.

По теме магистерской диссертации опубликована одна работа в сборнике «Актуальные вопросы современной науки. Выпуск 52» [1, с. 141].

1 ЦСОД и технологии виртуализации

1.1 Классические методы проектирования ЦСОД, основные компоненты и архитектуры

ЦСОД представляет собой комплекс различных аппаратно-программных систем, основной задачей которого является обеспечение оптимальных условий работы оборудования и программных средств во всей информационно-технологической структуре предприятия. Для организации ЦСОД выделяют отдельное помещение или здание, в котором размещается оборудование.

ЦСОД состоит из нескольких подсистем:

- Серверная часть
- Система хранения данных
- Сетевая часть
- Система резервного копирования
- Система охлаждения
- Система электропитания
- Система пожаротушения
- Система контроля доступом
- Система мониторинга

Серверная часть представляет собой совокупность аппаратного и программного обеспечения. Программным обеспечением для серверной части являются разные семейства операционных систем. Аппаратная часть представлена типами и моделями серверов различных классов. Основные крупные производители качественных серверов – Dell, HP, IBM, Fujitsu, Huawei, Lenovo, Hitachi, Cisco.

Сервера бывают в основном трех типов:

- Отдельные сервера
- Блейд-системы
- Гибридные системы

Отдельные сервера (standalone servers) представляют собой классическую архитектуру [11; 18], показанную на рисунке 1. Отдельный сервер представлен в виде 19” сервера высотой 1, 2, 4, 5, 6 U с количеством процессоров от одного до четырех, собственной корзиной для жестких дисков (от четырех до несколько десятков), собственными блоками питания.

Сервера разделяются на следующие классы:

- Low-End
- Middle-end
- High end.

Конфигурация и стоимость подбирается исходя из поставленных задач и вместительности ЦСОД.



Рисунок 1 – Отдельностоящий сервер

Второй тип это блейд-системы (блейд корзины, blade) – состоит из блейд-корзины и блейд-серверов (blade-servers) [30; 31] и показан на рисунке 2. Блейд-сервера представляют собой очень компактный сервер, предназначенный для установки в блейд-корзину. Блейд-корзина представляет из себя корпус 19” и высотой от 4U с собственными дублированными источниками питания, материнскими платами, портами ввода/вывода, встроенными сетевыми коммутаторами. Блейд-корзина позволяет более плотно размещать сервера, за счет модульности позволяет строить гибкую конфигурацию серверного оборудования, уменьшает количество используемых кабелей и занимает намного меньшее место. В каждый тип блейд-корзины можно устанавливать ограниченный перечень серверов и оборудования.



Рисунок 2 – Блейд-система

Третий тип это гибридная система – состоит из блейд-корзины, блейд-серверов и общей дисковой корзины (СХД) [7; 16; 34], показана на рисунке 3. Гибридная система похожа на обычную блейд-систему, но отличается тем, что имеет еще общую для всех блейд-серверов дисковую корзину (СХД). Обычно имеет меньше отсеков для установки блейд-серверов. Представляет собой гибрид из серверов и СХД в одном корпусе. Предназначена, в основном, для малых и средних предприятий.



Рисунок 3 – Гибридная система

В качестве операционной системы для серверов используют Windows или Linux. Из семейства Windows используется серверная версия ОС (Windows Server). Из семейства Linux используются различные дистрибутивы и родственные ОС, в зависимости от задач (Red Hat, Ubuntu, Debian и др.). На ОС устанавливаются и в дальнейшем функционируют необходимые программные комплексы для выполнения поставленных задач. При классическом подходе проек-

тирования рекомендуется следовать принципу «один сервер – одна роль», т. е. на один физический сервер устанавливать один программный комплекс.

Следующей составной частью ЦСОД является система хранения данных [3; 4; 38]. Система хранения данных (СХД) предназначена для организации высокоскоростных массивов дисков. Благодаря СХД можно организовывать различные общие дисковые ресурсы, доступные нескольким серверам одновременно. СХД позволяет организовать для каждого сервера отдельный дисковый массив для увеличения быстродействия. СХД должна размещаться рядом с серверами, для которых она предназначена. Максимальное расстояние между СХД и серверами ограничивается протоколом и средой передачи данных, которые использует сервер и СХД.

СХД разделяются на три уровня:

- Entry-level - начальный уровень. Для домашнего пользования и малого бизнеса.
- Mid-Range - средний уровень. Для небольших организаций и подразделений предприятий.
- Hi-End или Enterprise - уровня крупного предприятия.

Устройства начального уровня, как правило, состоят из небольшого (несколько единиц) количества дисков и либо имеют один контроллер, либо не имеют его вообще. Обычно реализованы в настольном исполнении, либо в виде одной дисковой полки и показаны на рисунке 4. Батареи резервного питания, как правило, не имеет.



Рисунок 4 – Система хранения данных

Устройства Mid-Range обычно имеют модульную конструкцию и состоят из одной или нескольких (до нескольких десятков) дисковых полок, монтируемых в стойку или серверный шкаф. Характеризуются наличием двух аналогичных контроллеров, каждый из которых имеет свою кэш-память и обслуживает часть дисков и серверных подключений. Имеет дублированные компоненты электропитания и вентиляции, а также резервную батарею. Не имеет единой точки отказа. В случае выхода из строя одного из контроллеров сохраняется доступ ко всей хранимой информации, но утрачивается половина производительности.

Массивы высшего класса предназначены для использования крупными предприятиями [19; 20]. Имеют более высокую по сравнению с предыдущими классами производительность и надёжность. Как правило, обладают следующими характеристиками: монолитная или монолитно-модульная конструкция в виде отдельно стоящего шкафа (шкафов). Возможность установки от сотни до тысяч дисков. Симметричная мультипроцессорная архитектура. Имеет до нескольких десятков специализированных контроллеров, каждый из которых предназначен либо для дисковых (BackEnd) либо для хостовых (FrontEnd) операций. Контроллеры разделяют общую память. Устройство полностью резервировано. При выходе из строя любого из компонентов (в т.ч. диска, контроллера) падение производительности незначительно (менее половины).

Класс СХД выбирается исходя из финансовых возможностей, поставленных задач и требуемой надежности.

Классификация на уровне относительно условна и не имеет четких границ, т. к. определяется ценой. Из-за высокой конкурентной борьбы производители обеспечивают устройства нижних уровней всё большим функционалом.

Также СХД разделяются в зависимости от типа используемого протокола подключения (SAS, FC, iSCSI) [39; 40]. Каждый протокол имеет свои преимущества, недостатки и ограничения. Выбор протокола зависит от поставленных задач и бюджета. На данном этапе наиболее перспективными протоколами являются FC и iSCSI.

Основные крупные производители качественных СХД – Dell, HP, IBM, Fujitsu, Huawei, Lenovo, Hitachi, NetApp, EMC.

Сетевое оборудование делится на две основные категории: оборудование локальных вычислительных сетей [6] (LAN-сетей) ЦСОД и оборудование SAN-сетей.

Оборудование для построения ЛВС ЦСОД выбирается исходя из поставленных задач и требуемой надежности. Современное оборудование позволяет резервировать как физические каналы, так и само оборудование за счет применения программно-аппаратных протоколов и специализированных технологий. Сюда относятся коммутаторы, маршрутизаторы, фаерволы. Ведущие производители: Cisco, HP, Huawei, ZTE, D-link, Netgear, Moxa, Zyxel и др.

Оборудование для построения SAN-сети [19] ЦСОД представлено специальными коммутаторами для построения высокой скоростной изолированной сети передачи между разными СХД и серверами. Данная сеть полностью изолирована от обычной ЛВС. SAN-сеть использует отличные от обычной ЛВС принципы построения сети и протоколы. Применение SAN-сетей оправдано с финансовой точки зрения только в средних и крупных ЦСОД, либо в ЦСОД с высокими требованиями к надежности и скорости передачи данных. Ведущие производители оборудования: Cisco, HP, Dell, IBM, D-link, Lenovo, Moxa и др.

Система резервного копирования предназначена для резервного копирования критически важных данных и систем, а также для архивного хранения данных. Резервное копирование не отменяет необходимости резервирования компонентов и использование отказоустойчивых решений и технологий. Система резервного копирования должна размещаться в другом помещении или здании, как можно дальше от ЦСОД. Система резервного копирования может представлять собой:

- отдельный сервер с несколькими дисками;
- сервер и одна или несколько СХД с дисками;
- сервер с одной или несколькими ленточными библиотеками.

Также приобретается специализированное ПО для автоматизации резервного копирования. Масштаб системы резервного копирования зависит от объемов данных, которые необходимо копировать. В свою очередь необходимость копирования данных определяется финансовыми потерями при безвозвратной утрате данных.

Система охлаждения подбирается исходя из площади ЦСОД. Она может быть отдельной и независимой для ЦСОД или общей на всё здание. Внутри самого ЦСОД могут создаваться теплые и холодные коридоры, для улучшения эффективности. Теплый/холодный коридор – размещение стоек рядами, одинаково ориентированными, со стороны тыльной части стоек устанавливаются вытяжную систему для отвода теплого воздуха, со стороны лицевой части устанавливаются приточную систему для подвода холодного воздуха. Холодный и горячий коридоры дополнительно разделяют перегородками. Для эффективности метода теплых и холодных коридоров необходимо, чтобы оборудование в стойке было одинаково ориентировано.

Система электропитания строится исходя из критериев надежности ЦСОД. Общая система питания ЦСОД строится в зависимости от выбранной категории надежности электроснабжения. Категории надежности электроснабжения определяются Правилами эксплуатации электроустановок (далее – ПУЭ)

[17]. По ПУЭ определяются следующие категории надежности электроснабжения:

- Электроприемники I категории
- Электроприемники II категории
- Электроприемники III категории
- Особая группа электроприемников I категории

Электроприемники I категории должны обеспечиваться электроэнергией от двух независимых взаимно резервирующих источников питания, и перерыв их электроснабжения при нарушении электроснабжения от одного из источников питания может быть допущен лишь на время автоматического восстановления питания.

Для электроснабжения особой группы электроприемников I категории должно предусматриваться дополнительное питание от третьего независимого взаимно резервирующего источника питания.

В качестве третьего независимого источника питания для особой группы электроприемников и в качестве второго независимого источника питания для остальных электроприемников I категории могут быть использованы местные электростанции, электростанции энергосистем (в частности, шины генераторного напряжения), специальные агрегаты бесперебойного питания, аккумуляторные батареи и т.п.

Если резервированием электроснабжения нельзя обеспечить необходимой непрерывности технологического процесса или если резервирование электроснабжения экономически нецелесообразно, должно быть осуществлено технологическое резервирование, например, путем установки взаимно резервирующих технологических агрегатов, специальных устройств безаварийного останова технологического процесса, действующих при нарушении электроснабжения.

Электроснабжение электроприемников I категории с особо сложным непрерывным технологическим процессом, требующим длительного времени на восстановление рабочего режима, при наличии технико-экономических обос-

нований рекомендуется осуществлять от двух независимых взаимно резервирующих источников питания, к которым предъявляются дополнительные требования, определяемые особенностями технологического процесса. [17, п. 1.2.18 ПУЭ].

Электроприемники II категории рекомендуется обеспечивать электроэнергией от двух независимых взаимно резервирующих источников питания.

Для электроприемников II категории при нарушении электроснабжения от одного из источников питания допустимы перерывы электроснабжения на время, необходимое для включения резервного питания действиями дежурного персонала или выездной оперативной бригады.

Допускается питание электроприемников II категории по одной ВЛ, в том числе с кабельной вставкой, если обеспечена возможность проведения аварийного ремонта этой линии за время не более 1 сут. Кабельные вставки этой линии должны выполняться двумя кабелями, каждый из которых выбирается по наибольшему длительному току ВЛ. Допускается питание электроприемников II категории по одной кабельной линии, состоящей не менее чем из двух кабелей, присоединенных к одному общему аппарату.

При наличии централизованного резерва трансформаторов и возможности замены повредившегося трансформатора за время не более 1 сут. допускается питание электроприемников II категории от одного трансформатора. [17, п.1.2.19].

Для электроприемников III категории электроснабжение может выполняться от одного источника питания при условии, что перерывы электроснабжения, необходимые для ремонта или замены поврежденного элемента системы электроснабжения, не превышают 1 сут. [17, п. 1.2.20].

Внутри ЦСОД каждая стойка с оборудованием должна иметь как минимум два резервированных источника бесперебойного питания (далее – ИБП), запитанных от разных фаз (при возможности от разных вводов), ЦСОД или помещения ЦСОД должны оснащаться автоматическим вводом резерва (далее – АВР). Оборудование, имеющее более одного блока питания, в стойке должно

запитываться от разных ИБП. Для оборудования с одним блоком питания используются быстродействующие стоечные АВР [26]. Время автономной работы на ИБП подбирается в зависимости от требований. Рекомендуется обеспечивать электропитание ЦСОД не ниже первой группы надежности электроснабжения, по классификации ПУЭ. В редких случаях используется вторая группа надежности электроснабжения по классификации ПУЭ.

Система пожаротушения выполняется в соответствии с требованиями пожарной безопасности и регламентирующими документами.

Система контроля и управления доступом (далее – СКУД) предназначена для предотвращения доступа в ЦСОД посторонних лиц и для ведения учета сотрудников, посещавших ЦСОД. Строится на специализированных контроллерах и сервере. Рекомендуется сервер СКУД с базой данных (далее – БД) размещать в отдельном помещении с ограниченным доступом.

Система мониторинга предназначена для контроля параметров ЦСОД и оперативного реагирования на отклонения критических параметров. Состоит из нескольких уровней:

Нижний уровень – установка датчиков температуры, влажности, открытия/закрытия дверей, контроль вводов питания, ИБП, качества электропитания, параметров электросети. Установка системы видеонаблюдения.

Средний уровень – автоматизация контроля за счет централизованного сбора параметров, чаще всего по протоколу SNMP [36; 37]. Для организации данной системы выделяется отдельный сервер, устанавливается специализированное ПО и настраивается сбор необходимых параметров. ПО для мониторинга есть как бесплатное, так и платное. Всё современное оборудование (сервера, СХД, ИБП, АВР и т.д.) совместимо с протоколом SNMP.

Верхний уровень – система контроля параметров операционной системы, специализированного ПО, производительности и загруженности оборудования. Позволяет контролировать параметры более высокого уровня. Чаще всего данное ПО платное и выпускается для различных ОС (Windows/Linux). Также представляет из себя отдельный сервер со специализированным ПО.

Кроме деления ЦСОД на подсистемы ЦСОД классифицируются по трем различным параметрам: надежности, эффективности использования электрической энергии, конструктивному исполнению и подходу построения.

По надежности ЦСОД классифицируются по 4-х уровневой системе, разработанной в Uptime Institute, отраслевого консорциума ЦСОД [21; 29]. Для каждого уровня в данном стандарте определены требования по архитектуре, безопасности, строительству и телекоммуникационным системам.

Кроме того, для каждого уровня определена «доступность» системы (т.е. время нормальной работы в процентах от всего времени службы, в которое входит и время простоя): 99,671% (28,8 часов простоя в год) для уровня 1 (Tier 1); 99,741% (22 час простоя в год) для уровня 2 (Tier 2), 99,982% (1,6 часа простоя в год) для уровня 3 (Tier 3), и 99,995% (0,4 часа простоя в год) для уровня 4 (Tier 4).

ЦСОД уровня I (N) подвержен нарушениям нормального хода работы как от плановых, так и от внеплановых действий. Он имеет системы распределения электропитания и охлаждения компьютеров, но может не иметь источников бесперебойного питания ИБП или резервного дизель-генератора. Если даже есть ИБП или генератор, то они представляют собой одномодульные системы. Поэтому инфраструктуру ЦСОД приходится регулярно останавливать для профилактических работ. Ошибки при эксплуатации, неверные действия администратора, отказы компонентов инфраструктуры ЦСОД будут вызывать перемены в его нормальной работе. Инженерная инфраструктура не зарезервирована.

