

УДК 004.052

ОБ ОДНОМ ПОДХОДЕ К ОЦЕНКЕ НАДЕЖНОСТИ ОБОРУДОВАНИЯ ЦЕНТРА ОБРАБОТКИ ДАННЫХ

И. Д. Гуз

*Сургутский государственный университет,
idguzzz@gmail.com*

В статье даны определения центра обработки данных, отказоустойчивости, доступности информации; описаны способы оценки стоимости вынужденного простоя для компании; выполнен расчет показателей доступности информации и показателей надежности. Целью работы является анализ надежности элементов инфраструктуры центра обработки данных на основе эксплуатационных данных. Основным свойством, которым должен обладать центр обработки данных высокого уровня надежности, является отказоустойчивость, которая оценивается при помощи показателей доступности информации. При анализе доступности информации оценивались частота отказов компонентов и среднее время ремонта, определяемые в понятиях среднего времени безотказной работы и среднего времени восстановления. После обработки входных данных были рассчитаны средний период доступности информации и средний период простоя в год.

Ключевые слова: центр обработки данных, отказоустойчивость, доступность, сбой, простой, среднее время безотказной работы, среднее время восстановления, период доступности информации.

ON CERTAIN APPROACH TO ASSESSMENT OF RELIABILITY FOR DATA CENTER EQUIPMENT

I. D. Guz

*Surgut State University,
idguzzz@gmail.com*

The article gives definitions to the data center, fault tolerance, information availability, and describes methods for estimating the cost of forced downtime for a company. The calculations for the indicators of information availability and reliability indicators are made. The aim of the study is to analyze the reliability of the data center infrastructure elements based on operation data. The main property that a data center of a high level of reliability must have is the fault tolerance. Fault tolerance of data center is assessed using information accessibility indicators. The component of the failure rate (meant time to failure) and the average repair time (mean time to recovery) are assessed during the analysis of the information availability. After processing the input data, the average information availability period and the average downtime per year are calculated.

Keywords: data center, fault tolerance, availability, failure, downtime, meant time to failure, mean time to recovery, information availability period.

Введение. В наши дни без непрерывного доступа к информации невозможно обеспечить должное проведение бизнес-операций. Очень велика цена недоступности информации, так как даже час простоя в ключевых отраслях промышленности грозит миллионными убытками.

В современных условиях наличие развитой и гибкой в управлении ИТ-инфраструктуры является залогом успешной деятельности в любой сфере, так как информационные инфраструктуры позволяют решать как текущие, так и глобальные бизнес-задачи. Разветвленная структура ИТ-систем и необходимость в автоматизации бизнес-процессов требуют создания

дата-центров для обработки и хранения информации, которые дают возможность эффективно управлять всеми ресурсами компании, грамотно их распределять и принимать своевременные решения. К системам хранения и обработки данных сегодня предъявляются особые требования, основными из которых являются адаптация под меняющиеся условия бизнеса, повышение надежности хранения информации, способность работать с большими объемами информационных ресурсов и сокращение затрат на обслуживание дата-центров [1].

Целью работы является анализ надежности элементов инфраструктуры центра обработки данных (далее – ЦОД) на основе эксплуатационных данных.

Характеристики отказоустойчивости ЦОД. Центр обработки данных (или дата-центр) – это комплекс взаимосвязанных элементов, включающий в себя вычислительные компоненты, элементы IT-инфраструктуры, строительных и инженерных систем. Его основными задачами являются хранение, обработка и передача информации. В дата-центре на небольшой площади сосредоточены мощные вычислительные ресурсы: серверы и системы хранения данных (далее – СХД), обеспечивающие хранение и обработку информации; сетевое оборудование, поддерживающее непрерывный обмен данными внутри ЦОД, а также связь с внешними потребителями; инженерные системы, системы безопасности, системы мониторинга и диспетчеризации, гарантирующие эффективную работу и защиту вычислительного центра [2].

