Мир ЦОД: обзор злободневных тем

ЦОД: Модели, сервисы, инфраструктура

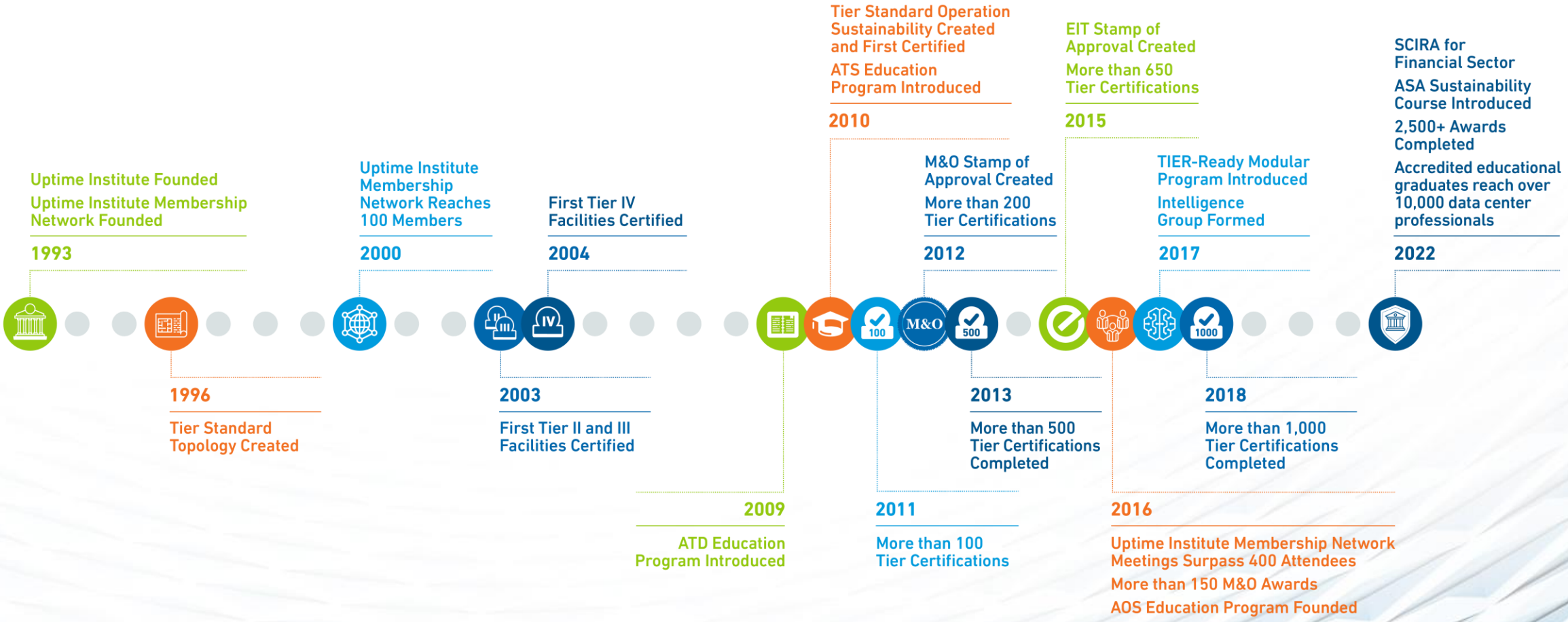
Казань, 20 апреля 2023

Konstantin Korolev

Director, Business Development
Uptime Institute

uptime INSTITUTE

30 лет Uptime Institute



uptime INSTITUTE

Наши приоритеты

- Глобальный опыт и экспертиза
- Снижение инфраструктурных рисков
- Эксплуатационная эффективность
- Управляемость затрат
- Рациональность и инновации
- Технологическая нейтральность
- Профессиональное развитие
- Аналитика и исследования
- Сообщество участников отрасли

Uptime Institute – это доверие,
и мы горды успехами наших партнеров.

uptime INSTITUTE

Обзор злободневных тем

- Плотность мощности стоек
- Отказы в ЦОД
- Глобальное потепление
- Кибербезопасность
- Sustainability
- Персонал ЦОД
- Edge