ЦСОД Уровня II (N+1) имеет резервирование (избыточность) компонентов, поэтому меньше подвержен нарушениям нормальной работы по причине плановых или внеплановых событий, чем ЦСОД уровня I. В ЦСОД Уровня II может быть фальшпол, ИБП и генераторы, однако резервирование осуществляется по схеме N+1 (Need plus One), т.е. один запасной компонент на нужное количество оборудования. Техническое обслуживание и ремонт системы электр.

троснабжения и других частей инфраструктуры объекта потребует остановки процесса обработки данных.

ЦСОД Уровня III (2N) имеет возможность параллельного проведения ремонтов и любых плановых работ без остановки работы оборудования и инфраструктуры. К плановым работам относится профилактическое и программируемое техническое обслуживание, ремонт и замена компонентов, добавление или удаление компонентов, влияющих на производительность, тестирование компонентов и пр. Например, в больших ЦСОД, где используются жидкостные системы охлаждения, это означает наличие двух независимых комплектов труб. Следовательно, вычислительная мощность серверов, емкость систем хранения и коммутации должны иметь достаточную величину и возможность распределения мощности и емкости, чтобы одновременно нести рабочую нагрузку в одной области ЦСОД, и в то же время выполнять ремонт или тестирование в другой. Тем не менее, внеплановые события, например ошибки при эксплуатации или самопроизвольные отказы компонентов инфраструктуры ЦОД, всё же могут вызывать перерывы нормальной работы. Инженерные системы однократно зарезервированы, имеется несколько каналов распределения электропитания и охлаждения, однако постоянно активен только один из них. ЦСОД уровня III зачастую проектируют с перспективой наращивания ресурсов до уровня IV, когда требования бизнеса клиента оправдают стоимость дополнительной защиты.

ЦСОД уровня IV (2(N+1)) создаются по принципу отказоустойчивости. Уровень IV предусматривает возможность проводить любые плановые работы без нарушения нормальной работы оборудования и инфраструктуры ЦСОД. Отказоустойчивая функциональность также обеспечивает способность инфраструктуры выдержать, по крайней мере, один отказ (или событие) наихудшего свойства без последствий для критически важной нагрузки. Это требует одновременной активности путей распределения, обычно в конфигурации «1+1», т.е. полного резервирования всех компонентов. В системе электропитания это означает наличие двух отдельных систем ИБП, причем каждая система

имеет внутреннее резервирование N+1. Тем не менее, согласно нормам противопожарной безопасности и электробезопасности все же возможны некоторые простои из-за срабатывания пожарной сигнализации или по причине аварийного отключения нагрузки. Уровень IV требует, чтобы всё оборудование ЦСОД имело двойной подвод питания. Инфраструктура ЦСОД Уровня IV наиболее соответствует концепции высокой эксплуатационной готовности, которая предусматривает использование технологий кластеризации, запоминающих устройств с прямым доступом (DASD), матрицы независимых дисковых накопителей с избыточностью (RAID) и дублирование связей с целью достижения высокой надёжности, готовности и ремонтпригодности. Имеется возможность проведения любых работ без остановки работы ЦСОД.

Другим важным параметром ЦСОД является эффективность использования электроэнергии. Эффективность использования электроэнергии представляет собой простое соотношение мощности, используемой в ЦСОД его ИТ-оборудованием (серверы, системы хранения и коммутационное оборудование), к общей потребляемой мощности, часть которой расходуется на системы охлаждения и вентиляции, а также на различные потери.

По конструктивному исполнению ЦСОД делятся на следующие типы: стационарные, модульные, мобильные и микро-ЦСОД.

Стационарный ЦСОД представляет из себя классическую схему, когда для ЦСОД строится отдельное здание (помещение) или используется существующее здание (помещение).

Модульный ЦСОД изображен на рисунке 5 и представляет собой законченную конструкцию, включающую в себя все элементы ЦСОД: серверы, накопители и коммутаторы, а также инфраструктурные элементы систем микроклимата и пожаротушения.

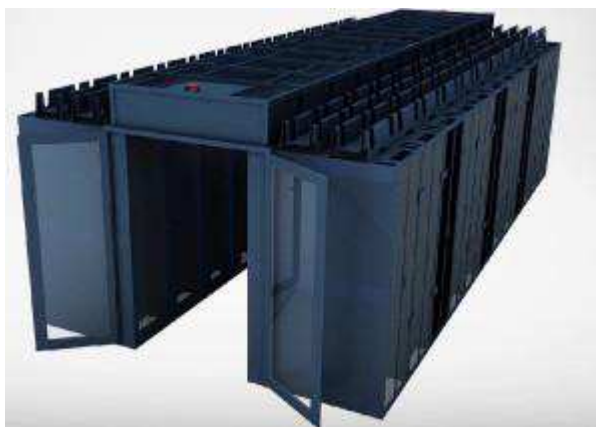


Рисунок 5 – Модульный ЦСОД

Как правило, модульный ЦСОД имеет отдельный вход, герметизирующий его внутренности от среды помещения, в котором он устанавливается. Хотя основное предназначение модульного ЦСОД – использование его в непригодных помещениях, его также можно использовать в зданиях стационарного ЦСОД.

Мобильные ЦСОД (контейнерные ЦОД) так называют потому, что их принято размещать в стандартных контейнерах. Это делается с целью повышения оперативности развертывания, снижения затрат на создание ЦСОД. Мобильный ЦСОД изображен на рисунке 6.



Рисунок 6 – Мобильный ЦСОД

Мобильные ЦСОД могут быть весьма эффективны при различных экстренных ситуациях, например, создания оперативных штабов по ликвидации

последствий стихийных бедствий, а также для задач оперативной деятельности малого и среднего бизнеса, где строительство больших стационарных ЦСОД экономически невыгодно.

Мобильные ЦСОД можно также использовать для оперативного расширения емкости больших стационарных ЦСОД, а также для целей резервирования, чтобы повысить уровень ЦСОД в случае необходимости.

Для небольших предприятий и филиалов крупных и средних предприятий могут подойти ЦСОД небольшого размера (микро-ЦСОД), представляющее собой решение «все в одном». Данное решение выполняется в виде отдельного шкафа, полностью герметичного и имеющего собственную систему охлаждения и питания.

Микро-ЦСОД могут быть как комнатного, так наружного исполнения. В последнем случае элементы ЦСОД помещаются в термозащищенный, вандалоустойчивый шкаф. Микро-ЦСОД изображен на рисунке 7.



Рисунок 7 – микро-ЦСОД

Строительство собственного ЦСОД предприятия требует значительных капитальных и текущих затрат, поэтому многие предприятия предпочитают вместо создания корпоративного ЦСОД заключить договор с коммерческими компаниями, предоставляющих в аренду часть своего ЦСОД или ресурсов ЦСОД.

1.2 Обзор подходов к построению ЦСОД

Кроме рассмотренной в Разделе 1.1 классификации ЦСОД, можно произвести разделение ЦСОД по методам и подходам, используемым в процессе построения внутренней структуры: классический подход, подход с использованием технологий виртуализации и подход с использованием технологий кластеризации.

1.2.1 Классический подход

Логическая схема классического подхода показана на рисунке 8. При данном подходе для каждого программного комплекса (каждой задачи) приобретается отдельный физический сервер с необходимым вспомогательным оборудованием. Сервера полностью независимы друг от друга и только обмениваются между собой данными.

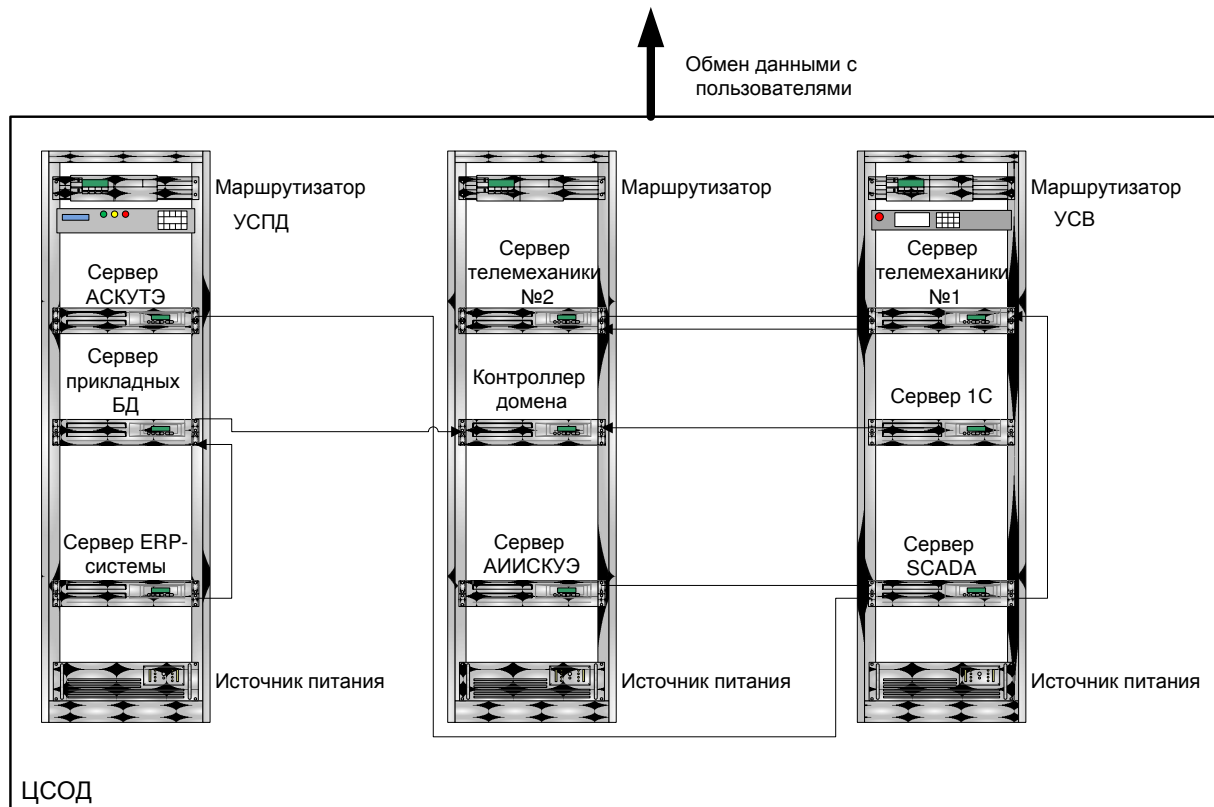


Рисунок 8 – Классическая схема ЦСОД

При классическом подходе к построению ЦСОД можно выделить ряд проблем, возникающих в процессе дальнейшей эксплуатации и обслуживании:

- Низкие коэффициенты использования вычислительных ресурсов при росте количества вычислительных узлов. Увеличение количества серверов ведет к увеличению вспомогательного оборудования (климатическое, сетевое, электрическое), что ведет к уменьшению эффективности использования ЦСОД, как по климатической системе, так и по электрической. Уменьшение процента использования вычислительных ресурсов из-за скачкообразной и неравномерной нагрузки на серверное оборудование. Необходимость приобретения более мощного оборудования (более дорого) для обеспечения необходимой производительности при пиковых нагрузках.

- Растущие расходы на физическую инфраструктуру. Увеличение количества физических серверов ведет к увеличению затрат на внедрение новых серверов и обслуживание существующих. Увеличение затрат при внедрении новых серверов связано с необходимостью обеспечения серверов кабельной продукцией, сетевым оборудованием для подключения к сети предприятия и вспомогательным электрическим оборудованием (модули распределения питания, источники бесперебойного питания). Увеличение затрат на содержание связано с увеличением затрат на электроэнергию, охлаждение помещения. Эти затраты не зависят от степени использования серверов, а зависят от фактического наличия серверов.

- Растущие расходы на службу поддержки. Увеличение количества серверов ведет к пропорциональному увеличению численности службы поддержки. Растет время, затраченное на аппаратное и техническое обслуживание. Увеличение количества серверов ведет к усложнению информационных систем, что требует наличия высококвалифицированного персонала, уникальных и редких компетенций и опыта. Необходимо увеличивать затраты на обучение персонала.

- Длительное и неэффективное аварийное переключение и слабая защита от сбоев. Увеличение финансовых потерь из-за простоя серверного оборудова-

ния и критических информационных систем ведет к повышению требований к отказоустойчивости и надежности оборудования. Выход из строя отдельных серверов ведет к длительным простоям и переключению оборудования. Отсутствует защита от техногенных и природных катастроф, длительное восстановление после таких катастроф. Слабая устойчивость классических ЦСОД от вирусных атак и угроз.

- Длительное и неэффективное внедрение и модернизация программных комплексов. Внедрение новых программных комплексов требует приобретения дополнительного серверного оборудования. Ввод новых серверов в эксплуатацию требует более длительной пуско-наладки, миграции данных и программных комплексов на новое оборудование. Для модернизации и улучшения аппаратной части серверов необходима их остановка, что ведет к остановке программных комплексов.

К основным достоинствам классического подхода к построению ЦСОД можно отнести:

- Полную совместимость со специфическим оборудованием, таким как устройства синхронизации времени (далее – УСВ), устройства сбора и передачи данных (далее – УСПД), преобразователи. На данном подходе строятся все системы и программные комплексы, данный подход поддерживается и производителями оборудования и разработчиками ПО по умолчанию.

- Проще организовать ограничения по физическому доступу оборудования. Достаточно вынести особо важный сервер с программным комплексом в отдельное защищенное помещение для обеспечения физической безопасности. Проще разграничить доступ к оборудованию для разных администраторов программных комплексов. Достаточно разнести программные комплексы в разные помещения и оставить доступ к оборудованию только для тех лиц, которые непосредственно работают с данным программным комплексом.

- Постепенное наращивание мощности. При внедрении новых программных комплексов вычислительная мощность ЦСОД растет постепенно, за счет покупки и модернизации серверов.

Данный подход был долгое время единственным, но с появлением и развитием технологии виртуализации появились два других подхода.

1.2.2 Виртуализация

Рассмотрим подход, при котором создается сервер виртуализации и используется технология виртуализации ресурсов. В основе данной технологии лежит идея виртуализации ресурсов, т. е. разделение ресурсов физического сервера на независимые логические разделы (виртуальные машины). Каждая такая виртуальная машина полностью изолирована от других, имеет свою ОС и может выполнять свои функции. Виртуальной машине выдается определенная часть физических ресурсов сервера таких как оперативное запоминающее устройство (далее – ОЗУ), центральное процессорное устройство (далее – ЦПУ), дисковое пространство). Виртуальная машина может не знать о том, что она виртуальная. ОС в виртуальной машине функционирует, так же как и на физическом сервере за счет эмуляции физических устройств. Для управления виртуальными машинами на сервере используется специальная программная надстройка – гипервизор. Логическая схема такого подхода показана на рисунке 9.

