

И. Д. Гуз, В. А. Острейковский

## АНАЛИЗ ЭКСПЛУАТАЦИОННОЙ НАДЕЖНОСТИ ОБОРУДОВАНИЯ ЦЕНТРА ОБРАБОТКИ ДАННЫХ КРУПНОЙ КОМПАНИИ<sup>1</sup>

I. D. Guz, V. A. Ostreykovsky

### ANALYSIS OF OPERATIONAL RELIABILITY OF EQUIPMENT CENTER FOR DATA PROCESSING OF A MAJOR COMPANY

**Аннотация.** Подробно описано предназначение современных центров обработки данных, даны определения центра обработки данных, отказоустойчивости, доступности информации, сбой, 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 (ЦОД) на основе эксплуатационных данных. Основным свойством, которым должен обладать ЦОД высокого уровня надежности, является отказоустойчивость. Отказоустойчивость ЦОД оценивается с помощью показателей доступности информации. При анализе доступности информации оценивались частота отказов компонентов и среднее время ремонта, которые определяются в понятиях среднего времени безотказной работы и среднего времени восстановления. В качестве показателей надежности были выбраны вероятность безотказной работы и средняя наработка до отказа. После обработки входных данных были рассчитаны период доступности информации, средний период простоя в год. Таким образом, из полученных результатов был сделан следующий вывод, что исследуемый ЦОД имеет высокий уровень надежности, а, следовательно, обладает всеми необходимыми системами восстановления после сбоев.

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

**Abstract.** The article describes in detail the purpose of modern data processing centers, provides data center definitions, fault tolerance, information availability, failures, describes methods for estimating the cost of forced downtime for a company, calculates information availability and reliability indicators. The purpose of this work is to analyze the reliability of data center infrastructure elements based on operational data. The main feature of the fact that the data center must have a high level of reliability is fault tolerance. Resilience of the data center is assessed using information availability indicators. When analyzing the availability of information, the failure rates of the components and the average repair time were estimated, which are determined in terms of the average uptime and average recovery time. As indicators of reliability, we chose the probability of failure-free operation and the average time to failure. After processing the input data, the period of availability of information was calculated, the average period of inactivity for the year. Thus, from the obtained results, the following conclusion was made that the data center under study has a high level of reliability and, therefore, has all the necessary disaster recovery systems.

**Keywords:** data center, data center, fault tolerance, availability, failure, downtime, average uptime, average recovery time, information availability period.

### Введение

В наши дни без непрерывного доступа к информации обеспечить должное проведение бизнес-операций невозможно. Цена недоступности информации возросла как никогда раньше, и даже час простоя в ключевых отраслях промышленности грозит миллионными убытками.

Центры обработки данных востребованы государственными службами (электронное правительство, госуслуги), крупными организациями, такими как банки, страховые и торговые корпорации, предприятия добывающей отрасли, телекоммуникационные компании (биллинговые системы,

<sup>1</sup> Работа выполнена при поддержке РФФИ (Проект №18-47-860007).

хостинги, всевозможные Web-сервисы и социальные службы). Все они используют сложные бизнес-приложения, и их деятельность зависит от надежности функционирования ИТ-инфраструктуры [1].

Целью работы является анализ надежности элементов инфраструктуры ЦОД на основе эксплуатационных данных.

### Задачи и функции современных ЦОД

ЦОД (или дата-центр) – это отказоустойчивая комплексная централизованная система, обеспечивающая автоматизацию бизнес-процессов с высоким уровнем производительности и качеством предоставляемых сервисов.

Современный ЦОД – комплексное решение по управлению информационными системами предприятия. Это совокупность помещений, внешних площадок, инженерного оборудования, образующая единую систему для размещения средств передачи, хранения и обработки информации с заданной степенью доступности. ЦОД включает в себя набор взаимосвязанных программных и аппаратных компонентов, организационных процедур, мест размещения этих компонентов и персонала для безопасной централизованной обработки, хранения и предоставления данных, сервисов и приложений [2].

С системной точки зрения ЦОД – это отказоустойчивое, комплексное, централизованное решение, охватывающее информационные и инженерные системы.

В обычном представлении ЦОД – это специализированное здание, где располагается серверное, сетевое оборудование и системы хранения данных, которые размещаются в стандартных стойках.

Предназначение ЦОД – обеспечение безотказной работы бизнес-процессов, надежное хранение данных и гарантированный доступ к ним.