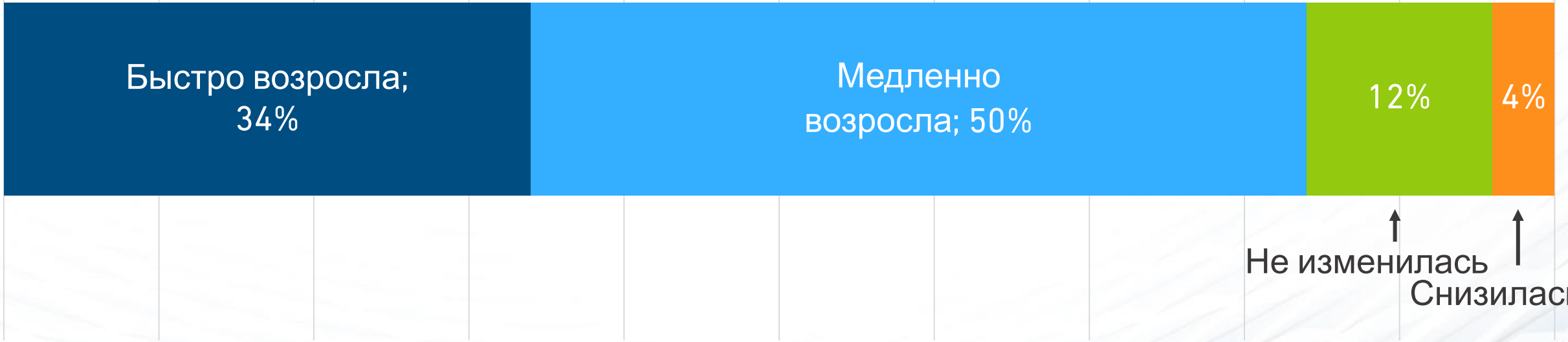
uptime INSTITUTE

Плотность мощности стоек

- Плотность мощности стоек возрастает. Каждая третья показывает быстрый темп роста
- 43% стоек имеют мощность 4-6 кВт, 18% - 7-9 кВт
- Максимальная нагрузка на стойку – до 10 кВт в 36% ЦОДов, от 10 до 19 кВт в 38% ЦОДов
- Высокоплотные стойки обычно размещены у владельца, но показывают тенденцию к миграции в колокейшн