Основным свойством, которым должен обладать ЦОД высокого уровня надежности, является отказоустойчивость. Отказоустойчивость – свойство технической системы сохранять свою работоспособность после отказа одного или нескольких составных компонентов. Высокий уровень отказоустойчивости достигается уменьшением количества «узких мест» в инфраструктуре ЦОД с помощью:

- резервирования физических и виртуальных компонентов ЦОД;
- применения специализированного программного обеспечения, позволяющего избежать или минимизировать простои систем;
- создания резервных копий баз данных и операционных систем.

Отказоустойчивость ЦОД оценивается при помощи показателей доступности информации. Под доступностью информации понимается возможность инфраструктуры, занимающейся ее обработкой, функционировать в течение временного периода, требуемого для выполнения определенной операции. Доступность информации обеспечивает пользователям беспрепятственный доступ к информации в любой необходимый момент времени [3].

Для обеспечения надежности основные системы ЦОД обычно резервируются, т. е. не устанавливаются в единственном экземпляре. Например, система электропитания ЦОД должна иметь вводы от двух подстанций системы электроснабжения, а для большей надежности устанавливаются дизель-генераторы и батареи на случай полного отключения электропитания в районе расположения ЦОД. Следует заметить, что аналогичным образом резервируются также и элементы сетей связи телекоммуникационных операторов.

Виртуальная инфраструктура предназначена для распределения и диспетчеризации физических вычислительных ресурсов между виртуальными машинами, используемыми для доступа к терминальным приложениям.

Виртуальная инфраструктура позволяет решить следующие задачи:

- обеспечение высокой доступности серверов и приложений;
- уменьшение количества серверного оборудования за счет увеличения коэффициента использования серверных ресурсов;
- уменьшение затрат на энергопотребление оборудования и уменьшение затрат на охлаждение оборудования ввиду консолидации различных физических серверов на меньшем количестве серверов виртуализации;
- быстрое восстановление серверов и приложений после системных ошибок.

Архитектура гипервизора обеспечивает:

- оптимизацию производительности виртуальной среды;
- быстрое развертывание, запуск и перезагрузку виртуальных машин.

Подключение серверного оборудования по принципу plug-and-play обеспечивает мгновенное наращивание ресурсов для предоставления мощностей по требованию.

Для подключения виртуальных машин к локальной сети на серверах виртуализации эмулируются сетевые коммутаторы. Для виртуального коммутатора доступно создание трех типов сетей:

- внешняя сеть – позволяет виртуальным машинам взаимодействовать с внешними сетями и хостом. При создании внешней сети гипервизор создает виртуальный коммутатор, к которому могут подключаться как виртуальные машины, так и хост посредством виртуальных сетевых адаптеров. Физический адаптер при этом отключается от хоста и становится портом виртуального коммутатора, через который происходит подключение к внешней сети;

- внутренняя сеть – предназначена для взаимодействия хоста и виртуальных машин без доступа к внешним сетям. При создании внутренней сети гипервизор создает виртуальный коммутатор, к которому подключаются хост и виртуальные машины посредством виртуальных сетевых адаптеров. Адаптеры должны быть настроены в соответствии с настройками виртуальной сети [4];

- частная сеть – предназначена для создания изолированных участков сети. При создании частной сети гипервизор создает виртуальный коммутатор, к которому могут подключаться только виртуальные машины. От хоста виртуальный коммутатор изолирован. В этом случае связь между внешней и частной сетью будет осуществляться через выделенную виртуальную машину, которая должна быть подключена к обеим сетям.

Причинами недоступности информации, как правило, являются различные запланированные и незапланированные события. К запланированным простоям относятся установка, сервисное обслуживание оборудования, профилактические работы, обновление операционных систем и программ, резервное копирование, восстановление данных, перенос программ из среды тестирования в среду продуктивную и т. д. Незапланированными простоями являются сбои, произошедшие по вине персонала, потеря данных, выход из строя физических и виртуальных составляющих. Кроме того, природные или техногенные катастрофы, такие как наводнения, пожары, землетрясения, также нередко становятся причинами незапланированных сбоев [5].

Возможные аварийные ситуации вычислительного кластера. Режим работы с недоступностью части функционала системы характеризуется отказом на уровне одной из функциональных подсистем:

- отказ подсистемы вычислений;
- отказ подсистемы визуализации;
- отказ подсистемы резервного копирования;
- отказ подсистемы мониторинга;
- отказ подсистемы управления аппаратным обеспечением.