Перед ЦОД ставится ряд основных задач:

- хранение и анализ большого количества информации;
- обеспечение безопасности ИТ-систем;
- максимальная доступность данных;
- обеспечение высокого уровня резервирования компонентов;
- объединение распределенных систем;
- обеспечение круглосуточной бесперебойной работы.

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, используя следующие методы:

- резервирование физических и виртуальных компонентов ЦОД;
- применение новых технологий хранения, передачи и обработки информации.

Отказоустойчивость ЦОД оценивается с помощью показателей доступности информации. Под доступностью информации понимается состояние инфраструктуры, занимающейся ее обработкой, позволяющее обеспечить работу с информацией в течение времени, отведенного на ту или иную операцию. Доступность информации гарантирует, что люди (служащие, клиенты, поставщики, партнеры) смогут получить доступ к информации в любой необходимый момент времени [3].

Важнейшей задачей управления доступностью является выбор верного направления на основе определенных уровней обеспечения доступности. Управление доступностью включает решение всех вопросов, связанных с доступностью компонентов или служб, с целью обеспечения требуемых уровней обслуживания. Основной деятельностью при управлении доступностью является обеспечение избыточности на всех уровнях, включая компоненты, данные и даже производственные объекты. Например, когда сервер развернут с целью поддержки жизненно важных бизнес-функций, он требует высокого уровня доступности. Как правило, выполнение этого требования обеспечивается развертыванием двух и более контроллеров (НВА-адаптеров), установкой программ, обеспечивающих работу по нескольким маршрутам, и созданием кластера серверов. Сервер должен быть подключен к массиву хранения данных с помощью как минимум двух независимых систем коммутации и коммутаторов, имеющих встроенную избыточность. Кроме того, у массивов хранения данных также должна быть встроенная избыточность различных компонентов, которые должны поддерживать как локальную, так и удаленную репликацию.

Недоступность информации может стать результатом различных плановых и внеплановых событий. К запланированным простоям можно отнести установку, компоновку и обслуживание нового

оборудования, обновления программ или установку обновлений, создание резервных копий, восстановление приложений и данных, проведение работ на объекте (ремонт и строительство), а также обновление и перемещение программ из среды тестирования в эксплуатационную среду. К незапланированным простоям можно отнести сбои, вызванные ошибочными действиями персонала, повреждением баз данных и сбой физических и виртуальных компонентов.

К событиям другого типа, которые могут стать причиной недоступности информации, можно отнести природные или техногенные катастрофы, такие как наводнения, пожары, землетрясения или химические заражения [4].

### Статистические данные сбоев и отказов ЦОД

На рис. 1 и в табл. 1 представлены статистика потерь данных и их причины по данным Ассоциации защиты информации (АЗИ) Российской Федерации.

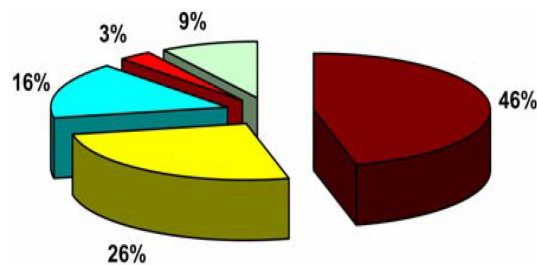


Рис. 1. Статистика потерь данных и их причины

Таблица 1

Статистика потерь данных и их причины

| Причины                                                                  | Значение, % |
|--------------------------------------------------------------------------|-------------|
| Сбой электроэнергии                                                      | 46          |
| Стихийные бедствия (пожары, теракты, ураганы, наводнения, землетрясения) | 26          |
| Программные и аппаратные сбои                                            | 16          |
| Ошибка оператора                                                         | 3           |
| Прочие причины                                                           | 9           |

По данным аналитического агентства «ИКС-Консалтинг» [3] была собрана статистика отказов ЦОД компании «РТК-ЦОД», расположенного в г. Екатеринбурге, за 2015–2018 гг. Данные статистики отказов представлены в табл. 2, 3 и 4, а также на диаграмме (рис. 2).