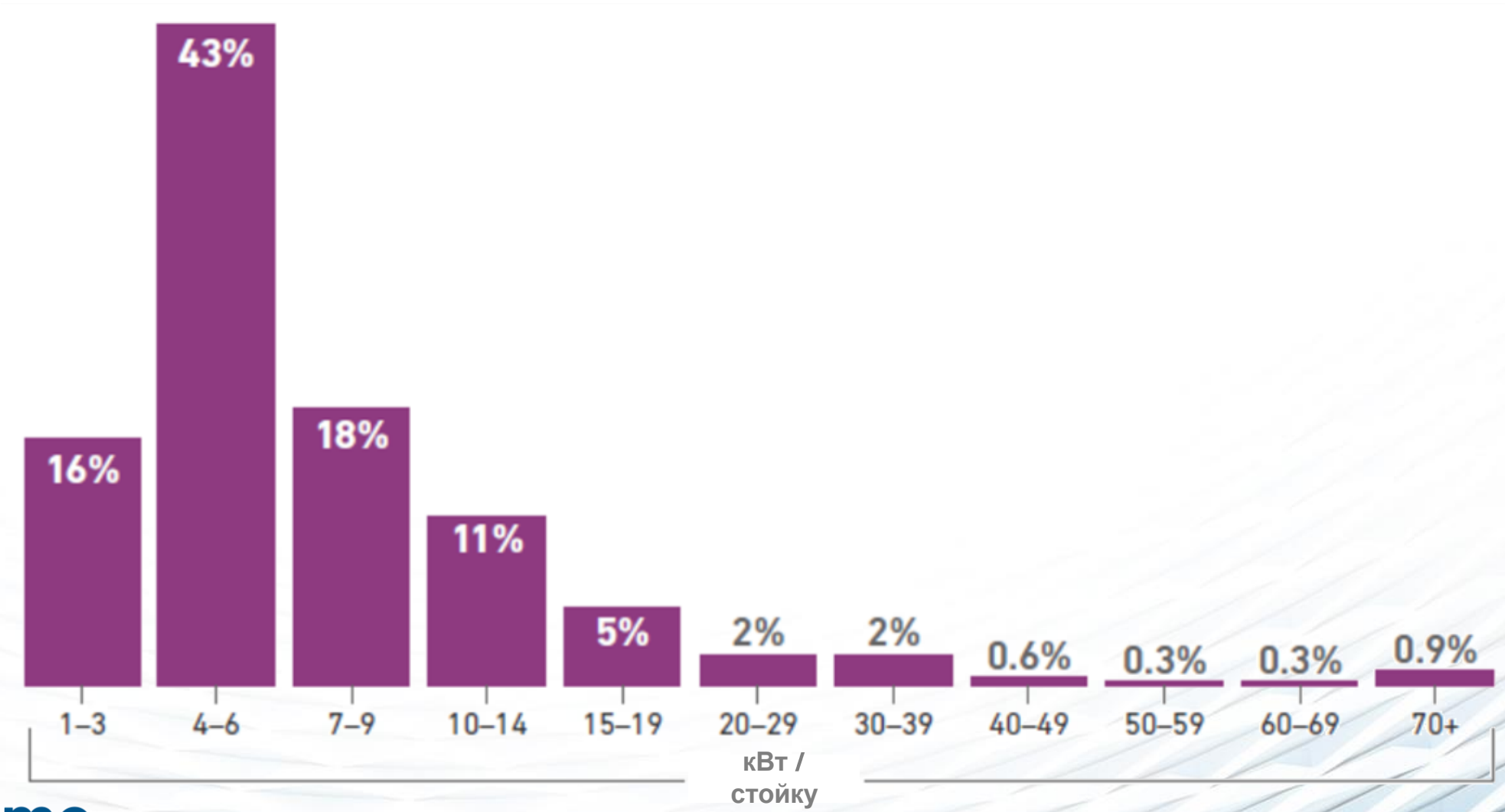
uptime INSTITUTE

Как изменилась плотность мощности стоек в вашем ЦОД за последние три года?