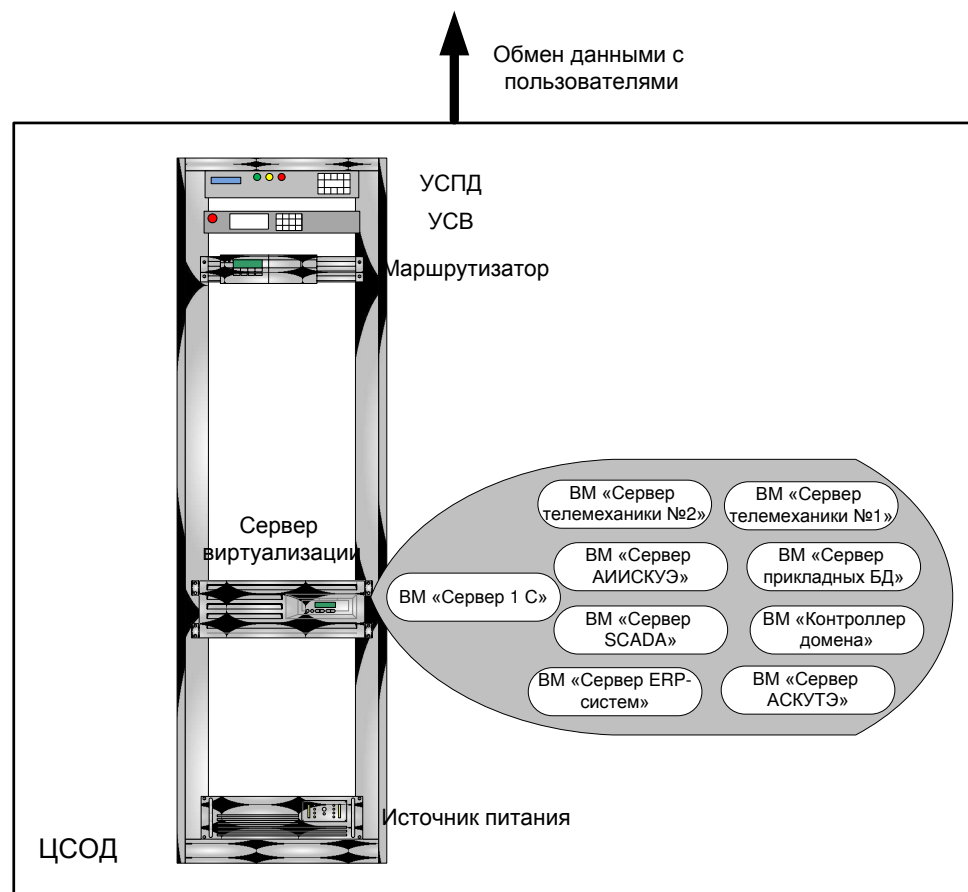


Рисунок 9 – Виртуализация ЦСОД

Данный подход обладает следующими преимуществами:

- Ресурсы физического сервера используются максимального эффективно. За счет размещения нескольких виртуальных машин нет простаивающих мощностей и ситуаций, когда физический сервер используется на 10-15 %.

- Гибкость и быстрота ввода новых программных комплексов. Можно менять лимит доступных ресурсов (в рамках ресурсов физического сервера) для каждой виртуальной машины (далее – VM) в зависимости от задач и нагрузки. Ввод новых программных комплексов происходит намного быстрее, т. к. нет необходимости закупать новый сервер, устанавливать и настраивать его, достаточно развернуть новую виртуальную машину из шаблона. Также легче обновлять программные комплексы и переходить на новые версии программного обеспечение (далее – ПО), достаточно для обновлений развернуть параллельно копию необходимой виртуальной машины и провести обновления на ней.

- Больше скорость взаимодействия программных комплексов. Все программные комплексы размещаются на одном физическом сервере, поэтому нет задержек на сетевое взаимодействие. Все виртуальные машины взаимодействуют между собой внутри физического сервера, и скорость взаимодействия ограничивается возможностями сервера.

- Экономия ресурсов. Один более мощный сервер виртуализации потребляет меньше электроэнергии, чем несколько более слабых серверов с аналогичной суммарной мощностью. Данному серверу нужна меньшая площадь ЦСОД. Можно использовать менее мощную систему охлаждения и электропитания. Меньше необходимо вспомогательного оборудования (распределители питания, источники бесперебойного питания, коммутаторы и т.п.).

- Уменьшение необходимого объема запасных частей из-за меньшего количества физических серверов и вспомогательного оборудования.

Данный подход имеет следующие недостатки:

- Для виртуализации необходим более мощный сервер. Суммарная мощность сервера виртуализации минимально должна быть равна суммарной мощности всех виртуальных машин. Из этого вытекает, что сервер виртуализации должен быть очень мощным, иметь большее количество дополнительных отсеков, модулей для наращивания вычислительных ресурсов. При наличии очень ресурсоемких виртуальных машин можно достигнуть потолка ресурсов физического сервера. Также из-за этого, возможно, придется приобретать сервера более высокого класса, которые могут быть технически более сложными.

- Проблема организации большого количества USB или COM-портов. При использовании большого количества USB-ключей или оборудования с COM-портами возникает необходимость иметь большее количество портов на сервере. Большее количество обеспечивается либо установкой дополнительных плат, либо установкой специальных устройств (преобразователей), преобразующих USB или COM в Ethernet. Использование данных устройств ведет к дополнительным финансовым затратам.

- Невозможность разделения физического доступа к разным программным комплексам. Администратор сервера виртуализации может отключать перезагружать все виртуальные машины. Нельзя вынести отдельный программный комплекс в отдельное помещение, ограничив к нему доступ.

- Скачкообразное наращивание вычислительной мощности. При достижении пределов наращивания мощности сервера виртуализации, для размещения виртуальных машин нужен будет дополнительный сервер виртуализации или новый более мощный сервер взамен старого. Дополнительный сервер виртуализации требует значительных капиталовложений. На начальном этапе (при размещении 1-2 виртуальных машин) данный дополнительный сервер виртуализации будет использовать свои вычислительные ресурсы на 5-15 %.

- Некоторое оборудование и программные комплексы не поддерживают виртуализацию, как правило, это касается старых программных комплексов, поэтому возникает необходимость приобретения нового ПО. Часть оборудования невозможно виртуализировать из-за используемых оборудованием протоколов или из-за запрета государственных контролирующих органов.

- Один сервер виртуализации представляет собой единую точку отказа. При отказе данного сервера остановятся все программные комплексы, развернутые в виртуальных машинах. Также затруднительно остановить данный сервер для проведения обслуживания или изменения аппаратной конфигурации, из-за необходимости остановки всех систем.

Последний недостаток был очень существенным и стал толчком для дальнейшего развития технологий виртуализации, в ходе которого появился третий подход к построению ЦСОД.

1.2.3 Кластеризация

Кластеризация ЦСОД – подход, при котором несколько серверов виртуализации собираются в общую логическую единицу (кластер). Данный подход также основывается на технологии виртуализации и виртуальных машин. Несколько серверов виртуализации имеют общее хранилище – систему хранения

данных (СХД). СХД специализированное устройство, имеющее большое количество жестких дисков. На СХД размещаются файлы виртуальных машин. Сервера виртуализации предоставляют виртуальным машинам свои ресурсы (ОЗУ, ЦПУ). Виртуальные машины переносятся с одного сервера виртуализации на другой без остановки и потери связи. При отказе одного сервера виртуализации виртуальные машины с данного сервера переносятся на другие сервера виртуализации, но с перезагрузкой. Логическая схема такого подхода показана на рисунке 10.

Данный подход не только имеет те же преимущества, что и подход с применением технологий виртуализации ЦСОД, но обладает рядом следующих преимуществ:

- Надежность. Отсутствие единой точки отказа, сервера полностью взаимозаменяемые. Отказ одного сервера виртуализации не приводит к катастрофическим отказам.

- Большая гибкость. Проводить обслуживание серверов, добавление аппаратных ресурсов можно без остановки программных комплексов и незаметно для пользователей.

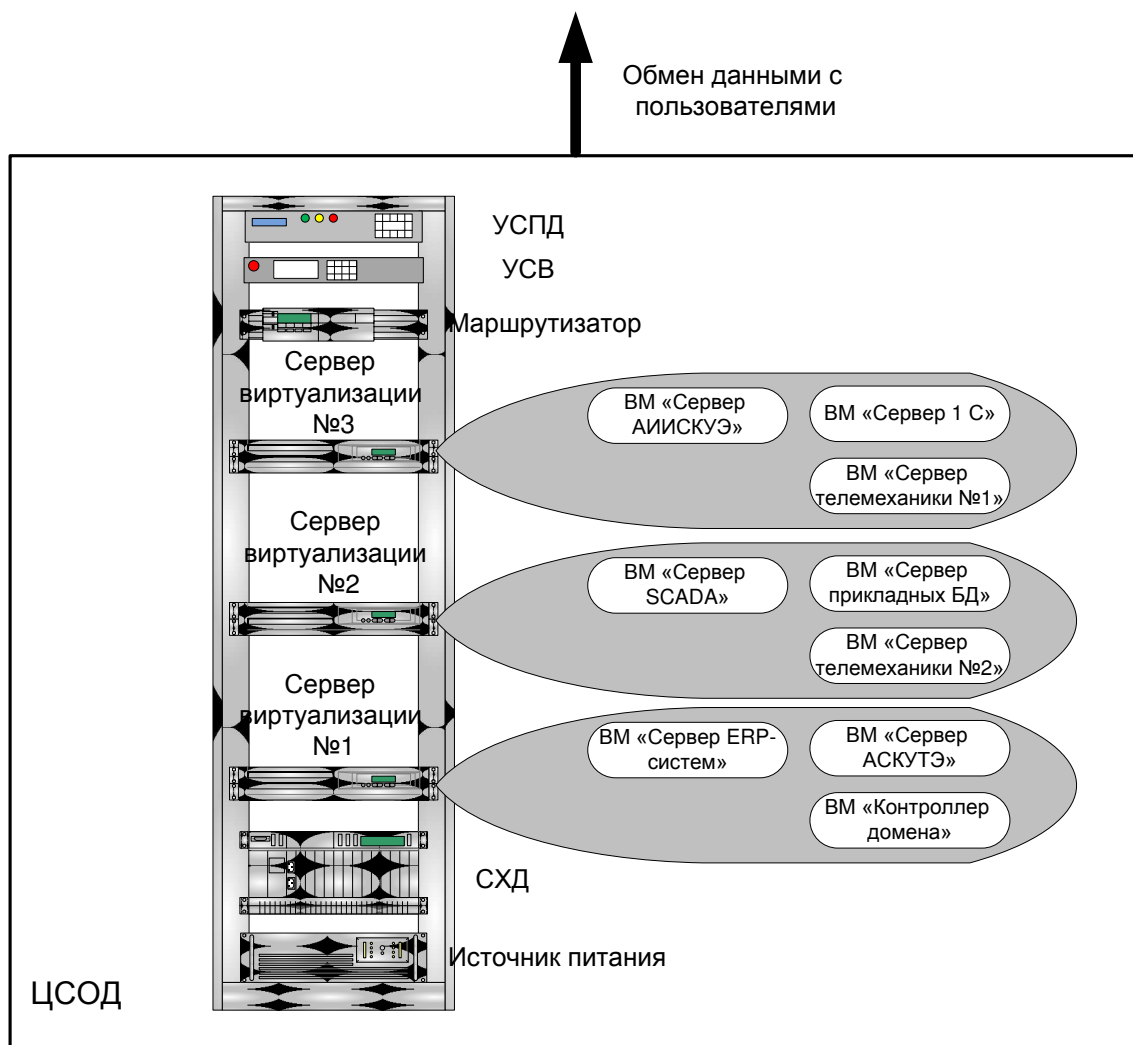


Рисунок 10 – Кластеризация ЦСОД

- Масштабирование. Увеличение вычислительных мощностей превращается в типовую задачу и происходит проще – увеличивается количество серверов виртуализации и СХД.

- Гибкость достижения необходимого уровня надежности. Количеством серверов виртуализации достигается необходимый уровень надежность. Можно довести количество серверов виртуализации до такого уровня, чтобы один сервер виртуализации могут обслуживать все виртуальные машины (максимальная надежность) при отказах оборудования. Надо понимать, что обратной стороной надежности является увеличение избыточности (стоимости) и уменьшение коэффициента использования оборудования.

При применении данного подхода решаются следующие недостатки виртуализации:

- Скачкообразное увеличение мощности. При добавлении новых узлов в кластер коэффициент использования серверов снижается незначительно. Чем больше количество узлов, тем меньше падает коэффициент.

- Единая точка отказа. Теперь сервера виртуализации не являются единственными точками отказа.

Остальные недостатки сохраняются и к ним добавляются следующие:

- Необходимость больших финансовых затрат на начальном этапе создания ЦСОД, т. к. необходимо больше оборудования (СХД, преобразователи и т. п.). Но в дальнейшем, при наращивании мощности данный подход потребует меньше средств, либо не потребует вовсе.

- Невозможность территориального разнесения кластера. На данном этапе развития виртуализации не рекомендуется территориально разносить кластер. Все сервера кластера виртуализации должны находиться в одном помещении или в соседних помещениях.

На данный момент классический подход построения ЦСОД уже начинает устаревать и является неперспективным. Подход кластеризации ЦСОД является самым перспективным и современным. В перспективе, при дальнейшем развитии технологий кластеризации и виртуализации, оставшиеся недостатки такого подхода к построению ЦСОД будут решены.

1.3. Особенности ЦСОД предприятий энергетического комплекса

На построение ЦСОД накладываются определенные ограничения некоторые особенности электроэнергетики. Таким особенностями являются: наличие устаревшего ПО, наличие специфического оборудования, требования контролирующих органов, использование самостоятельно разработанного ПО для решения локальных задач. Рассмотрим данные особенности более подробно.

Использование устаревшего ПО, не поддерживающего современные технологии и версии ОС вызвано давним внедрением данного ПО. Реформирование энергетической отрасли было связано с формированием современного рынка электроэнергии (ОРЭМ), правил, регламентов и структуры и активно происходило в 2005-2008 годах. В этот временной промежуток все предприятия электроэнергетики внедряли программные комплексы из-за требований контролирующих органов, для того чтобы иметь возможность работы по новым правилам. В дальнейшем ПО не модернизировалось и не приобретались новые версии, т. к. переход на новую версию ПО связан со значительными финансовыми затратами. Новый функционал новых версий ПО не обеспечивал рентабельность данных затрат.

В электроэнергетике используются такие специфические комплексы как АИИСКУЭ, ССПИ, АСКУТЭ. Для обеспечения надежности данные системы строятся по иерархическому многоуровневому принципу. Данное оборудование невозможно виртуализировать и оно накладывает ограничение сервера. Необходимо использовать устаревшие СОМ-порты на серверах, либо использовать сервера с СОМ-портами для консолидации и преобразования СОМ в Ethernet. Современная тенденция в серверном оборудовании это уход от СОМ-портов. Также в электроэнергетике используется специфичное оборудование: устройства синхронизации, устройства сбора и передачи данных и т. п. Данные устройства также невозможно виртуализировать.

Энергетическая отрасль является стратегической для государства и населения, поэтому в данной отрасли существуют жесткие требования к оборудованию и надежности для снижения аварийности. Во времена существования СССР энергетическая отрасль строилась как единая система, из-за этого вытекает необходимость в настоящее время поддержания данной системы как единого организма. Так как в настоящее время различные генерирующие мощности принадлежат различным компаниям, то необходимо устанавливать более жесткие требования для поддержания отрасли как единой системы. Для этих целей были сформированы государственные региональные диспетчерские цен-

тры (РДУ) для управления и контроля над энергетической системой. Для обеспечения такого контроля все генерирующие предприятия обязаны в режиме реального времени передавать информацию об основных параметрах генерирующего оборудования в РДУ. Из этого вытекает высокие требования к надежности системы сбора и передачи данных (ССПИ) в РДУ. Данная система должна работать в режиме «24/7».

Последняя особенность возникла из-за пути развития электроэнергетики при возникновении рыночных отношений и краха СССР. До начала реформы энергетики (до 2005-2006 годов) все генерирующие мощности были независимы друг от друга и развивались независимо. Каждая станция выбирала свой путь информатизации – где-то разрабатывалось собственное ПО силами персонала станции, на других станциях приобреталось ПО. После реформы электроэнергетики и объединения генерирующих мощностей в крупные ТГК и ОГК появилась проблема унификации информационных комплексов и консолидация информации от всех станций. Самостоятельно разработанные программные комплексы трудно увязать в единую общую информационную систему, приходится держать персонал, знающий именно данный программный комплекс, трудно перевести пользователей станции с самостоятельно разработанного ПО на новое единое.

Данные особенности энергетики необходимо учитывать при выборе подхода к построению ЦСОД на предприятиях электроэнергетики.