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

Таблица 2

## Статистика отказов продуктивных систем

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

Таблица 3

## 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 4

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

|                                 |       |
|---------------------------------|-------|
| Количество единиц оборудования  | 463   |
| Отказы с простоем               | 39    |
| Период работы 2015–2018 гг., ч  | 35040 |
| Период простоя 2015–2018 гг., ч | 49,98 |

## Методика расчета стоимости вынужденного простоя

Недоступность данных, или вынужденный простой, может привести к потерям продуктивности и доходов, плохим финансовым показателям и нанесению урона репутации компании. Потери продуктивности уменьшают выработку на единицу труда, оборудования или капитала. Потери доходов включают в себя прямые потери, компенсационные выплаты, а также будущие потери доходов, оплату выставленных счетов за понесенные убытки и потерю инвестиций. Плохие финансовые показатели отрицательно влияют на признание дохода, движение наличности, процент скидки, гарантии платежей, кредитные рейтинги и цены акций. Падение репутации может привести к потере доверия со стороны клиентов, поставщиков, финансовых рынков, банков и бизнес-партнеров. Другие возможные последствия простоя включают в себя стоимость аренды дополнительного оборудования, выплату за сверхурочную работу и оплату доставки оборудования.

Влияние простоя складывается из всех понесенных в результате данного нарушения режима работы потерь. Ключевую оценку при определении влияния простоя на доходы предприятия позволяют дать такие показатели, как средняя стоимость простоя в час (далее –  $C_{пр}$ ), средняя потеря продуктивности в час (далее –  $P_{пот}$ ), средняя потеря дохода в час (далее –  $D_{пот}$ ), которые вычисляются по формулам

$$C_{пр} = P_{пот} + D_{пот}, \quad (1)$$

где  $C_{пр}$  – средняя стоимость простоя в час;  $P_{пот}$  – средняя потеря продуктивности в час;  $D_{пот}$  – средняя потеря дохода в час;

$$P_{пот} = \frac{C_{зп}}{T_{раб}}, \quad (2)$$

где  $C_{\text{зп}}$  – общая сумма зарплат и пособий всех работников за неделю;  $T_{\text{раб}}$  – среднее количество рабочих часов в неделю;

$$D_{\text{пот}} = \frac{D_{\text{орг}}}{T_{\text{биз}}}, \quad (3)$$

где  $D_{\text{орг}}$  – общий доход организации за неделю;  $T_{\text{биз}}$  – среднее количество часов в неделю, когда организация открыта для бизнес-операций.

Средняя стоимость простоя может также включать в себя оценки прогнозируемых потерь дохода от других последствий, таких как ухудшение репутации и дополнительные затраты на восстановление работоспособности системы [1, 5].

### 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 –  $T_{\text{без}}$ ) понимается период времени, в течение которого система или компонент ЦОД может выполнять свои функции без сбоев.

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

При вычислении  $T_{\text{вост}}$  предполагается, что неисправность, приведшая к сбою, обнаружена и необходимые детали и персонал доступны. Под неисправностью понимается физический дефект на компонентном уровне, который может привести к недоступности данных.  $T_{\text{вост}}$  включает в себя время, необходимое для того, чтобы произвести следующие действия: обнаружить неисправность, привлечь ремонтную бригаду, провести диагностику неисправности, приобрести запасные части, провести ремонт, тестирование и восстановление данных. На рис. 3 представлена диаграмма доступности информации, описывающая процессы устранения неисправности компонентов ЦОД [1].