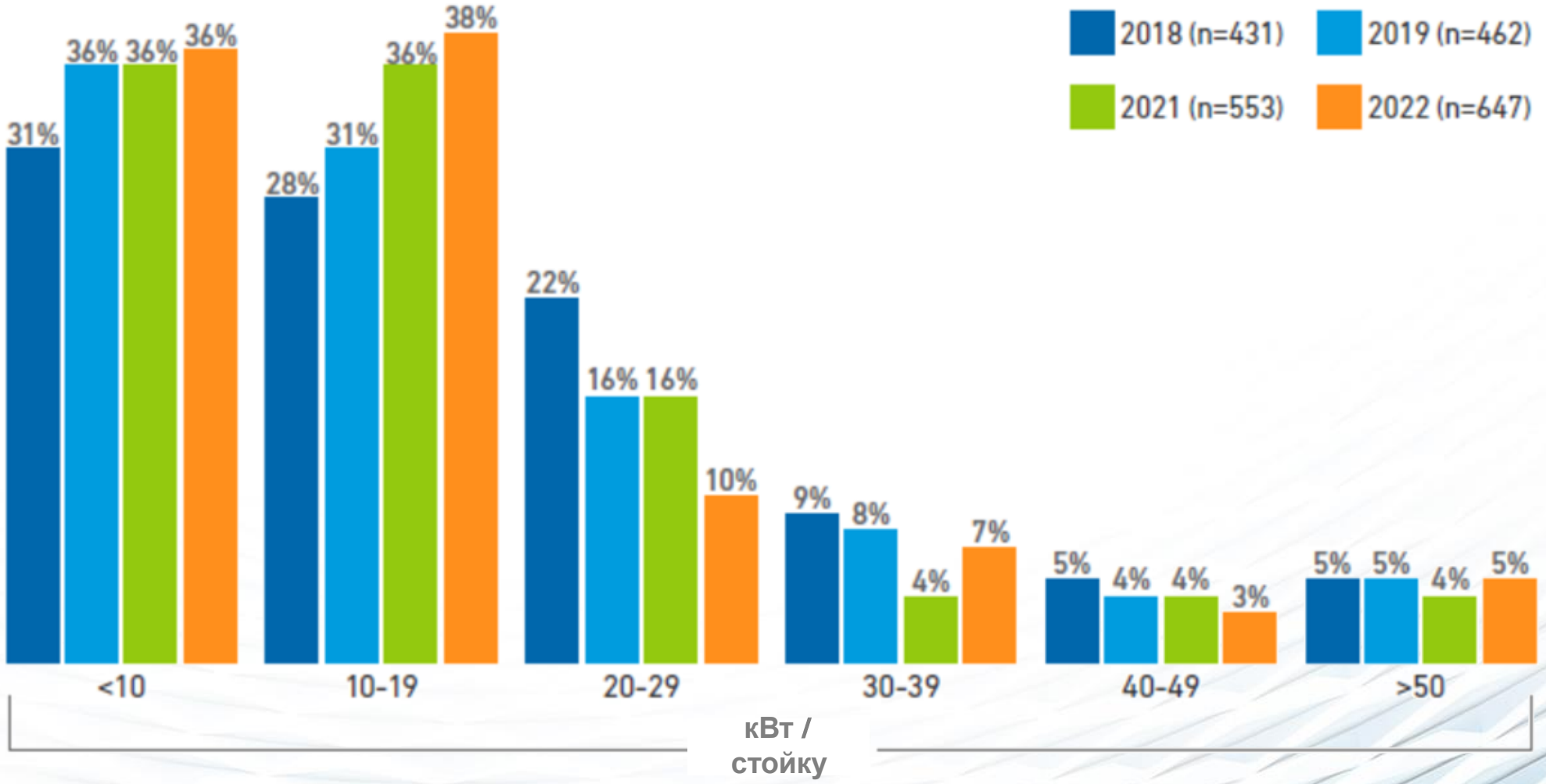
uptime INSTITUTE

Какова средняя мощность на стойку в вашем ЦОД?



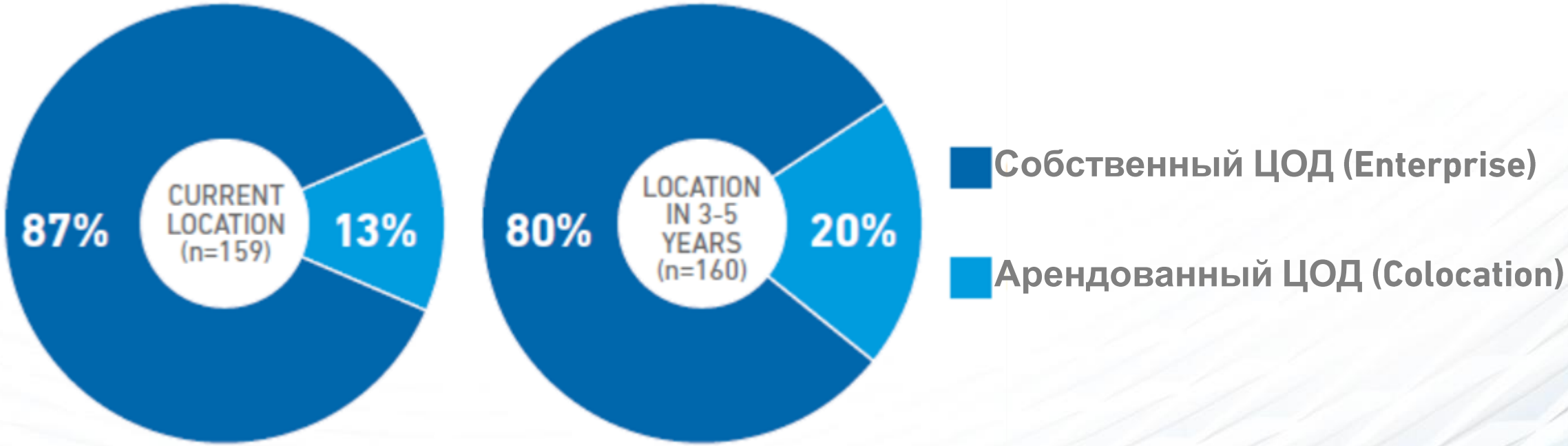
uptime INSTITUTE

Какова максимальная мощность на стойку в вашем ЦОД?



uptime INSTITUTE

Где размещены ваши самые нагруженные стойки? И где будут размещены через 3-5 лет?