Причиной неработоспособности на уровне функциональной подсистемы может быть как отказ компонентов подсистемы, так и отказ одной из технических подсистем комплекса, а именно:

- отказ сети передачи данных будет иметь последствия в виде неработоспособности подсистемы вычислений;
- отказ сети управления будет иметь последствия в виде неработоспособности подсистемы управления аппаратным обеспечением.

Также возможны ситуации с ограничением функциональности в границах отдельных подсистем, например:

- отказ сети управления будет иметь последствия в виде ограничений в функциональности подсистемы вычислений и подсистемы мониторинга;

- сбой в работе одного из модулей пакета программного обеспечения подсистемы.

Режим полной неработоспособности системы характеризуется недоступностью функционала двух ключевых функциональных подсистем одновременно – вычислительного кластера и подсистемы визуализации. Такая ситуация возможна по следующим причинам:

- отказ системы хранения данных (недоступность данных для проведения расчетов и результатов уже выполненных расчетов приводит к невозможности выполнения кластером и подсистемой визуализации своих функций);

- отказ продуктивной сети в целом (приводит к невозможности осуществления продуктивного информационного взаимодействия между всеми техническими компонентами системы).

Вычислительная система переводится в режим проведения регламентного технического обслуживания с целью выполнения мероприятий, направленных:

- на снижение вероятности возникновения сбоев и отказов;

- устранение обнаруженных уязвимостей программного обеспечения путем установки обновлений операционной системы (далее – ОС) и программного обеспечения, установленного в ОС;

- устранение обнаруженных уязвимостей аппаратного обеспечения путем установки обновлений микрокода оборудования (BIOS, микрокода плат ввода\вывода);

- изменение функциональности комплекса;

- повышение эффективности работы комплекса.

Переход в режим регламентных работ осуществляется в плановом порядке. В данном режиме допускается полная или частичная потеря производительности, функциональности и доступности комплекса в зависимости от характера производимых изменений.

В системе хранения данных возможны различные аварийные ситуации, например выход из строя отдельных накопителей. В этом случае СХД автоматически инициирует подмену вышедшего из строя накопителя на аналогичный из назначенного конкретной RAID-группе SparePool. Далее запустится процесс восстановления информации на новом накопителе. После исключения системой неисправного накопителя из RAID-группы от администратора требуется заменить вышедший из строя накопитель на исправный.

Статистические данные сбоев и отказов ЦОД. На рис. 1 представлена статистика потерь данных и их причины по данным Ассоциации защиты информации (далее – АЗИ) Российской Федерации.

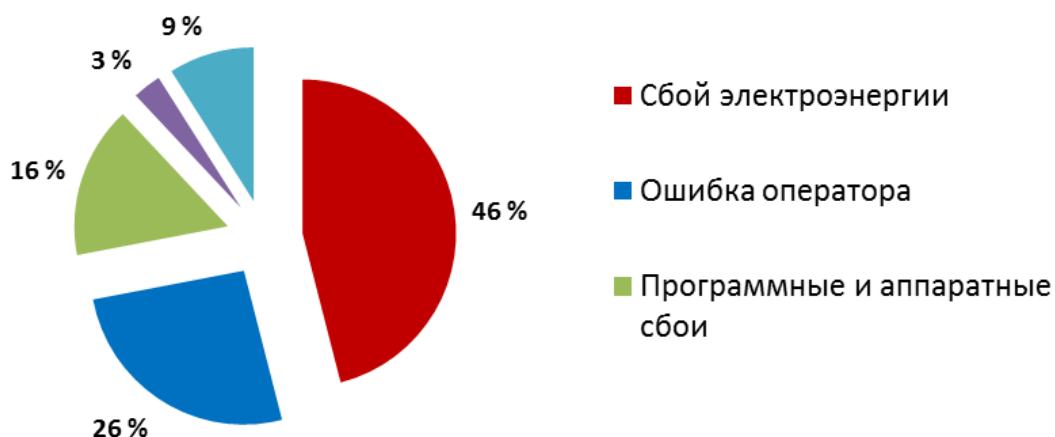


Рис. 1. Статистика потерь данных и их причины

По данным аналитического агентства «ИКС-Консалтинг» [6] была собрана статистика отказов ЦОД компании «РТК-ЦОД», расположенного в г. Екатеринбурге, за 2015–2018 гг. Данные статистики отказов представлены в табл. 1–3, а также на диаграмме (рис. 2).