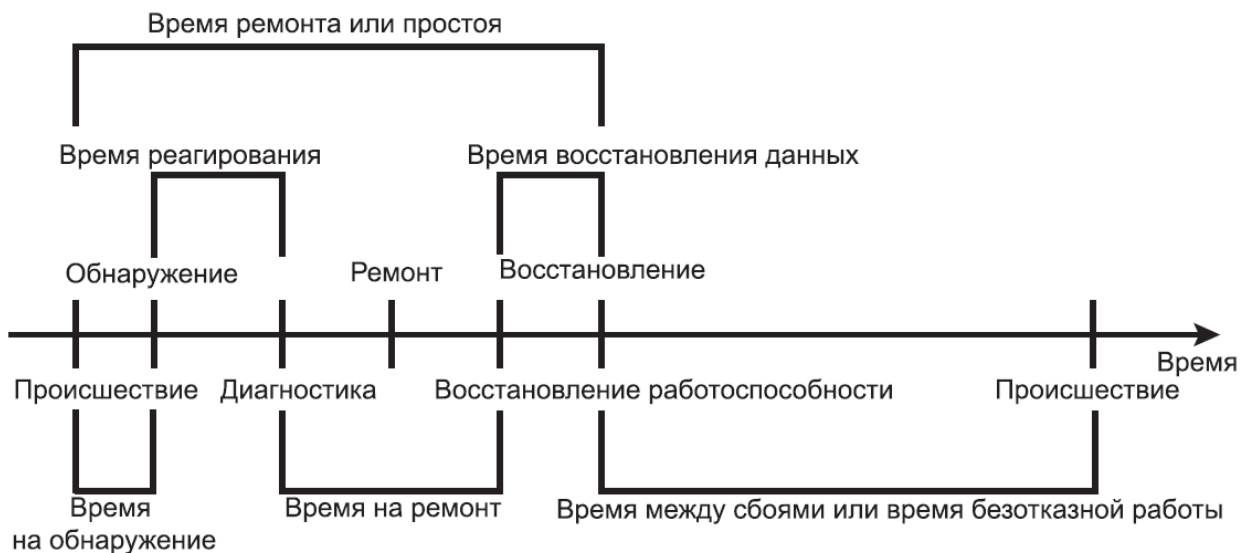


Рис. 3. Диаграмма доступности информации

Период доступности информации (далее –  $T_{\text{дост}}$ ) – это время, в течение которого система в состоянии выполнять возлагаемые на нее функции по предназначению, оценивается в процентном показателе безотказного периода работы системы, вычисляется по формуле

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

Значение периода безотказной работы в течение года основано на конкретных требованиях к своевременности предоставления рассматриваемой службы. Его вычисление приводит к определению количества девяток, фигурирующих в показателях доступности. В табл. 5 приведены средние значения периода простоя, допустимые для службы, при которых можно достичь конкретного уровня девяток в показателе доступности.

Таблица 5

## Средние значения периода простоя

| Период доступности информации, % | Период простоя, % | Время простоя за год | Время простоя за неделю |
|----------------------------------|-------------------|----------------------|-------------------------|
| 98                               | 2                 | 7,3 дня              | 3 часа 22 минуты        |
| 99                               | 1                 | 3,65 дня             | 1 час 41 минута         |
| 99,8                             | 0,2               | 17 часов 31 минута   | 20 минут 10 секунд      |
| 99,9                             | 0,1               | 8 часов 45 минут     | 10 минут 5 секунд       |
| 99,99                            | 0,01              | 52,5 минуты          | 1 минута                |
| 99,999                           | 0,001             | 5,25 минуты          | 6 секунд                |
| 99,9999                          | 0,0001            | 31,5 секунды         | 0,6 секунды             |

По данным приведенным в табл. 2, 3 и 4, по выражению (4), а также по выражениям, приведенным в работах [7, 8], были рассчитаны показатели доступности информации (табл. 6).

Таблица 6

## Показатели доступности информации

|                                                         |           |
|---------------------------------------------------------|-----------|
| Период безотказной работы, ч                            | 34990,017 |
| Период доступности информации $T_{\text{дост}}$ , %     | 99,857    |
| Средний период простоя в год, час                       | 12,496    |
| Период недоступности информации, %                      | 0,143     |
| Среднее время безотказной работы $T_{\text{без}}$ , час | 897,180   |
| Среднее время восстановления $T_{\text{восст}}$ , час   | 1,282     |
| Вероятность безотказной работы $P(t)$                   | 0,916     |
| Вероятность отказа $Q(t)$                               | 0,084     |

## Заключение

После обработки входных данных были рассчитаны период доступности информации (4), средний период простоя в год – 99,8 % и 12,5 ч соответственно. Таким образом, из полученных результатов можно сделать следующие выводы:

1. ЦОД компании «РТК-ЦОД» имеет высокий уровень надежности, а следовательно, обладает всеми необходимыми системами восстановления после сбоев [9–11].

2. При наличии данных о численности работников компании, средней заработной плате и среднего дохода предприятия по выражениям 1,2 и 3 можно вычислить стоимость 1 ч 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 увеличения численности персонала, закупки нового оборудования и т.д.

## Библиографический список

1. Вильчинский, Н. В. От хранения данных к управлению информацией / Н. В. Вильчинский. – Санкт-Петербург : Питер, 2016. – 544 с.
2. Джад, Д. Основы проектирования SAN / Д. Джад. – Москва : Brocade Россия и СНГ, 2008. – 589 с.
3. Басина, Н. Д. Центры обработки данных: Существенные факты / Н. Д. Басина // СЮ. – 2015. – № 2. – С. 5–9.
4. Гоменюк, А. Р. Строим центр обработки данных / А. Р. Гоменюк, С. И. Сопенко // Корпоративные системы. – 2017. – № 5. – С. 6–11.
5. Орлов, С. А. Оптимальный ЦОД / С. А. Орлов // Журнал сетевых решений Lan. – 2011. – С. 50–61.