2 Исследование технологии виртуализации

2.1 Обзор наиболее популярных гипервизоров

При классическом подходе «один сервер – одна роль» затрудняется проведение технического обслуживания (далее – ТО) сервера, ремонтные работы, увеличение ресурсов, т. к. для этого необходимо отключать физический сервер. Это приводит к необходимости остановки определенного программного комплекса. При таком подходе при выходе из строя сервера останавливается работа

программного комплекса. Для важных программных комплексов это может быть очень критично. Наличие данных ограничений послужило толчком к развитию технологии виртуализации серверов на базе гипервизоров.

Гипервизор (англ. Hypervisor) или Монитор виртуальных машин (в компьютерах) — программа или аппаратная схема, обеспечивающая или позволяющая одновременное, параллельное выполнение нескольких операционных систем на одном и том же физическом сервере. Гипервизор также обеспечивает изоляцию операционных систем друг от друга, защиту и безопасность, разделение ресурсов между различными запущенными ОС и управление ресурсами. Изолированная операционная система с определенным набором ресурсов и виртуального оборудования, выполняемая на гипервизоре называется виртуальной машиной.

Гипервизор также может предоставлять, работающим под его управлением виртуальным машинам, средства связи и взаимодействия между собой (например, через обмен файлами или сетевые соединения) так, как если бы ОС виртуальных машин выполнялись на разных физических компьютерах.

Гипервизор сам по себе в некотором роде является минимальной операционной системой (микроядром или наноядром). Он предоставляет запущенным под его управлением операционным системам сервис виртуальной машины, виртуализируя или эмулируя реальное (физическое) аппаратное обеспечение конкретной машины. И управляет этими виртуальными машинами, выделением и освобождением ресурсов для них. Гипервизор позволяет независимые «включение», перезагрузку, «выключение» любой из виртуальных машин с той или иной ОС. При этом операционная система, работающая в виртуальной машине под управлением гипервизора, может, но не обязана «знать», что она выполняется в виртуальной машине, а не на реальном аппаратном обеспечении.

Виртуальная машина (VM, от англ. virtual machine) — программная и/или аппаратная система, эмулирующая аппаратное обеспечение некоторой платформы и исполняющая программы.

Виртуальная машина исполняет некоторый машинно-независимый код или машинный код реального процессора. Помимо процессора, ВМ может эмулировать работу как отдельных компонентов аппаратного обеспечения, так и целого реального компьютера (включая BIOS, оперативную память, жёсткий диск и другие периферийные устройства). В последнем случае в ВМ, как и на реальный компьютер, можно устанавливать операционные системы (например, Windows можно запускать в виртуальной машине под Linux или наоборот). На одном компьютере может функционировать несколько виртуальных машин.

VMware ESXi Server — программный продукт для виртуализации уровня предприятия, предлагаемый компанией VMware в качестве компонента VMware vSphere [41; 42].

ESXi является встроенным гипервизором и ставятся непосредственно «на железо», то есть при установке не требуют наличия на машине установленной операционной системы.

ESX/ESXi позволяет разделить физический компьютер на логические разделы, называемые виртуальными машинами. Включает в себя средства управления виртуальными ресурсами. Предъявляет определённый набор требований к аппаратному обеспечению — в частности, является обязательным наличие поддержки виртуализации со стороны процессора.

Xen — кроссплатформенный гипервизор, разработанный в компьютерной лаборатории Кембриджского университета и распространяемый на условиях лицензии GPL [43; 44]. Основные особенности: поддержка режима паравиртуализации помимо аппаратной виртуализации, минимальность кода самого гипервизора за счёт выноса максимального количества компонентов за пределы гипервизора.

Основной концепцией гипервизора является домен. Доменом называется запущенная копия виртуальной машины. Если виртуальная машина перезагружается, то её домен завершается (в момент перезагрузки) и появляется новый домен. Более того, даже при миграции содержимое копируется из одного домена в другой домен. Таким образом, за время своей жизни практически все вир-

туальные машины оказываются по очереди в разных доменах. Xen оперирует только понятием домена, а понятие «виртуальной машины» появляется на уровне администрирования (прикладных программ, управляющих гипервизором).

Домены бывают нескольких типов. Самые известные `dom0` и `domU`. `dom0` — первый запущенный Xen домен, обычно он автоматически создаётся и загружается сразу после загрузки и инициализации гипервизора. Этот домен имеет особые права на управление гипервизором и по умолчанию всё аппаратное обеспечение компьютера доступно из `dom0`. Фактически, `dom0` — это место жизни ПО, управляющего Xen. `dom0` всегда один.

`domU` — рядовой домен (сокращение от User domain), содержащий в себе домен выполняющихся виртуальных машин. Обычно не имеет доступа к реальному оборудованию и является «полезной нагрузкой» системы виртуализации. В отличие от `dom0`, `domU` может быть множество (обычно несколько десятков).

`stub-domain` — домен, в котором запущена очень специализированная ОС, обеспечивающая работу с каким-либо оборудованием или бэк-эндом драйвера. Является развитием модели безопасности Xen.

`domain builder` (конструктор доменов) — программа, которая создаёт `domU` (загружает в него нужный код и сообщает гипервизору о необходимости запуска). Помимо конструирования домена, обычно занимается подключением и конфигурированием виртуальных устройств, доступных для виртуальной машины. Она же отвечает за процесс миграции виртуальной машины с хоста на хост.

Microsoft Hyper-V — система аппаратной виртуализации для x64-систем на основе гипервизора. Бета-версия Hyper-V была включена в x64-версии Windows Server 2008, а финальная версия (автоматически, через Windows Update) была выпущена 26 июня 2008 [32; 33; 35]. Ранее была известна как виртуализация Windows Server (Windows Server Virtualization).

Hyper-V существует в двух вариантах: как отдельный продукт Microsoft Hyper-V Server и как роль Windows Server.

Отдельная версия Hyper-V Server является бесплатной. Является базовым («Server Core») вариантом Windows Server 2008, то есть включает в себя полную функциональность Hyper-V, прочие роли Windows 2008 Server отключены, также лимитированы службы Windows. Бесплатная 64-битная Core-версия Hyper-V ограничена интерфейсом командной строки (PowerShell), где конфигурация текущей ОС, физического аппаратного и программного оборудования выполняется при помощи команд оболочки. Новое меню интерфейса управления позволяет выполнить простую первичную конфигурацию, а некоторые свободно распространяемые скрипты расширяют данную концепцию. Администрирование и конфигурирование виртуального сервера (или гостевых ОС) осуществляется при помощи ПО, установленного на ПК под управлением Windows Vista, Windows 7 или Windows 2008 Server с установленным дополнением для администрирования Hyper-V из MMC. Другим вариантом администрирования/конфигурирования сервера Windows 2008 Core является использование удаленной Windows или Windows Server при перенаправлении (некоторой) консоли управления (MMC), указывающей на Core Server. Это значительно упрощает настройку, сводя её к нескольким кликам мыши.

Hyper-V поддерживает разграничение согласно понятию раздел. Раздел — логическая единица разграничения, поддерживаемая гипервизором, в котором работают операционные системы. Каждый экземпляр гипервизора должен иметь один родительский раздел, с запущенной Windows Server 2008. Стек виртуализации запускается на родительском разделе и обладает прямым доступом к аппаратным устройствам. Затем родительский раздел порождает дочерние разделы, на которых и располагаются гостевые ОС. Дочерний раздел также может породить собственные дочерние разделы. Родительский раздел создает дочерние при помощи API-гипервизора, представленного в Hyper-V.

Виртуализированные разделы не имеют ни доступа к физическому процессору, ни возможности управлять его реальными прерываниями. Вместо этого у них есть виртуальное представление процессора и гостевой вирту-

альный адрес, зависящий от конфигурации гипервизора, вовсе необязательно при этом занимающий все виртуальное адресное пространство. Гипервизор может определять подмножество процессоров для каждого раздела. Гипервизор управляет прерываниями процессора и перенаправляет их в соответствующий раздел, используя логический контроллер искусственных прерываний (Synthetic Interrupt Controller или сокр. SynIC). Hyper-V может аппаратно ускорять трансляцию адресов между различными гостевыми виртуальными адресными пространствами при помощи IOMMU (I/O Memory Management Unit — Устройство управления вводом-выводом памяти), которое работает независимо от аппаратного управления памятью, используемого процессором.

Дочерние разделы не имеют непосредственного доступа к аппаратным ресурсам, но зато получают виртуальное представление ресурсов, называемое виртуальными устройствами. Любая попытка обращения к виртуальным устройствам перенаправляется через VMBus к устройствам родительского раздела, которые и обработают данный запрос. VMBus — это логический канал, осуществляющий взаимодействие между разделами. Ответ возвращается также через VMBus. Если устройства родительского раздела также являются виртуальными устройствами, то запрос будет передаваться дальше, пока не достигнет такого родительского раздела, где он получит доступ к физическим устройствам. Родительские разделы запускают провайдер сервиса виртуализации (Virtualization Service Provider или сокр. VSP), который соединяется с VMBus и обрабатывает запросы доступа к устройствам от дочерних разделов. Виртуальные устройства дочернего раздела работают с клиентом сервиса виртуализации (Virtualization Service Client или сокр. VSC), который перенаправляет запрос через VMBus к VSP родительского раздела. Этот процесс прозрачен для гостевой ОС.

Виртуальные устройства также поддерживают технологию Windows Server Virtualization, называемую прогрессивный ввод-вывод (англ. Enlightened I/O), для накопителей, сетевых и графических подсистем в том числе. Enlightened I/O — специализированная виртуализационная реализация высоко-

уровневых протоколов, как, например, SCSI, для возможности работать с VMbus напрямую, что позволяет параллельно обрабатывать любые уровни эмуляции устройства. Это делает взаимодействие более эффективным, но взамен требует от гостевой ОС поддержки Enlightened I/O. Только Windows Server 2008 R2, Windows Server 2008, Windows 7, Windows Vista, Red Hat Enterprise Linux и SUSE Linux сейчас обладают поддержкой Enlightened I/O, позволяющей им работать быстрее в качестве гостевых ОС под Hyper-V по сравнению с прочими операционными системами, которым требуется более медленная эмуляция устройств.

2.2 Сравнение параметров гипервизоров

Для корректного сравнения гипервизоров различных производителей необходимо учесть несколько особенностей. Первая особенность это необходимость выделения характеристик, критичных для гипервизоров. Определив такие характеристики проводить оценку и сравнение по ним. Вторая особенность это необходимость выбрать равноценные версии гипервизоров. Производители гипервизоров постоянно улучшают свое ПО, поэтому необходимо у каждого производителя выбрать определенную версию ПО. Версии ПО различных производителей должны быть выпущены примерно в одно и то же время. Третья особенность это необходимость учитывать редакцию гипервизора. У производителей гипервизоров одна и та же версия гипервизора может иметь несколько редакций. Различные редакции одной и той же версии гипервизора могут отличаться по возможностям, поддерживаемым функциям и цене.

Как уже говорилось в Разделе 2.1, на данный момент есть три ведущих производителя гипервизоров – Microsoft (Hyper-V), Citrix (Xen), VMware (vSphere). Для корректного сравнения выбираем близкие по времени выхода версии продукта. Для сравнения от Microsoft выбираем версию Windows Server 2012R2, в данную ОС включен гипервизор. Для Citrix выбираем версию XenServer 6.0. Для VMware выбираем версию vSphere 5.5. Все эти версии выпущены в 2013 году.

Теперь рассмотрим существующие редакции данных версий продуктов у каждого производителя. У Microsoft имеет две редакции: Standard и Datacenter. Обе редакции не отличаются по возможностям и поддерживаемым функциям. Основное различие редакций это схема лицензирования виртуальных машин. В редакции Standard все виртуальные машины лицензируются за отдельную плату. В версии Datacenter все виртуальные машины с ОС Windows не надо лицензировать. Исходя из изложенного, можно сделать вывод, что для оценки функциональности гипервизора Microsoft редакция гипервизора не важна. У Citrix XenServer есть две редакции: бесплатная и платная. Бесплатная редакция имеет ограниченный функционал и предназначена для использования в ознакомительных или обучающих целях. В платной редакции имеется весь функционал данного производителя. Для сравнения XenServer с другими гипервизорами мы будем использовать платную редакцию. У гипервизора от VMware имеется две редакции: Standard и Enterprise Plus. Редакция Standard имеет ограничение по Масштабируемость и поддерживаемым функциям. Функциональность данной редакции значительно уступает гипервизорам от Microsoft и Citrix. Редакция Enterprise Plus имеет максимально возможный функционал данного производителя, поэтому при сравнении гипервизоров будем использовать данную редакцию.

Для дальнейшего корректного сравнения гипервизоров необходимо определить параметры, по которым мы будем сравнивать их. Первая группа параметров, по которым можно сравнить гипервизоры это параметры масштабируемости и максимального количества ресурсов, выделяемых виртуальной машине. Сравнение по этим параметрам предоставлено в Таблице 1 [24].

Таблица 1 – Сравнение параметров гипервизоров

Группа	Параметр	Windows Server 2012R2	vSphere 5.5 Enterprise +	XenServer 6.0
Сервер	Макс ЛЦПУ, шт.	320	320	160
	Макс ЦПУ, шт.	2048	4096	4000
	Макс ОЗУ, Тб.	4	4	1
	Макс ВМ, шт.	1024	1024	512
Кластер	Макс Хост, шт.	64	32	16

	Макс ВМК, шт.	8000	4000	1000
VM	Макс ЦПУ VM, шт.	64	64	16
	Макс ОЗУ VM, Гб.	1024	1024	128
	Макс диск, Тб	64	62	16

Расшифруем параметры, указанные в Таблице 1, для лучшего понимания.

Макс ЛЦПУ – максимальное количество логических процессоров на физическом сервере. Данный параметр определяет максимальное количество ядер процессоров, поддерживаемое гипервизором.

Макс ЦПУ – максимальное количество логических процессоров на сервере. Данный параметр определяет количество процессоров, которое может быть отдано всем виртуальным машинам на физическом сервере.

Макс ОЗУ – максимальное количество ОЗУ на физическом сервере, поддерживаемое гипервизором.

Макс VM – максимально возможное количество виртуальных машин на одном физическом сервере.

Макс Хост – максимальное количество физических серверов (хостов), которые могут объединиться в кластер.

Макс ВМК – максимальное количество виртуальных машин, которые могут быть развернуты в кластере серверов.

Макс ЦПУ VM - максимальное количество ЦПУ, которое физический сервер может предоставить одной виртуальной машине.

Макс ОЗУ VM – максимальное количество ОЗУ, которое физический сервер может предоставить одной виртуальной машине.

Макс диск – максимальный размер диска в виртуальной машине.

Как видно из Таблицы 1 по параметрам масштабирования гипервизоры VMware и Microsoft имеют паритет. Пределы масштабирования, предлагаемые этими производителями на данный момент, со значительным запасом перекрывают потребности современных ЦСОД. Пределы масштабирования XenServer значительно ниже. Узким местом в параметрах XenServer являются ограничения параметров VM (ОЗУ, ЦПУ, диск). Ограничения по параметрам VM в

XenServer могут уже не удовлетворять требованиям ЦСОД средних масштабов (средний бизнес).

Гипервизоры так же необходимо сравнить по важным функциональным параметрам. Такое сравнение сделано в Таблице 2.

Таблица 2 – сравнение функциональных возможностей гипервизоров

Параметр	Windows Server 2012R2	vSphere 5.5 Enterprise +	XenServer 6.0
Поддержка МPIO	есть	есть	есть
Live Migration	есть	есть	есть
Одновременное LM, шт.	Не ограничено	4	Нет данных
Live Storage Migration	есть	есть	есть
Репликация ВМ	есть	нет	нет
Динамическая память	есть	есть	есть
Добавление ресурсов	есть	есть	есть
Шифрование дисков	есть	есть	есть
Правила распределения ВМ	есть	есть	нет

Расшифруем параметры, указанные в Таблице 2, для лучшего понимания.