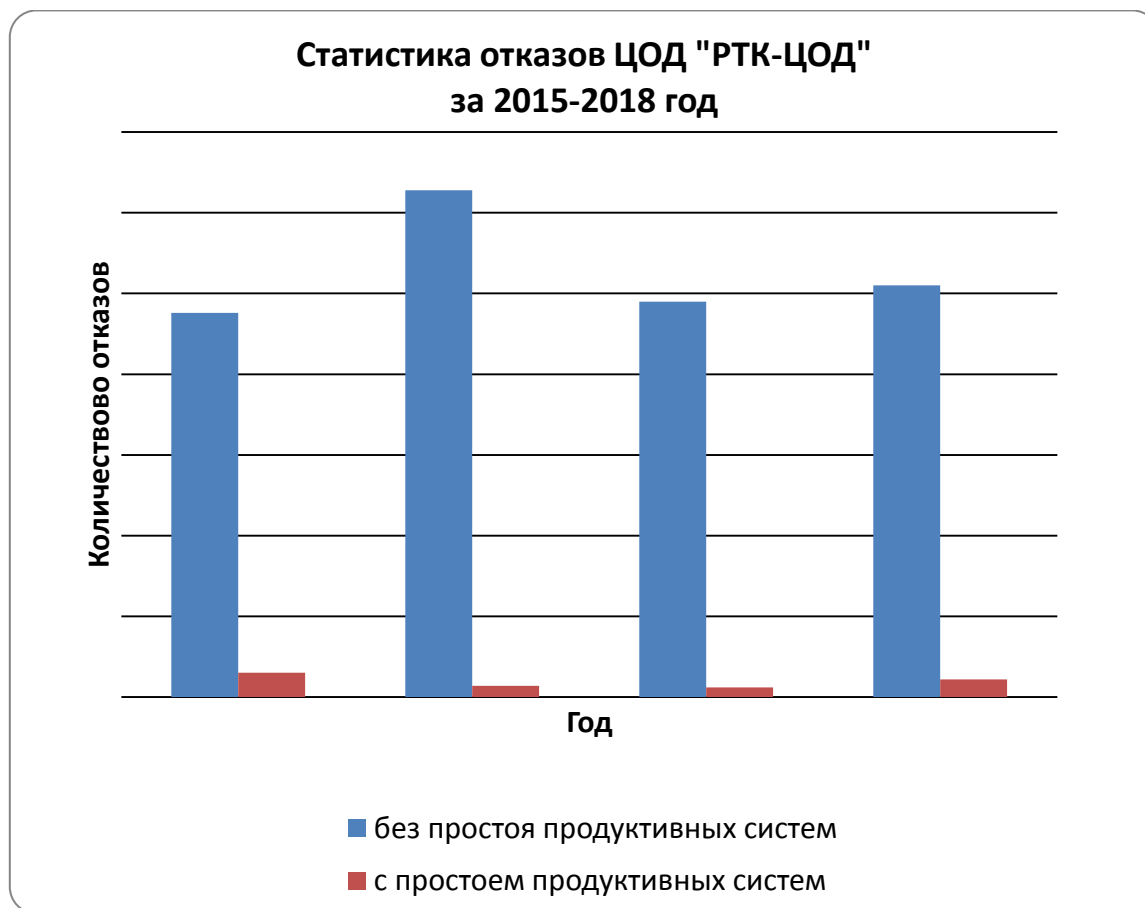


Рис. 2. Диаграмма статистики отказов ЦОД компании «РТК-ЦОД» за 2015–2018 гг.