6. Острейковский, В. А. Теория надежности : учеб. для вузов / В. А. Острейковский. – Москва : Высш. шк., 2003. – 463 с.
7. Гмурман, В. Е. Теория вероятностей и математическая статистика : учеб. пособие / В. Е. Гмурман. – Москва : Высшее образование, 2008. – 479 с
8. Острейковский, В. А. Анализ моделей распределения характеристик техногенного риска по статистическим данным аварий и катастроф сложных критически важных объектов / В. А. Острейковский, Е. Н. Шевченко // Надежность и качество сложных систем. – 2015. – № 2 (10). – С. 3–12.
9. Острейковский, В. А. Математические модели оценки техногенного риска сложных систем на основе распределения Эрланга / В. А. Острейковский, А. С. Павлов // Надежность и качество сложных систем. – 2016. – № 1. – С. 99–116.
10. Гришко, А. К. Выбор оптимальной стратегии управления надежностью и риском на этапах жизненного цикла сложной системы / А. К. Гришко // Надежность и качество сложных систем. – 2017. – № 2 (18). – С. 26–31.
11. Мишанов, Р. О. Методика определения набора информативных параметров для проведения индивидуального прогнозирования показателей качества и надежности радиоэлектронных средств / Р. О. Мишанов, М. Н. Пиганов // Надежность и качество сложных систем. – 2017. – № 1 (17). – С. 93–104.

### References

1. Vil'chinskiy N. V. *Ot khraneniya dannykh k upravleniyu informatsiy* [From data storage to information management]. Saint-Petersburg: Piter, 2016, 544 p. [In Russian]
2. Dzhad D. *Osnovy proektirovaniya SAN* [SAN design basics]. Moscow: Brocade Rossiya i SNG, 2008, 589 p. [In Russian]
3. Basina N. D. *CIO*. 2015, no. 2, pp. 5–9.
4. Gomenyuk A. R., Sopenko S. I. *Korporativnye sistemy* [Corporate system]. 2017, no. 5, pp. 6–11. [In Russian]
5. Orlov S. A. *Zhurnal setevykh resheniy Lan* [Journal of LAN network solutions]. 2011, pp. 50–61. [In Russian]
6. Ostreykovskiy V. A. *Teoriya nadezhnosti: ucheb. dlya vuzov* [Reliability theory: textbook for universities]. Moscow: Vyssh. shk., 2003, 463 p. [In Russian]
7. Gmurman V. E. *Teoriya veroyatnostey i matematicheskaya statistika: ucheb. posobie* [Probability theory and mathematical statistics: a textbook]. Moscow: Vysshee obrazovanie, 2008, 479 p. [In Russian]
8. Ostreykovskiy V. A., Shevchenko E. N. *Nadezhnost' i kachestvo slozhnykh sistem* [Reliability and quality of complex systems]. 2015, no. 2 (10), pp. 3–12. [In Russian]
9. Ostreykovskiy V. A., Pavlov A. S. *Nadezhnost' i kachestvo slozhnykh sistem* [Reliability and quality of complex systems]. 2016, no. 1, pp. 99–116. [In Russian]
10. Grishko A. K. *Nadezhnost' i kachestvo slozhnykh sistem* [Reliability and quality of complex systems]. 2017, no. 2 (18), pp. 26–31. [In Russian]
11. Mishanov R. O., Piganov M. N. *Nadezhnost' i kachestvo slozhnykh sistem* [Reliability and quality of complex systems]. 2017, no. 1 (17), pp. 93–104. [In Russian]

#### Гуз Игорь Дмитриевич

аспирант,  
Сургутский государственный университет  
(628412, Россия, г. Сургут, проспект Ленина, 1)  
E-mail: idguzzz@gmail.com

#### Острейковский Владислав Алексеевич

доктор технических наук, профессор,  
кафедра информатики и вычислительной техники,  
Сургутский государственный университет  
(628412, Россия, г. Сургут, проспект Ленина, 1)  
E-mail: ostreykovsky\_va@surgu.ru

#### Guz Igor Dmitrievich

postgraduate student,  
Surgut State University  
(628412, 1 Lenin avenue, Surgut, Russia)

#### Ostreykovsky Vladislav Alekseevich

doctor of technical sciences, professor,  
sub-department of informatics and computer science,  
Surgut State University  
(628412, 1 Lenin avenue, Surgut, Russia)

#### Образец цитирования:

Гуз, И. Д. Анализ эксплуатационной надежности оборудования центра обработки данных крупной компании / И. Д. Гуз, В. А. Острейковский // Надежность и качество сложных систем. – 2019. – № 4 (28). – С. 87–93. – DOI 10.21685/2307-4205-2019-4-9.