Поддержка МPIO – поддержка функции распределения нагрузки между каналами, при резервировании каналов.

Live Migration – перенос виртуальной машины с одного физического сервера на другой без выключения виртуальной машины.

Одновременное LM – максимальное количество виртуальных машин, которые могут одновременно мигрировать с одного физического сервера на другой.

Live Storage Migration – поддержка функции переноса файлов виртуальных машин с одного RAID-массива на другой в рамках одной СХД.

Репликация ВМ – постоянное клонирование (репликация) виртуальной машины из одного кластера серверов в другой кластер с определенной периодичностью.

Динамическая память – возможность выделения ОЗУ виртуальной машине динамически. Виртуальной машине задается максимальное и минимальное

количество ОЗУ. Память выделяется виртуальной машине в заданных рамках в зависимости от запросов самой виртуальной машины.

Добавление ресурсов – возможность добавлять виртуальной машине ресурсы (ЦПУ, ОЗУ, диски и т. п.) без выключения самой виртуальной машины.

Шифрование дисков – функция шифрования дисков виртуальных машин для обеспечения безопасности данных.

Правила распределения ВМ – возможность создание правил, определяющих распределение определенных виртуальных машин по серверам кластера.

Из Таблицы 2 видно, что полным набором функций обладает гипервизор Microsoft. Гипервизор VMware не имеет функцию репликации. Гипервизор Citrix не имеет функций репликации и правил распределения виртуальных машин.

Из сравнения параметров, заявленных разработчикам гипервизоров, можно сделать вывод, что гипервизор XenServer от Citrix значительно уступает двум другим гипервизорам. Гипервизоры Microsoft и VMware близким по характеристикам и набору функций. Гипервизор Microsoft больше нацелен на поддержку виртуальных машин на базе ОС производства Microsoft. Гипервизор VMware больше нацелен на поддержку ОС семейства Unix/Linux. Поскольку в России в целом и в энергетике в частности больше распространены ОС семейства Microsoft, то в ходе дальнейшего исследования и моделирования будет использоваться гипервизор от Microsoft.

2.3 Моделирование центров сбора и обработки данных в программной среде AnyLogic.

Для экспериментального сравнения подходов к построению ЦСОД были построены соответствующие модели в среде имитационного моделирования AnyLogic [14; 28].

AnyLogic — программное обеспечение для имитационного моделирования, разработанное российской компанией The AnyLogic Company (бывшая «Экс Джей Текнолоджис»). Инструмент обладает современным графическим ин-

терфейсом и позволяет использовать язык Java для разработки моделей. Версия AnyLogic PLE доступна бесплатно для образовательных целей и самообучения. Данный продукт поддерживает следующие методы моделирования: системная динамика, дискретно-событийное моделирование, агентное моделирование. Также AnyLogic поддерживает любую комбинацию данных методов моделирования в рамках одной модели. AnyLogic поддерживает разработку моделей в следующих областях: производство, логистика, сфера обслуживания, здравоохранение, фармацевтика, телекоммуникации, информационные системы, оборона, дорожное движение, экологическая система, социальная система, управление проектами. В рамках политики лицензирования существует несколько редакций AnyLogic: PLE, University Researcher, Professional. PLE редакция бесплатна, в отличие от остальных, предназначена для обучения работе с программой и простейшего моделирования. PLE поддерживает все методы моделирования и полно функциональна. Основные отличия бесплатной версии от платных – количество библиотек, поддержка специфичных функций, техническая поддержка, поддержка работы со сторонними СУБД [13; 23]. На рисунке 11 показан основной интерфейс программы.

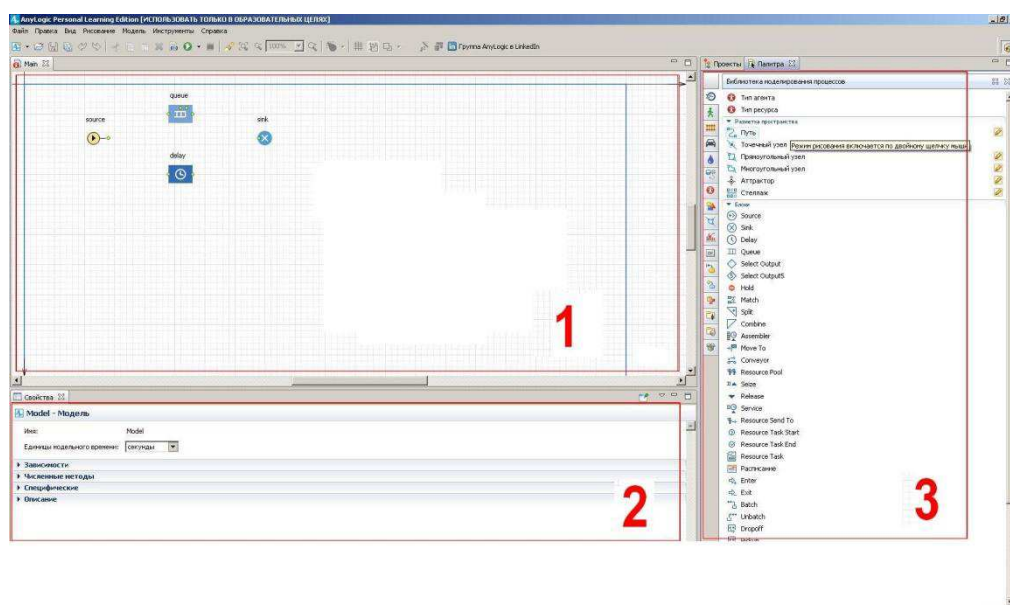


Рисунок 11 – Интерфейс AnyLogic

Область №1 на рисунке 11 – область моделирования. В данной области отображаются элементы моделирования и визуализация модели. Область №2 на рисунке 11 – область свойств элемента. В этой области отображаются и редактируются свойства выбранного элемента. Область №3 на рисунке 11 - библиотека элементов. В этой области отображаются доступные элементы в библиотеке.

Для создания модели, необходимо определить по каким параметрам будут сравниваться различные подходы к построению ЦСОД (классический и виртуализация/кластеризация).

Первая группа параметров для сравнения - параметры эффективности ЦСОД. К параметрам эффективности ЦСОД относятся: потребление электрической энергии северным оборудованием, мощность системы охлаждения, количество занятых портов в сетевом оборудовании. Группа этих параметров характеризует эффективность использования прочих систем ЦСОД. Основываясь на вышеизложенных теоретических рассуждениях виртуализация (кластеризация) должна приводить к увеличению эффективности ЦСОД, т. е. должны уменьшиться все указанные параметры.

Вторая группа параметров – надежность серверного оборудования. К данной группе относятся: время простоя оборудования после аварий, время простоя оборудования при проведении технического обслуживания, скорость переноса ресурсов на другое оборудование. Данные параметры характеризуют надежность работы оборудования и гибкость серверного оборудования ЦСОД. Основываясь на предыдущих теоретических рассуждениях данные параметры должны уменьшаться при использовании кластеризации.

Третья группа параметров – эффективность использования серверного оборудования. К данным параметрам относятся: расход ресурсов серверного оборудования на работу гипервизора, эффективность использования ресурсов сервера. Теоретически при использовании кластеризации эффективность использования ресурсов должна увеличиваться.

Для построения модели необходимо часть параметров получить в ходе натурального эксперимента. В качестве платформы для натурального эксперимента будет использоваться следующее оборудование и ПО:

- Корзина для Blade-серверов IBM Blade Center E;
- Два сервера лезвия IBM HS21 (1 процессор Intel Xeon E5420 2,5 ГГц, 8 ядер, 16 Гб ОЗУ, RAID1, 2 диска 136 Гб) – используются в качестве серверов виртуализации и объединены в кластер;
- СХД IBM DS4200 (два RAID10 по 4 шт. дисков 500 Гб в каждом);
- Microsoft Windows Server 2012R2 Data Center с Hyper-V;
- Две виртуальные машины с ОС Microsoft Windows Server 2012R2 Standard, каждой выделен виртуальный диск в 40 Гб.

СХД используется для хранения виртуальных машин. Сервера подключены к СХД напрямую с помощью оптического кабеля. Конфигурация сервера виртуализации показана на рисунке 12.

Operating system version	Microsoft Windows Server 2012 R2 Datacenter
Hardware information	IBM IBM eServer BladeCenter HS21 -[8853G3G]-
Processors	Intel(R) Xeon(R) CPU E5420 @ 2.50GHz, Intel(R) Xeon(R) CPU
Installed memory (RAM)	16 GB
Total disk space	136.39 GB

Рисунок 12 – Конфигурация сервера виртуализации

Первым параметром, полученным в ходе натурального эксперимента, будет скорость выполнения миграции ВМ на другой сервер виртуализации (Live Migration). Дополнительно будет анализироваться количество потерянных пакетов при миграции с помощью команды ping. Данные параметры покажут время простоя виртуальной машины при миграции. Функция миграции используется для проведения ТО, увеличения ресурсов сервера виртуализации, проведения прочих работ.

Процесс миграции виртуальной машины был повторен для каждой виртуальной машины десять раз. Полученные в ходе эксперимента результаты указаны в Таблице 3.

Таблица 3 – Время миграции ВМ

№ эксперимента	№ ВМ	Время миграции, с.	Кол-во потерянных пакетов, шт.
1	ВМ №1	10	1
2	ВМ №1	9	1
3	ВМ №1	8	0
4	ВМ №1	7	0
5	ВМ №1	8	0
6	ВМ №1	9	0
7	ВМ №1	8	0
8	ВМ №1	8	0
9	ВМ №1	9	0
10	ВМ №1	7	0
11	ВМ №2	12	1
12	ВМ №2	10	1
13	ВМ №2	8	0
14	ВМ №2	9	0
15	ВМ №2	7	0
16	ВМ №2	7	0
17	ВМ №2	7	0
18	ВМ №2	8	0
19	ВМ №2	8	0
20	ВМ №2	7	0

По результатам эксперимента видно, что среднее время миграции составило 8,3 секунды. В процессе миграции было потеряно в среднем 0,2 пакета. На основании этого можно сделать вывод, что в процессе миграции пакеты практически не теряются. Для большинства ПО потеря одного или двух пакетов не критична. Отсюда следует вывод, что при миграции время простоя ВМ равно нулю.

Следующим параметром, полученным в ходе натурального эксперимента, будет время простоя при отказе сервера виртуализации. В рамках данного эксперимента будет моделироваться ситуация отказа сервера виртуализации. От-

каз сервера виртуализации будет имитироваться путем отключения питания сервера и последующим включением питания. При неожиданном отключении сервера виртуализации, виртуальные машины, запущенные на этом сервере останавливаются и выключаются. Другой сервер виртуализации захватывает управление данными виртуальными машинными, размещает их на своих ресурсах и запускает виртуальные машины (Quick migration). Со стороны ОС виртуальной машины это выглядит как перезагрузка виртуальной машины. Данный эксперимент моделирует нештатные ситуации с физическим оборудованием, такие как пропажа питания, ошибочные отключения, аппаратные сбои, выход из строя сервера и т. п.

Процесс отключения сервера виртуализации был повторен десять раз. Засекалось время между прекращением связи с виртуальной машиной и восстановлением связи, т. е. до момента полного запуска всех служб ВМ. Полученные в ходе эксперимента результаты указаны в Таблице 4.

Таблица 4 – Время перезагрузки ВМ

№ эксперимента	№ ВМ	Время перезагрузки ВМ, с.	Время перезагрузки сервера виртуализации ВМ, с.
1	ВМ №1	185	580
2	ВМ №1	153	603
3	ВМ №1	168	573
4	ВМ №1	180	589
5	ВМ №1	172	595
6	ВМ №2	145	625
7	ВМ №2	168	580
8	ВМ №2	170	575
9	ВМ №2	158	598
10	ВМ №2	163	602

По данным эксперимента среднее время перезагрузки ВМ при отключении сервера виртуализации составило 166,2 секунд. Низкое время перезагрузки также обусловлено использованием новой версии ОС Microsoft в ВМ. Для более старых версий ОС ВМ время перезагрузки будет больше. При этом время

перезагрузки сервера виртуализации было намного больше и в среднем составило 592 секунды.

Для сравнения также необходимо замерить время перезагрузки обычного сервера без установленной системы виртуализации. В качестве такого сервера будет использоваться аналогичная модель IBM HS 21 с такими же характеристиками что и сервера виртуализации. Но на данный сервер не будет устанавливаться гипервизор. Данный эксперимент будет имитировать отказ физического сервера при классическом подходе построения ЦСОД, т. е. без виртуализации.

Процесс отключения сервера был повторен десять раз. Засекалось время между прекращением связи с сервером и восстановлением связи, т. е. до момента полного запуска всех служб. Полученные в ходе эксперимента результаты указаны в Таблице 5.

Таблица 5 – Время перезагрузки сервера

№ эксперимента	Время перезагрузки сервера, с.
1	480
2	500
3	498
4	502
5	487
6	478
7	485
8	495
9	490
10	493

По данным эксперимента среднее время перезагрузки сервера при отключении питания составило 490,8 секунд. Более быстрая перезагрузка сервера в сравнении с серверов виртуализации объясняется отсутствием роли гипервизора. Разница между перезагрузкой виртуальной машины и физического сервера составляет 324,6 секунд.

Рассчитаем суммарное время простоя оборудования в год из-за выполнения ТО. По регламентам ООО «СГК» техническое обслуживание каждого физического сервера проводится два раза в год. Продолжительность ТО одного

сервера два часа. При использовании классического подхода суммарное время простоя в год при проведении ТО для одного сервера составит 4 часа. При использовании кластеризации время простоя при проведении ТО будет равно нулю, за счет использования функций Live Migration.

Третьим параметром, полученным экспериментально, будет количество ресурсов, затраченных на работу гипервизора. Сам гипервизор для обслуживания системы виртуализации и виртуальных машин потребляет часть процессорных ресурсов и ОЗУ. Из этого следует, что ПО установленное на физическом сервере будет иметь больше ресурсов, чем ПО установленное на виртуальной машине на таком же физическом сервере. Для определения ресурсоемкости гипервизора использовалась стандартная консоль Microsoft Failover Clustering. С помощью этой консоли определялась ресурсоемкость гипервизора на сервере виртуализации без развернутых виртуальных машин. Результат показан на рисунке 13 и рисунке 14.

Status:	Up
Node ID:	1
Uptime:	8 Days 11:34:4
Memory:	14.6 GB Available, 16.0 GB Total
Processors:	(8) Intel(R) Xeon(R) CPU E5420 @ 2.50GHz
CPU Usage:	0%
Operating System:	Microsoft Windows Server 2012 R2 Datacenter
Version:	6.3.9600
Service Pack:	No Service Pack Installed
System Type:	x64-based PC
Manufacturer:	IBM
Model:	IBM HS21

Рисунок 13 – Ресурсоемкость гипервизора сервера №1

Status:	Up
Node ID:	2
Uptime:	8 Days 11:34:4
Memory:	14.2 GB Available, 16.0 GB Total
Processors:	(8) Intel(R) Xeon(R) CPU E5420 @ 2.50GHz
CPU Usage:	1%
Operating System:	Microsoft Windows Server 2012 R2 Datacenter
Version:	6.3.9600
Service Pack:	No Service Pack Installed
System Type:	x64-based PC
Manufacturer:	IBM
Model:	IBM HS21

Рисунок 14 – Ресурсоемкость гипервизора сервера №2

По данным консоли Microsoft Failover Clustering видно, что сам гипервизор потребляет очень мало процессорных ресурсов и около 1-2 Гб ОЗУ.