Таблица 1

Статистика отказов продуктивных систем

Отказы	2015	2016	2017	2018
Без простоя продуктивных систем	238	314	245	255
С простоем продуктивных систем	15	7	6	11
Всего	253	321	251	266

Таблица 2

Статистика сбоев физических компонентов

Тип ситуации	Без простоя	С простоем	Всего
Выход из строя жесткого диска	471	0	471
Неисправность ленточной библиотеки	61	0	61
Выход из строя модуля (платы, процессора, контроллера)	74	7	81
Неисправность блока питания, батареи, вентиляторов	88	0	88
Неисправность коммутатора	29	2	31
Сбой кондиционера	60	1	61
Ошибки программного обеспечения (микрокода, операционной системы, приложения)	92	22	114
Сбой источника бесперебойного питания, бросок питания	143	1	144
Повышение температуры в помещении	5	1	6
Пропадание питания на удаленных площадках	29	5	34

Таблица 3

**Данные по единицам оборудования, периодам работы
и простоям ЦОД компании «РТК-ЦОД»**

Показатели	Количественные данные
Всего единиц оборудования	463
Отказы с простоем	39
Период работы 2015–2018 гг., час	35040
Период простоя 2015–2018 гг., час	49,98

Методика расчета стоимости вынужденного простоя. Вынужденные простои приводят к потерям дохода предприятия, а также наносят огромный урон репутации компании. Потери доходов влекут за собой компенсационные выплаты, оплату счетов клиентов за понесенные убытки, потерю инвестиций. Кроме того, простои отрицательно сказываются на репутации компании, что влечет за собой потерю доверия со стороны клиентов и партнеров по бизнесу.

Влияние простоя на доходы предприятия оценивается такими показателями, как средняя стоимость простоя в час (далее – C_{np}), средняя потеря продуктивности в час (далее – P_{nom}), средняя потеря дохода в час (далее – D_{nom}), которые вычисляются по формулам [7]:

$$C_{np} = P_{nom} + D_{nom}, \quad (1)$$

$$P_{nom} = \frac{C_{зн}}{T_{раб}}, \quad (2)$$

где $C_{зн}$ – общая сумма зарплат и пособий всех работников за неделю;

$T_{раб}$ – среднее количество рабочих часов в неделю;

$$D_{nom} = \frac{D_{орг}}{T_{бизнес}}, \quad (3)$$

где $D_{орг}$ – общий доход организации за неделю;

$T_{бизнес}$ – среднее количество часов в неделю, когда организация открыта для бизнес-операций.

Расчет показателей доступности информации. Доступность информации зависит от доступности физических и виртуальных компонентов дата-центра. При анализе доступности информации оцениваются частота отказов компонентов и среднее время ремонта, которые определяются в понятиях среднего времени безотказной работы и среднего времени восстановления.

Под средним временем безотказной работы (далее – $T_{без}$) понимается период времени, в течение которого система или компонент ЦОД может выполнять свои функции без сбоев.

Под средним временем восстановления (далее – $T_{восст}$) понимается период времени, в течение которого можно восстановить отказавший компонент.

При вычислении $T_{восст}$ предполагается, что неисправность (физический дефект на компонентном уровне, способный привести к недоступности данных) обнаружена и необходимые детали и персонал доступны. На рис. 3 представлена диаграмма доступности информации, описывающая процессы устранения неисправности компонентов ЦОД [8].