Следующей рассматриваемой группой параметров будут параметры теплового выделения и электрического потребления серверов. Данные по тепловому потреблению будут получены с помощью стандартных средств отображения физического сервера. Данные средства отображения каждый производитель делает встроенными в сервер. Просмотреть эти данные можно с помощью веб-интерфейса. На рисунках 15, 16, 17 показано потребление физических серверов с различным ПО, но без установленной системы виртуализации. Данные сервера моделируют электрическое потребление и тепловое выделение физических серверов при классическом подходе к построению ЦСОД. На рисунке 15 показано потребление сервера БД АИИСКУЭ. На рисунке 16 показано потребление сервера ИКМ системы АИИСКУЭ. На рисунке 17 показано потребление сервера SCADA-системы.

Power History			
	5 min	20 min	24 hr
Average Power	164 Watts	167 Watts	164 Watts
Maximum Power	188 Watts	200 Watts	247 Watts
Minimum Power	162 Watts	162 Watts	156 Watts

Рисунок 15 – Электрическое потребление сервера БД АИИСКУЭ

Power History			
	5 min	20 min	24 hr
Average Power	133 Watts	134 Watts	132 Watts
Maximum Power	159 Watts	159 Watts	165 Watts
Minimum Power	133 Watts	133 Watts	131 Watts

Рисунок 16 – Электрическое потребление сервера ИКМ системы АИИ-СКУЭ

Power History			
	5 min	20 min	24 hr
Average Power	141 Watts	144 Watts	143 Watts
Maximum Power	193 Watts	193 Watts	209 Watts
Minimum Power	140 Watts	138 Watts	139 Watts

Рисунок 17 – Электрическое потребление сервера SCADA-системы

Как видно из рисунков среднее электрическое потребление сервера составляет примерно 150 Вт. Эти данные соответствуют данным полученным в ходе эксплуатации оборудования на станциях ООО «Сибирская генерирующая компания». При дальнейшем моделировании в AnyLogic будет считать электрическое потребление физического сервера при классическом подходе к построению ЦСОД равным 150 Вт. Данные модели серверов не показывают тепловое выделение сервера, т. к. они не новые. Тепловое выделение серверов необходимо будет вычислить. На рисунке 18 показана часть официальной документации к серверов, где указано тепловое выделение.

Power	
AC power supply (per power supply)	
Wattage	495 W, 750 W, or 1100 W
Heat dissipation	1908 BTU/hr maximum (495 W power supply)
 NOTE: Heat dissipation is calculated using the power supply wattage rating.	2891 BTU/hr maximum (750 W power supply)
	2843 BTU/hr maximum (750 W Titanium power supply)
	4100 BTU/hr maximum (1100 W power supply)

Рисунок 18 – Тепловое выделение сервера

Вычислим теперь, сколько теплового выделения приходится на один ватт потребленной электрической энергии, но перед этим переведем тепловое выделение из BTU/hr в метрические Вт по формуле (1):

$$(1)$$

—
—

Получаем, что один ватт потребленной электрической энергии приводит к выделению 1,13 Вт тепловой энергии. Рассчитаем тепловое выделение для физических серверов без установленной системы виртуализации:

Вт

Один сервер при классическом подходе к построению ЦСОД выделяет 170 Вт тепловой энергии. Эти данные будем в дальнейшем использовать при моделировании в AnyLogic.

Теперь проведем аналогичный анализ и вычисление для серверов виртуализации. В качестве источника будут использоваться сервера IBM HS21. На рисунках 19 и 20 показано тепловое выделение и электрическое потребление серверов.

Present Power Reading and Thresholds		
Status	Probe Name	Present Reading
<input checked="" type="checkbox"/>	System Board Pwr Consumption	266 W 908 BTU/hr

Рисунок 19 – Электрическое потребление сервера №1

Present Power Reading and Thresholds		
Status	Probe Name	Present Reading
<input checked="" type="checkbox"/>	System Board Pwr Consumption	252 W 860 BTU/hr

Рисунок 20 – Электрическое потребление сервера №2

Как видно из данных среднее электрическое потребление сервера виртуализации равно 260 Вт. Среднее тепловое выделение равно 884 BTU/hr. Переведя тепловое выделение из BTU/hr в Вт, получим среднее тепловое выделение равное 260 Вт. Более низкий коэффициент теплового выделение к потребленной электрической мощности обусловлен более новой моделью серверов. В дальнейшем при моделировании в AnyLogic будет считать потребление электрической энергии сервера виртуализации равным 260 Вт. Тепловое выделение также будет считать равным 260 Вт.

Рассмотрим ситуацию с сетевыми подключениями физических серверов к ЛВС. Подключение физических серверов к ЛВС осуществляется, путем подключения сервера к коммутатору. Коммутатор в свою очередь уже является одним из узлов ЛВС. При виртуализации виртуальные машины используют для передачи данных через ЛВС сетевые порты физического сервера виртуализации. Виртуальные машины делят, в соответствии с заданными правилами, пропускную способность сетевых портов сервера виртуализации между собой. Основываясь на опыте эксплуатации кластера виртуализации в Красноярском филиале ООО «Сибирская генерирующая компания», внедрении кластера виртуализации на Красноярской ТЭЦ-1 и рекомендациях разработчиков гипервизоров, будем считать, что на одном сервере виртуализации будет находиться, в среднем, десять виртуальных машин. Чаще всего сервера виртуализации имеют четыре сетевых порта для подключения к ЛВС. Из этого делаем вывод, что для одной виртуальной машины необходимо 0,4 сетевых порта. Данный параметр будем использовать при моделировании. При классическом подходе чаще всего используются сервера имеющие два сетевых порта для подключения к ЛВС. При моделировании будем считать, что при классическом подходе каждый физический сервер требует два сетевых порта в коммутаторе.

Перейдем к моделированию в AnyLogic. В AnyLogic было создано несколько моделей для моделирования разных параметров. В первой модели была смоделированы инженерные системы ЦСОД (электрическое питание и охлаждение). Перед запуском модели определялась мощность системы электрическо-

го питания (условные источники бесперебойного питания), мощность системы охлаждения (условны кондиционеры) и количество портов в сетевом оборудовании (условные коммутаторы). В процессе запуска модели проверялось, при каком количестве физических серверов или виртуальных машин будет, достигнут предел мощности инженерных систем ЦСОД. На данной модели сравнивались два подхода к созданию ЦСОД: классический и виртуализация.

Инженерные системы ЦСОД были представлены как компоненты системы массового обслуживания. В начале, создавалась заявка на ресурсы, т. е. необходимость в новом физическом сервере или виртуальной машине. Данная заявка дублировалась и передавалась на два подхода к построению ЦСОД. В дальнейшем виртуальная машина или физический сервер были представлены как сущность, для обслуживания которой необходимы ресурсы. В качестве ресурсов были представлены мощность системы электропитания, мощность системы охлаждения и количество портов в коммутаторе. Для данной сущности было выставлено очень большое время обслуживания. Заявки на создание нового сервера или виртуальной машины появлялись с заданной частотой. Таким образом моделировалась ситуация при которой в ЦСОД нельзя будет разместить новый сервер или виртуальную машину из-за достижения предела по инженерным системам ЦСОД. На данной модели будет видно, какой подход к построению ЦСОД более экономично расходует ресурсы инженерных систем ЦСОД. Удельное потребление электрической энергии, теплового выделения и количества портов были взяты из описанного выше натурального эксперимента. При моделировании классического подхода было условно принято, что для каждого программного комплекса используется отдельный физический сервер. Процесс моделирования показан на рисунке 21.

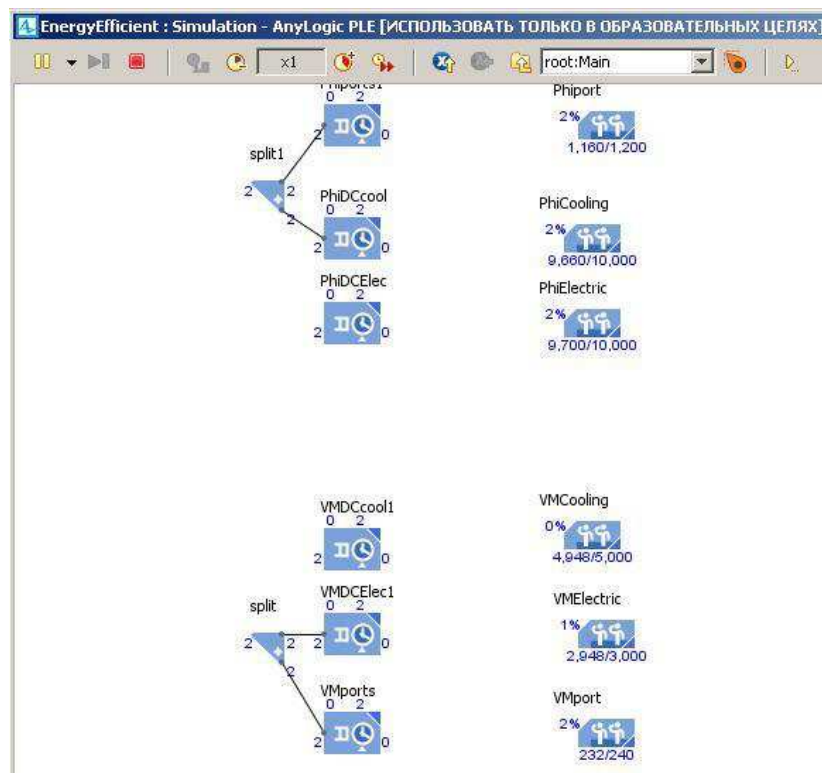


Рисунок 21 – Моделирования инженерных систем ЦСОД

Данные моделирования отображены в таблице 6, таблице 7 и таблице 8. Для каждого заданных параметров инженерных систем ЦСОД запуск модели осуществлялся десять раз. В таблице отображено среднее значение для каждой группы из десяти попыток.

Таблица 6 – Результаты моделирования инженерных систем ЦСОД

№	Мощность системы охлаждения, Вт	Мощность системы электропитания, Вт	Количество портов в коммутаторе, шт.	Кол-во серверов / VM при достижении предела, шт.
1	5000	3000	24	12
2	5000	3000	48	20
3	5000	5000	48	24
4	5000	5000	72	30
5	7500	5000	72	33
6	7500	6000	72	36
7	7500	6000	96	40
8	7500	8000	96	44
9	10000	8000	96	48
10	10000	8000	120	53
11	10000	10000	120	58
12	12500	10000	120	60

Таблица 7 – Предел инженерных систем ЦСОД

№	Тип подхода	Тип инженерной системы
1	Классический	Сеть передачи данных
2	Классический	Электропитание
3	Классический	Сеть передачи данных
4	Классический	Охлаждение
5	Классический	Электропитание
6	Классический	Сеть передачи данных
7	Классический	Электропитание
8	Классический	Охлаждение
9	Классический	Сеть передачи данных
10	Классический	Электропитание
11	Классический	Охлаждение
12	Классический	Сеть передачи данных

Таблица 8 – Ресурсоемкость системы виртуализации

№	Необходимая мощность системы охлаждения, Вт	Потребление электроэнергии, Вт	Кол-во портов в коммутаторе, шт.	Количество необходимых серверов виртуализации	Кол-во серверов / ВМ при достижении предела, шт.
1	260	260	4	1	12
2	520	520	8	2	20
3	780	780	12	3	24
4	780	780	12	3	30
5	1040	1040	16	4	33
6	1040	1040	16	4	36
7	1040	1040	16	4	40
8	1300	1300	20	5	44
9	1300	1300	20	5	48
10	1560	1560	24	6	53
11	1560	1560	24	6	58
12	1560	1560	24	6	60

Столбец «Кол-во серверов/ВМ при достижении предела» в таблице 6, показывает количество серверов или виртуальных машин, при котором моделирование было остановлено из-за достижения предела мощности инженерных систем ЦСОД. В таблице 7 в столбце «Тип подхода» указывается при каком под-

ходе к построению ЦСОД был, достигнут предел инженерных систем (остановка моделирования). В таблице 7 в столбце «Тип инженерной системы» указывается по какой из трех инженерных систем наступил предел. В таблице 8 отображены данные по потреблению и необходимому количеству серверов виртуализации. Количество серверов виртуализации рассчитывалось исходя из соотношения – один сервер виртуализации для 10-12 виртуальных машин.

Как видно из результатов в ходе моделирования и при любых начальных параметрах предел по инженерным системам происходил при использовании классического подхода к построению ЦСОД. В 5 случаях из 12 предел достигался по количеству портов сети передачи данных. В 4 случаях из 12 предел достигался по системе электропитания. В 3 случаях из 12 предел достигался по системе охлаждения. При этом при использовании кластеризации, инженерные системы были загружены следующим образом: электропитание 15-20%, охлаждение 10-15%, сетевые порты 5-10%. Из результатов моделирования можно также сделать вывод, что даже при снижении плотности размещения ВМ до 3-5 ВМ на сервер виртуализации кластеризация будет приводить к меньшему потреблению ресурсов инженерных систем ЦСОД. Благодаря этому моделированию было подтверждено теоретическое предположение, что использование виртуализации и кластеризации при построении ЦСОД дает снижение потребления электрической энергии, снижению необходимой мощности системы охлаждения и уменьшению количества кабельных линий ЛВС и сетевого оборудования.

В ходе следующего моделирования в AnyLogic было исследовано скорость сетевого взаимодействия и загруженность сети. На данной модели было смоделировано сетевое взаимодействие между серверами кластера (при виртуализации) и между физическими серверами (классический подход).

При использовании кластеризации сетевое взаимодействие происходит следующим образом. Виртуальные машины, расположенные на одном сервере виртуализации, взаимодействуют друг с другом, не используя ЛВС. Виртуальные машины взаимодействуют между собой за счет использования SAN-сети.

SAN-сеть это изолированная от ЛВС сеть между серверами виртуализации и СХД. Пропускная способность SAN-сети определяется используемыми протоколами. Для протокола SAS в настоящее время это 6 или 12 Гбит/сек. Для Fiber Channel 8 или 16 Гбит/сек. Если виртуальные машины расположены на различных серверах виртуализации, то взаимодействие между ними будет происходить по ЛВС. Современные коммутаторы для ЛВС поддерживают скорость передачи данных по одному порту 1 Гбит/сек. Общая максимальная пропускная способность коммутатора ЛВС зависит от модели.

При моделировании были сделаны следующие допущения. При кластеризации количество серверов виртуализации было принято равным трем. На каждом сервере виртуализации оба сетевых порта объединялись в один общий логически для виртуальных машин с пропускной способностью 2 Гбит/с. Скорость взаимодействия физических серверов при классическом подходе была принята равная 1 Гбит/с. Считалось что все сервера виртуализации или физические сервера подключены к одному коммутатору. Перед запуском модели определялся тип протокола SAN-сети и его скорость. Также определялось количество виртуальных машин или физических серверов. Определялось количество виртуальных машин на одном сервере виртуализации. Определялась необходимая пропускная способность сети для каждой виртуальной машины, но одинаковая для всех виртуальных машин. При моделировании сравнивались два подхода к построению ЦСОД: классический и кластеризация.

Сетевое взаимодействие было представлено как компоненты системы массового обслуживания. В начале, создавалась заявка на ресурсы, т. е. необходимость в новом физическом сервере или виртуальной машине. Данная заявка дублировалась и передавалась на два подхода к построению ЦСОД. Количество конечных заявок было конечно и определялось перед моделированием. В дальнейшем виртуальная машина или физический сервер были представлены как сущность, для обслуживания которой необходимы ресурсы. В качестве ресурсов была представлена пропускная способность ЛВС или SAN-сети. Для данной сущности было выставлено очень большое время обслуживания. Заявки на

создание нового сервера или виртуальной машины появлялись с заданной частотой. Таким образом, моделировалась загруженность ЛВС и SAN-сети. Также в дальнейшем было смоделирована ситуация полной загруженности сети и было выявлено при каком количестве серверов это происходит. На данной модели будет видно, какой подход к построению ЦСОД меньше нагружает ЛВС и как при кластеризации лучше размещать виртуальные машины. Процесс моделирования показан на рисунке 22.