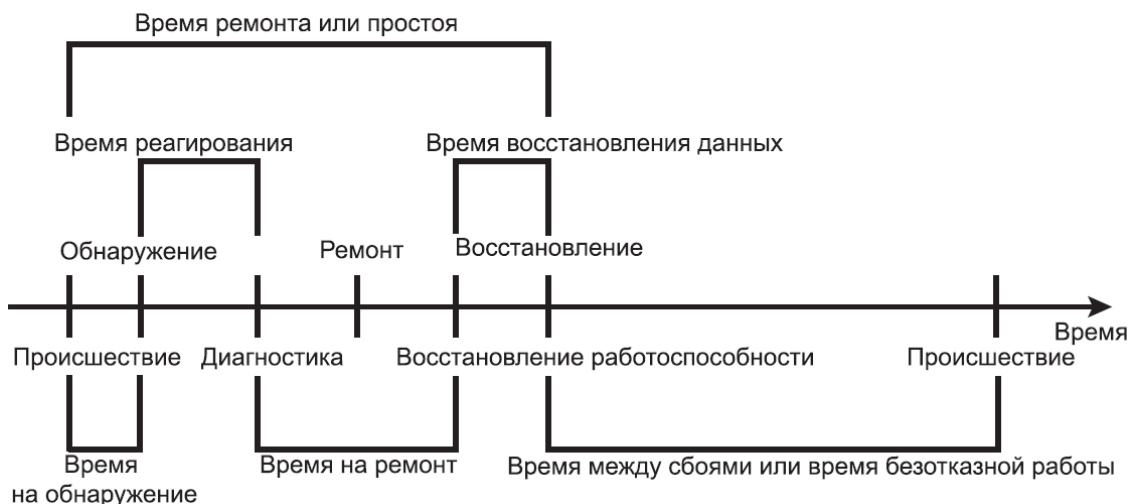


Рис. 3. Диаграмма доступности информации

Повышение готовности информационной системы – один из способов снижения времени ее простоя. Коэффициент готовности ($T_{\text{дост}}$) – это выраженное в процентах отношение времени, когда система предоставляет сервисы своим пользователям, к общему времени работы системы, вычисляется по формуле:

$$T_{\text{дост}} = \frac{T_{\text{без}}}{T_{\text{без}} + T_{\text{восст}}} \times 100\%. \quad (4)$$

Значение коэффициента готовности в течение года основано на конкретных требованиях к своевременности предоставления рассматриваемой службы.

По данным, приведенным в табл. 1–3, по выражению (4), а также по выражениям, приведенным в [9], были рассчитаны показатели доступности информации (табл. 5).

Таблица 5

Показатели доступности информации

Показатели	Количественные данные
Период безотказной работы, час	34990,017
Коэффициент готовности ($T_{\text{дост}}$), %	99,857
Средний период простоя в год, час	12,496
Коэффициент простоя, %	0,143
Среднее время безотказной работы ($T_{\text{без}}$), час	897,180
Среднее время восстановления ($T_{\text{восст}}$), час	1,282

Выводы. После обработки входных данных были рассчитаны коэффициент готовности (4) – 99,8 %, средний период простоя в год – 12,5 часов. Таким образом, из полученных результатов можно сделать следующие выводы:

1. ЦОД компании «РТК-ЦОД» имеет высокий уровень надежности, и, следовательно, обладает всеми необходимыми системами восстановления после сбоев.

2. При наличии данных о численности работников компании, средней заработной плате и среднем доходе предприятия по выражениям (1), (2) и (3) можно вычислить стоимость 1 часа простоя продуктивных систем и стоимость среднего периода простоя в год.

3. Необходимо пересмотреть статистику сбоев и отказов, определить самые длинные периоды простоя и принять меры по предотвращению долгих и непредвиденных отказов путем использования технологий резервирования продуктивных систем, закупки нового оборудования и т. д.

Литература

1. Басина Н. Д. Центры обработки данных: существенные факты // СЮ. 2015. № 2. С. 5–9.
2. Губарева Т. В., Патрусова А. М. Центры обработки данных в Российской Федерации // Проблемы социал.-экономического развития Сибири. 2015. № 2. С. 16–23.
3. Вильчинский Н. В. От хранения данных к управлению информацией. СПб. : Питер, 2016. 544 с.
4. Сэвилл Д. Знакомимся с Hyper-V в Windows Server 2012 // WINDOWS IT PRO/RE. 2013. № 8. С. 58.
5. Гоменюк А. Р., Сопенко С. И. Строим центр обработки данных // Корпоратив. системы. 2017. № 5. С. 6–11.
6. Облачный провайдинг 2014–2018: экономика, стратегии, бизнес-модели. URL: <http://www.iksconsulting.ru/reports-91.html> (дата обращения: 15.09.2019).
7. Джош Джад Основы проектирования SAN. М. : Brocade Россия и СНГ, 2008. 589 с.
8. Таненбаум Э., Уэзеролл Д. Современные компьютерные сети. Изд. 5-е. СПб. : Питер, 2015. 960 с.
9. Острейковский В. А. Теория надежности. М. : Высш.шк., 2003. 463 с.