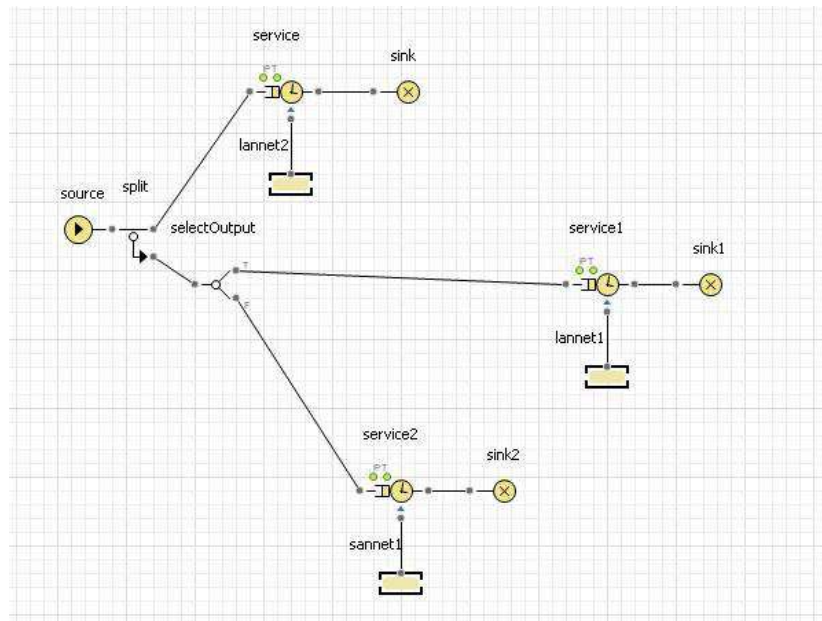


Рисунок 22 – Моделирование ЛВС

Данные моделирования отображены в таблице 9 и таблице 10. Для каждого заданных параметров запуск модели осуществлялся десять раз. В таблице отображено среднее значение для каждой группы из десяти попыток. В таблице 9 отображены результаты моделирования для кластеризации ЦСОД. В таблице 10 результаты моделирования при классическом подходе к построению ЦСОД.

Таблица 9 – Моделирование ЛВС при кластеризации

Кол-во ВМ, шт.	Кол-во ВМ на сервер, шт.	Ресурсоемкость ВМ, Мбит/с.	Загруженность SAN-сети, Мбит/с.	Загруженность ЛВС, Мбит/с.
9	3	5	45	135
9	3	10	90	270
9	3	20	180	540

9	3	30	270	810
15	5	5	150	375
15	5	10	300	750
15	5	20	600	1500
15	5	30	900	2250
21	7	5	315	735
21	7	10	720	1380
24	8	5	420	960
27	9	5	540	1215
30	10	5	675	1500

Таблица 10 – Моделирование ЛВС при классическом подходе

Кол-во ВМ, шт.	Кол-во ВМ на сервер, шт.	Ресурсоем- кость ВМ, Мбит/с.	Загружен- ность ЛВС, Мбит/с.
9	3	5	180
9	3	10	360
9	3	20	720
9	3	30	1080
15	5	5	525
15	5	10	1050
15	5	20	2100
15	5	30	3150
21	7	5	1050
21	7	10	2100
24	8	5	1380
27	9	5	1755
30	10	5	2175

По результатам моделирования можно сделать следующие выводы. При использовании кластеризации снижается загруженности ЛВС. Средняя загруженности ЛВС при кластеризации снижается в среднем на 30%. При кластеризации имеется дополнительная возможность снижения нагрузки на ЛВС путем размещения максимального количества ВМ на одном сервер виртуализации. Количество виртуальных машин, при котором достигается предел пропускной способности сети для классического подхода намного меньше, чем при кластеризации. Скорость копирования данных или файлов между виртуальными ма-

шинами, размещенными на одном хосте, будет в несколько раз выше (в 6-16 раз).

2.4 Выводы и рекомендации по использованию технологий виртуализации ЦСОД в энергетике.

Основываясь на результатах натуральных экспериментов и моделировании можно сделать следующие выводы:

- Применение кластеризации при построении ЦСОД приводит к сокращению времени простоя оборудования до нуля при проведении планового технического обслуживания;
- Применение кластеризации при построении ЦСОД приводит к сокращению времени простоя оборудования до нуля при проведении различных запланированных работ (увеличение ресурсов, добавление устройств и т. п.);
- Применение виртуализации и кластеризации приводит к снижению потребления электрической энергии в ЦСОД в несколько раз;
- Применение виртуализации и кластеризации приводит к снижению выделения тепловой энергии в ЦСОД в несколько раз;
- Применение кластеризации приводит к снижению времени простоя оборудования (системы) на 324,6 секунд при каждой незапланированной перезагрузке;
- Применение кластеризации приводит к снижению необходимого количества сетевых устройств (коммутаторы, маршрутизаторы) и уменьшению количества кабельных линий ЛВС;
- Применение кластеризации приводит к уменьшению парка физического серверного оборудования;
- Уменьшение парка серверного оборудования приводит к снижению общего времени, затраченного на ТО оборудования ЦСОД.

Основываясь на результатах натуральных экспериментов и моделировании, далее будут даны рекомендации при построении ЦСОД с помощью кластеризации в энергетической отрасли.

Рекомендуется выбирать разработчика гипервизора в зависимости от масштаба энергетического холдинга и семейства используемых ОС. Для небольших и средних по размеру энергохолдингов или при большом распространении ОС семейства Windows рекомендуется использовать гипервизор от Microsoft. В случае больших масштабов предприятия или сильного распространения ОС семейства Linux рекомендуется использовать гипервизор VMware. Применение гипервизора Microsoft в среде Windows даст экономию по лицензированию виртуальных машин. Гипервизор Microsoft больше оптимизирован и более эффективен при работе с виртуальными машинами на базе ОС семейства Windows. Гипервизор VMware больше оптимизирован при работе с ОС семейства Linux.

Для обеспечения непрерывной работы виртуализированных программных комплексов в энергетической отрасли рекомендуется создавать ЦСОД минимум уровня III, в исключительных случаях можно строить ЦСОД уровня II. Необходимо резервировать или дублировать компоненты инфраструктуры ЦСОД такие как электропитание, т. е. в серверном шкафу должно быть два источника бесперебойного питания. Данные источники бесперебойного питания должны быть запитаны от двух разных линий. Мощность источников бесперебойного питания должна подбираться с учетом того, чтобы один ИБП мог нести всю нагрузку в серверном шкафу при выходе из строя другого ИБП. ЦСОД должен иметь АВР для серверного оборудования. Необходимо дублировать кондиционеры системы охлаждения. Кондиционеры системы охлаждения должны иметь либо свой АВР, либо должны быть запитаны от различных электрических линий. Оборудование в серверном шкафу должно иметь два блока питания. Каждый блок питания должен подключаться к своему ИБП. Оборудование, имеющее один блок питания, должно подключаться к быстродействующему стоечному АВР. Необходимо приобретать современное серверное оборудо-

дование с дублированными или резервированными компонентами (контроллеры, ОЗУ, диски, боки вентиляторов и т. п.). Серверное оборудование должно иметь возможность «горячей» замены вышедшего из строя компонента, т. е. без отключения оборудования.

При построении виртуальной среды, более перспективным будет использование кластеризации, а не виртуализации. Для построения кластера необходимо выбирать серверное оборудование минимум с гарантией в три года, что гарантирует высокое качество и бесперебойную работу оборудования. У оборудования с большей гарантией чаще всего, больше срок службы. Для построения кластера рекомендуется использовать СХД. Выбор класса СХД осуществляется исходя из бюджета и поставленных задач. При возможности рекомендуется дублировать СХД или сам кластер полностью. При отсутствии такой возможности необходимо предусмотреть различные способы повышения надежности хранимых на СХД данных. Минимальное рекомендуемое количество физических серверов для построения кластер три штуки. Оптимальное количество серверов для кластера выбирается в зависимости от предполагаемой нагрузки на кластер. Рекомендуется выбирать, по возможности, мощные сервера с большим количеством ОЗУ, мощными процессорами, но с возможностью дальнейшего наращивания объемов ОЗУ. Меньшее количество более мощных серверов лучше, чем большее количество менее мощных серверов. Для подключения серверов к СХД необходимо использовать протоколы Fiber Channel или SAS. Протокол Fiber Channel лучше использовать в кластерах, где предполагается создание SAN-сети или значительное увеличение количества хостов. Протокол SAS лучше использовать в небольших кластерах, где не предполагается построение SAN-сетей. Необходимо все сервера кластера размещать в одном помещении и в одном серверном шкафу.

Для обеспечения эффективной работы виртуальных машин в кластере необходимо учитывать следующие рекомендации. VM, между которыми будет осуществляться большой и постоянный обмен данными рекомендуется размещать на одном сервере виртуализации для уменьшения нагрузки на ЛВС. Для

увеличения пропускной способности серверов виртуализации, необходимо использовать технологии объединения физических сетевых портов в несколько логических. Рекомендуется разделять сетевые порты сервера виртуализации на порты для обмена данными ВМ и на порты для обмена данными между серверами виртуализации в кластере. Виртуальные машины, резервирующие друг друга, необходимо размещать на разных серверах виртуализации в рамках одного кластера. Для обеспечения максимально эффективной работы виртуальных машин рекомендуется как на сервера виртуализации, так и на сами ВМ ставить новейшие версии ОС.

Необходимо резервировать критически важные ВМ. Резервирование выполняется на уровне прикладного ПО, если такое было предусмотрено разработчиком ПО. Необходимо резервировать важные БД на уровне СУБД.

Для обеспечения надежности работы ВМ и архивного хранения данных, необходимо предусматривать при построении ЦСОД наличие системы резервного копирования. Система резервного копирования не должна находиться в одном помещении с серверами кластера.

Для обеспечения бесперебойной передачи данных по ЛВС необходимо предусматривать как резервирование узлов сети (коммутаторов), так и линий связи (проводов). Все ведущие производители сетевого оборудования предлагают свои технологии обеспечения резервирования коммутаторов. Также ведущие производители предлагают свои протоколы резервирования и объединения сетевых портов. Необходимо учитывать, что гипервизор от Microsoft в области резервирования портов и линий связи больше ориентирован на поддержку сетевого оборудования Cisco. Для повышения скорости обмена данными между серверами виртуализации в кластере, рекомендуется эти сервера подключать к одному коммутатору или к дублирующим коммутаторам. Коммутаторы и сервера виртуализации рекомендуется размещать в одном серверном шкафу.

Для предотвращения аварийных ситуации и их предупреждения необходимо предусматривать в ЦСОД систему мониторинга. Минимально для мониторинга необходимо использовать протокол SNMP. Работу по этому протоколу

должно поддерживать все оборудование: серверное, сетевое, электрическое и прочее. Рекомендуется устанавливать дополнительный мониторинг параметров электросети на вводах в ЦСОД.

3 Апробация результатов

3.1 Описание текущей ситуации и структуры ЦСОД СГК

В настоящее время структура ЦСОД ООО «Сибирская генерирующая компания» разрознена и не унифицирована между различными станциями. Сервера и прочее оборудование рассредоточено по территории станции. Технологии виртуализации и кластеризации практически не применяются. Состав, структура ЦСОД и их инженерных систем различен между станциями. Единых требований внутри компании к оснащению и построению ЦСОД нет. Площадкой с самой развитой ИТ-инфраструктурой является исполнительный аппарат СГК.

Разнородность аппаратных средств и уровня развития ИТ-инфраструктуры станций связаны с независимым развитием каждой станции. До реформы энергетической отрасли каждая станция была независима. Вложения в информационные технологии и их развитие были минимальны. После консолидации станций в одной компании развитие ИТ-систем также продолжалось независимо, т. к. ИТ-персонал станций не был объединен между собой. Из-за отсутствия консолидации ИТ-персонала не были разработаны единые требования к структуре и оснащению ЦСОД, принципы развития ИТ-инфраструктуры. Уровень ИТ-персонала станции сильно отличается из-за независимого развития станций. Уровень развития ИТ-систем зависел от уровня ИТ-персонала станций и направленности директора станции на развитие ИТ-систем. Основные вложения в ИТ-инфраструктуру были осуществлены после реформирования энергетической отрасли страны (2007-2008 гг.). После проведения реформы все станции должны были оснащаться такими программными комплексами как АИИСКУЭ, СОТИАССО, АСКУТЭ. Данные комплексы мас-

сово внедрялись на станциях. На момент их внедрения технологии виртуализации были развиты слабо, поэтому при построении данных систем был использован классический подход. После внедрения данных комплексов вложения в информационные технологии были минимальны и были связаны либо с внедрением новых программных комплексов и систем, либо с поддержанием в работоспособном состоянии текущих систем.

Консолидация ИТ-персонала была проведена в 2014 году. Следующим шагом стала разработка единой ИТ-стратегии, в рамках которой определили пути развития информационных технологий. После утверждения ИТ-стратегии были частично унифицированы зоны ответственности персонала. Разработаны единые требования и обязанности персонала. Разработаны единые требования к оснащению ЦСОД инженерными и прочими системами. Разработана единая политика по унификации оборудования.

3.2 Результаты внедрения предложенного типового решения для ЦСОД на основе технологий виртуализации

В качестве экспериментальной площадки для внедрения кластеризации ЦСОД была выбрана Красноярская ТЭЦ-1. Состояние ИТ-инфраструктуры до внедрения кластеризации показано в приложении А.

Из схемы в приложении А видно, что до внедрения использовался классический подход к построению ЦСОД. Основное серверное и сетевое оборудование было размещено в двух серверных помещениях (Пристройка №1 и Серверная №1). Оба серверных помещения были в разной степени оснащены инженерными системами. Электропитание серверных помещений было организовано через АВР. Критически важное оборудование дополнительно было запитано от источников бесперебойного питания. Система мониторинга имела не на всем оборудовании и не была централизована. Остальное серверное оборудование было размещено по всей территории станции. Чаще всего новые системы и серверное оборудование максимально близко располагалось к пользова-

телям или к устройствам нижнего уровня (датчики, контроллеры). Персонал не стремился размещать оборудование в серверных помещениях. Серверное оборудование, размещенное вне серверных помещений, не всегда обеспечивалось оптимальными температурными условиями. Часть оборудования размещалась на ГЩУ, что осложняло доступ персоналу. На ГЩУ не обеспечивались оптимальные климатические условия. Территориальная разрозненность серверного оборудования по территории станции увеличивало время реакции персонала на аварийные ситуации и скорость выполнения ТО.

В рамках инвестиционной программы ООО «Сибирская генерирующая компания» была проведена модернизация серверных помещений и серверного оборудования.

На первом этапе была проведена модернизация существующего серверного помещения. Помещение было приведено в соответствие требованиям Инструкции компании по оснащению серверных помещений. В рамках данного проекта был заменен АВР для серверного помещения на более мощный. Была заменена система охлаждения на более производительную. После модернизации система охлаждения позволяет охлаждать помещение даже при выходе из строя одного из двух кондиционеров. Был проведен косметический ремонт с заменой окон, демонтаж старых кабельных лотков и прочего оборудования. Было заменено электросетевое хозяйство – кабельные линии, провода, автоматические выключатели. Серверное помещение оснастили электронной системой контроля и управления доступом. После модернизации каждый серверный шкаф имеет два отдельных ввода от разных фаз с различными автоматическими выключателями. В рамках модернизации ЛВС были зарезервированы все каналы связи, выходящие из серверного помещения. Всё оборудование было оснащено системами мониторинга по ЛВС.

На втором этапе была проведена модернизация серверного оборудования. Модернизации оборудования предшествовал выбор способов модернизации оборудования. В течение нескольких месяцев сотрудники ООО «Сибирская генерирующая компания» анализировали пути модернизации серверной инфра-

структуры. На основании современных тенденций развития ИТ и на основании опыта использования кластеризации в Исполнительном аппарате ООО «Сибирской генерирующей компании» сразу была выбрана кластеризация ЦСОД. В дальнейшем встал выбор аппаратной платформы для кластеризации. Рассматривались различные варианты: классические отдельные сервера и СХД, блейд-корзина с серверами-лезвиями и с СХД, гибридная система. Проанализировав преимущества и недостатки каждой платформы и цены на сервера, был сделан выбор в пользу stand-alone серверов. Такой выбор обусловлен большим положительным опытом эксплуатации подобных платформ, несмотря на меньшую компактность данного решения. После выбора типа серверной платформы, был осуществлен отбор ведущих производителей, выпускающих сервера, соответствующие техническому заданию. Для построения кластера были выбраны модели СХД начального уровня, т. к. текущая и перспективная нагрузка на кластер должна была быть невысокой. СХД планировалось подключать к серверам напрямую (вырожденная SAN-сеть). Для бесперебойной работы кластера виртуализации было подобрано вспомогательное оборудование. В первую очередь была выбрана модель серверного шкафа увеличенных размеров и стандартной высоты для облегчения проведения работ и монтажа дополнительного оборудования. Для бесперебойного питания всего оборудования были выбраны модели источников бесперебойного питания. Для выполнения рекомендаций указанных выше приобретались два ИБП. Каждый источник бесперебойного питания подключался к своему автоматическому выключателю. Оборудование в серверном шкафу, имеющее два блока питания подключалось к разным ИБП. Мощность и время автономной работы выбиралось с учетом требований к информационным системам электроэнергетики. Также модель источников бесперебойного питания выбиралась исходя из того, чтобы один источник бесперебойного питания мог нести всю нагрузку в серверном шкафу. Для обеспечения бесперебойного питания оборудования с одним блоком питания был приобретен быстродействующий АВР стоечного исполнения. АВР подключался к двум источникам бесперебойного питания. Выбор в пользу стоечного АВР был сде-

лан из-за разницы в цене между такой моделью и общим быстродействующим АВР для всего ЦСОД. Для распределения питания в серверном шкафу были выбраны модули распределения питания с мониторингом общей нагрузки и возможностью удаленного управления отдельными розетками. Для обеспечения дублированного подключения серверов к коммутаторам и для внешних подключений ЛВС было выбрано оборудование Cisco. Данный производитель был выбран из-за широкого распространения оборудования в компании и из-за большого количества специалистов по данному оборудованию. Также для обеспечения отказоустойчивости коммутаторов компания Cisco предоставляет технологию стекирования коммутаторов [22]. Стекирование коммутаторов это технология, при которой несколько коммутаторов объединяются в один логический коммутатор с помощью выделенной шины для стекирования. Стекирование обеспечивает отказоустойчивое соединение между всеми коммутаторами на высокой скорости (от 20 Гбит/с). За счет данной технологии и при правильном распределении портов между оборудованием в стойке все сетевые подключения будут работоспособны при выходе из строя коммутатора. В данном случае было принято решение стекировать два коммутатора. Для надежного подключения серверов к коммутатору была использована еще одна технология Cisco – LACP. LACP – протокол Cisco, позволяющий объединить несколько физических портов в один логический. Пропускная способность логического порта равна сумме пропускных способностей всех портов. Также данный протокол поддерживает операционной системой Microsoft Windows Server 2012 и выше. В серверах для надежности одна пара физических портов объединялась в один логический для организации сети виртуальных машин. Вторая пара физических портов объединялась в один логически для организации сетевого обмена между серверами виртуализации. В каждой паре порты подключались к разным коммутаторам стека. Для организации подключения USB-ключей к виртуальным машинам был приобретен преобразователь позволяющий «пробрасывать» USB-ключи используя ЛВС. В качестве гипервизора был выбран гипервизор Microsoft из-за большей распространенности в компании ОС семейства Windows и

наличия компетенции у сотрудников по данному гипервизору. В приложении В показана логическая схема электрических подключений в серверном шкафу. В приложении Г показана логическая схема размещения оборудования в серверном шкафу.

Проанализировав текущий состав серверов, запланированный рост нагрузки, было принято решение приобрести более мощные серверы, но в меньшем количестве. На основании имеющегося бюджета и расчетов нагрузки было определено, что наиболее оптимальным будет приобретение трех серверов для кластеризации. Как видно из схем после модернизации планировалось организовать ЦСОД третьего уровня, а по некоторым пунктам второго. Монтаж и пуско-наладка оборудования осуществлялась силами персонала ООО «Сибирская генерирующая компания». Схема Красноярской ТЭЦ-1 после модернизации показана в приложении Б. После успешного проведения испытаний кластер был принят в опытную эксплуатацию. Акт ввода в опытную эксплуатацию представлен в приложении Д. После введения кластера в опытную эксплуатацию начался процесс постепенной виртуализации физических серверов. На данный момент виртуализация ресурсов зарекомендовала себя с положительной стороны. За счет виртуализации повысилась надежность работы программных комплексов. Упростилось увеличение ресурсов (ОЗУ, дисковое пространство) для виртуальных серверов. На новых версиях ОС увеличение ресурсов производится без выключения виртуальной машины. Виртуализация серверов решила проблему с недостаточностью ресурсов для части серверов. За счет виртуализации уменьшился необходимый запас запчастей для серверов. Благодаря системе мониторинга появилась возможность следить за потреблением ресурсов виртуальных машин. Благодаря гипервизору можно в одной консоли быстро оценить потребление ресурсов виртуальными машинами. Увеличилась скорость передачи данных по сети, т. к. до модернизации часть серверов была подключена по каналам с пропускной способностью 100 Мбит/с. Снизилось количество кабельных линий LAN-сети. Кластер позволил разместить новые

программные комплексы. В дальнейшем планируется увеличивать количество виртуализированных ресурсов.

ЗАКЛЮЧЕНИЕ

В рамках данной работы было подтверждено предположение, что технологии виртуализации и кластеризации являются более надежными. По результатам проведенного моделирования можно сделать вывод, что при использовании кластеризации снижается нагрузка на инженерные системы ЦСОД. Кластеризация снижает нагрузку на локальную систему предприятия, облегчает проведения технического обслуживания и прочих работ с оборудования. Несмотря на преимущества, кластеризация требует дополнительного вспомогательного оборудования, производительных серверов и резервирования оборудования. Кластеризация является перспективной технологией. Рекомендуется внедрять кластеризацию на всех промышленных предприятиях, в энергетике особенно из-за повышенных требований к надежности.

Основываясь на успешно опыте внедрения кластеризации на Красноярской ТЭЦ-1, будет осуществлено дальнейшее распространение данной технологии на все станции. В перспективе в виртуальную среду будут перенесены все физические серверы. Как дальнейшее развитие данной технологии виртуализации подвергнуться все специализированные автоматизированные места работников (далее – АРМ). В данный момент АРМ представляют собой персональные компьютеры. Планируется заменить их виртуальными АРМ или виртуальным сервером терминалов, который предоставляет доступ к определенному ПО множеству пользователей.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Актуальные вопросы современной науки : сборник научных трудов. Выпуск 52 / Под общ. ред. С. С. Чернова. – Новосибирск : Издательство ЦРНС, 2017. – 258с.
- 2 Гвоздева, В.А. Информатика, автоматизированные информационные технологии и системы [Текст] : учебник / В. А. Гвоздева. - Москва : ИД Форум : НИЦ ИНФРА-М, 2015. - 544 с.
- 3 Дисковые массивы Dell EMC корпоративного класса для хранения данных [Сайт] – Режим доступа: <http://www.dell.com/ru/business/p/disk-arrays>
- 4 Интеллектуальный кластер Intelligent Cluster [сайт]. – Режим доступа: <http://www3.lenovo.com/ru/ru/data-center/servers/high-density/HD-Intelligent-Cluster/p/77XDDVLDV01>
- 5 Информационные технологии [Текст] : учебное пособие / Л. Г. Гагарина [и др.] ; под ред. Л. Г. Гагарина. - Москва : ИД Форум : НИЦ ИНФРА-М, 2015. - 320 с.
- 6 Коммутаторы Cisco [сайт]. – Режим доступа: http://www.cisco.com/c/ru_ru/products/switches/index.html
- 7 Конвергентные системы [сайт]. – Режим доступа: <https://www.hpe.com/ru/ru/integrated-systems/converged.html#portfolio>
- 8 Корпоративные информационные системы управления [Текст] : учебник / под науч. ред.: Н. М. Абдикеев, О. В. Китова. - Москва : НИЦ ИНФРА-М, 2014. - 464 с.
- 9 Мартемьянов, Ю. Ф. Операционные системы. Концепции построения и обеспечения безопасности [Электронный ресурс] : учебное пособие / Ю. Ф. Мартемьянов, Ал. В. Яковлев, Ан. В. Яковлев. - Москва : Горячая линия-Телеком, 2011. - 332 с.
- 10 Моисеева, Н. К. Управление операционной средой организации [Текст] : учебник / Н. К. Моисеева, А. Н. Стерлигова ; Нац. исслед. ун-т "Высш. шк. экономики". - Москва : НИЦ ИНФРА-М, 2014. - 336 с.

- 11 Монтируемые в стойку серверы [сайт]. – Режим доступа: <http://www3.lenovo.com/ru/ru/data-center/servers/racks/c/racks>
- 12 Новожилов, О. П. Архитектура ЭВМ и систем [Текст] : учеб. пособие для вузов / О. П. Новожилов. - Москва : Юрайт, 2012. - 527 с.
- 13 Новые возможности AnyLogic [сайт]. – Режим доступа: <https://www.anylogic.ru/new-features>
- 14 Об AnyLogic [сайт]. – Режим доступа: <https://www.anylogic.ru/overview>
- 15 Операционные системы. Основы UNIX [Текст] : учебное пособие / А. Б. Вавренюк [и др.]. - Москва : ИНФРА-М, 2015. - 184 с.
- 16 Платформа Dell PowerEdge VRTX для модульной инфраструктуры [сайт]. – Режим доступа: http://www.dell.com/ru/business/p/poweredge-vrtx/pd?refid=poweredgevrtx&baynote_bnrack=0&baynote_irrack=1&~ck=dellSearch&isredirect=true
- 17 Правила эксплуатации электроустановок, 7-е издание [Электронный ресурс]. – Режим доступа: <http://pue7.ru/pue7/sod.php>
- 18 Сервер для установки в стойку Dell PowerEdge [сайт]. – Режим доступа: <http://www.dell.com/ru/business/p/poweredge-rack-servers>
- 19 Сеть хранения данных [сайт]. – Режим доступа: <http://www3.lenovo.com/ru/ru/data-center/storage/storage-area-network/c/storage-area-network>
- 20 Система VxRack с FLEX [сайт]. – Режим доступа: <http://www.dell.com/ru/business/p/vmware-vxrack/pd>
- 21 Система классификации Tier [сайт]. – Режим доступа: <https://ru.uptimeinstitute.com/tiers>
- 22 Создание и управление стеком Cisco 3750 [сайт]. – Режим доступа: http://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/71925-cat3750-create-switch-stks.html?referring_site=RE&pos=1&page=http://www.cisco.com/c/ru_ru/support/docs/switches/catalyst-3750-series-switches/71925-cat3750-create-switch-stks.html

- 23 Справка AnyLogic [сайт]. – Режим доступа: <http://help.anylogic.ru/index.jsp>
- 24 Сравнение функций в версиях Windows Server [сайт]. – Режим доступа: <https://www.microsoft.com/ru-ru/cloud-platform/windows-server-comparison>
- 25 СТО 4.2–07–2014 Система менеджмента качества. Общие требования к построению, изложению и оформлению документов учебной деятельности. – Введ. 30.12.2013. – Красноярск : СФУ, 2014. 60 с.
- 26 Стоечные переключатели нагрузки [сайт]. – Режим доступа: http://www.apc.com/shop/ru/ru/categories/power-distribution/transfer-switches/rack-mount-transfer-switches/_/N-1eg32mv
- 27 Таненбаум, Э. Современные операционные системы / Э. Таненбаум. – Санкт-Петербург : Питер, 2013. - 1120 с.
- 28 AnyLogic [сайт]. – Режим доступа: <https://ru.wikipedia.org/wiki/AnyLogic>
- 29 Explaining the Uptime Institute’s Tier Classification System [сайт]. – Режим доступа: <https://journal.uptimeinstitute.com/explaining-uptime-institutes-tier-classification-system/>
- 30 Flex System [сайт]. – Режим доступа: <http://www3.lenovo.com/ru/ru/data-center/servers/blades-flex-servers/c/blades-flex>
- 31 HPE Blade System [сайт]. – Режим доступа: <https://www.hpe.com/ru/ru/integrated-systems/bladesystem.html#portfolio>
- 32 Hyper-V [сайт]. – Режим доступа: <https://ru.wikipedia.org/wiki/Hyper-V>
- 33 Hyper-V Technology Overview [сайт]. – Режим доступа: <https://docs.microsoft.com/ru-ru/windows-server/virtualization/hyper-v/Hyper-V-Technology-Overview>
- 34 Lenovo Converged HX Series [сайт]. – Режим доступа: <http://www3.lenovo.com/ru/ru/data-center/converged-systems/Lenovo-Converged-HX-Series/p/WMD00000036#galleryPhoto>

- 35 Microsoft Hyper-V Server 2012 [сайт]. – Режим доступа:
<https://technet.microsoft.com/en-us/hyper-v-server-docs/hyper-v-server-2012>
- 36 SNMP [сайт]. – Режим доступа: <https://ru.wikipedia.org/wiki/SNMP>
- 37 SNMP RFC1157 [Электронный ресурс] – Режим доступа:
<https://tools.ietf.org/html/rfc1157>
- 38 System x GPFS Storage Server [сайт]. – Режим доступа:
<http://www3.lenovo.com/ru/ru/data-center/servers/high-density/System-x-GPFS-Storage-Server/p/77XDDOTDO01>
- 39 T10 Technical Committee [Электронный ресурс] – Режим доступа:
<http://www.t10.org/>
- 40 T11 Fiber Channel Interface [Электронный ресурс] – Режим доступа:
https://standards.incits.org/apps/group_public/workgroup.php?wg_abbrev=t11
- 41 VMware [сайт]. – Режим доступа:
<https://ru.wikipedia.org/wiki/VMware>
- 42 VSphere [сайт]. – Режим доступа:
<http://www.vmware.com/ru/products/vsphere.html>
- 43 Xen [сайт]. – Режим доступа: <https://ru.wikipedia.org/wiki/Xen>
- 44 Xen Server [сайт]. – Режим доступа:
<https://www.citrix.ru/products/xenserver/>

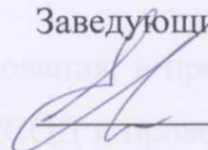
Федеральное государственное автономное
образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт космических и информационных технологий

Системы автоматизации, автоматизированного управления и проектирования

УТВЕРЖДАЮ

Заведующий кафедрой

 С. В. Ченцов





« 22 » июня 2017 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

ПРОЕКТИРОВАНИЕ ЦЕНТРОВ СБОРА И ОБРАБОТКИ ДАННЫХ ДЛЯ
ПРЕДПРИЯТИЙ ЭЛЕКТРОЭНЕРГЕТИКИ НА ОСНОВЕ ТЕХНОЛОГИИ
ВИРТУАЛИЗАЦИИ

27.04.04 Управление в технических системах

27.04.04.03 Автоматизация управления технологическими процессами в энергетике

Научный руководитель		<u>22</u> .06.2017	доцент, канд. техн. наук С. А. Темербаев
Выпускник		<u>22</u> .06.2017	А. А. Потерайло
Рецензент		<u>22</u> .06.2017	доцент, канд. пед. наук С. А. Виденин
Нормоконтролер		<u>22</u> .06.2017	Т. А. Грудинова

Красноярск 2017