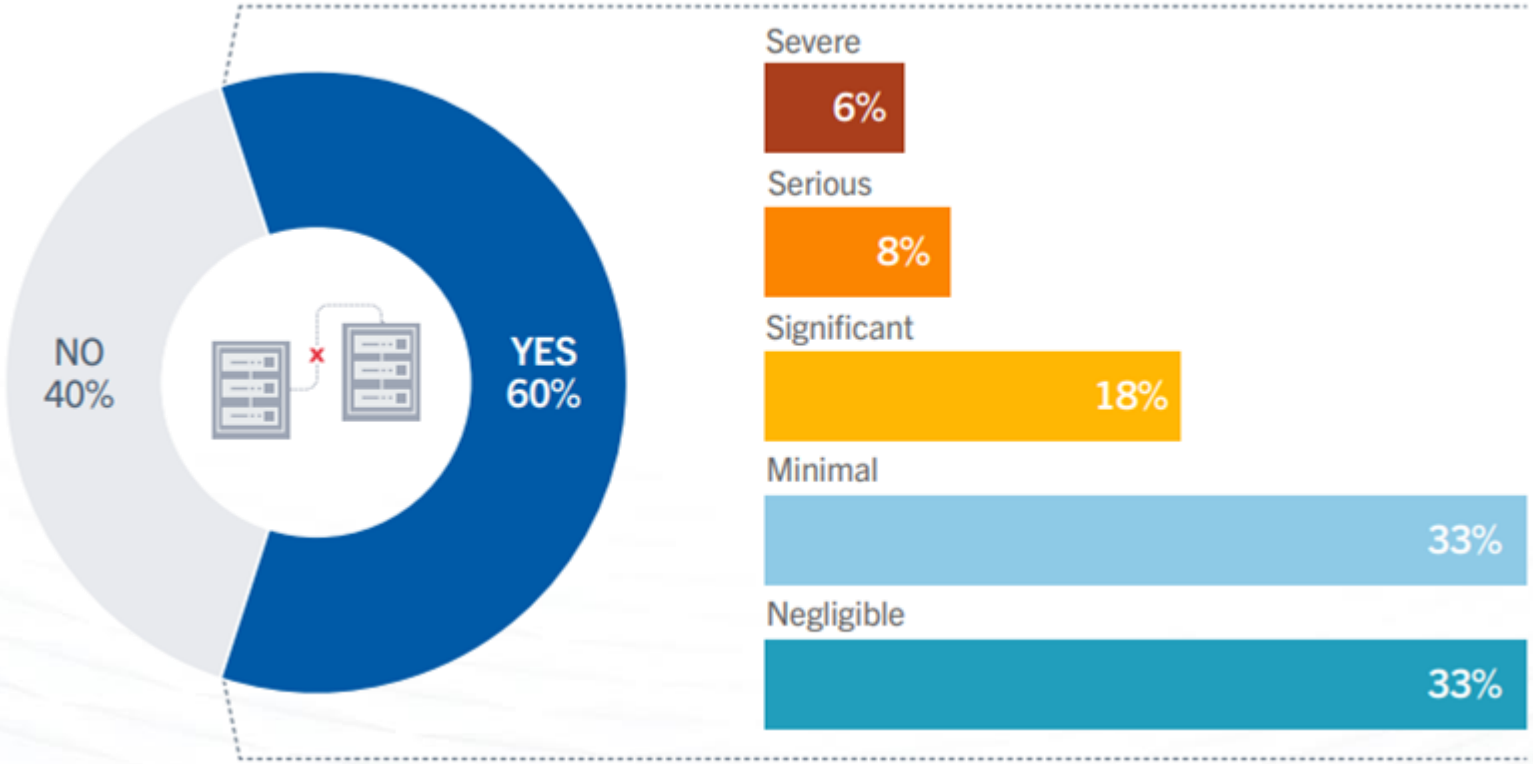


Отказы в ЦОД

- Отказы продолжают происходить регулярно, но число «тяжелых случаев» сокращается
- Основными причинами отказов сервисов являются системы электропитания (ИБП, ДГУ и АВР), далее – сети, системы охлаждения и ИТ-системы
- Несмотря на широкое применение геораспределенной модели, призванной минимизировать последствия отказов, степень резервирования критических систем на уровне ЦОД продолжает расти
- «Человеческий фактор» продолжает быть частой причиной отказов, как правило, в силу неверных управленческих решений, нечетких или неполных регламентов или нарушения персоналом процедур в ходе их исполнения

uptime INSTITUTE

За последние три года сталкивались ли вы с отказами в ЦОД и, если да, насколько серьезными оказывались последствия?

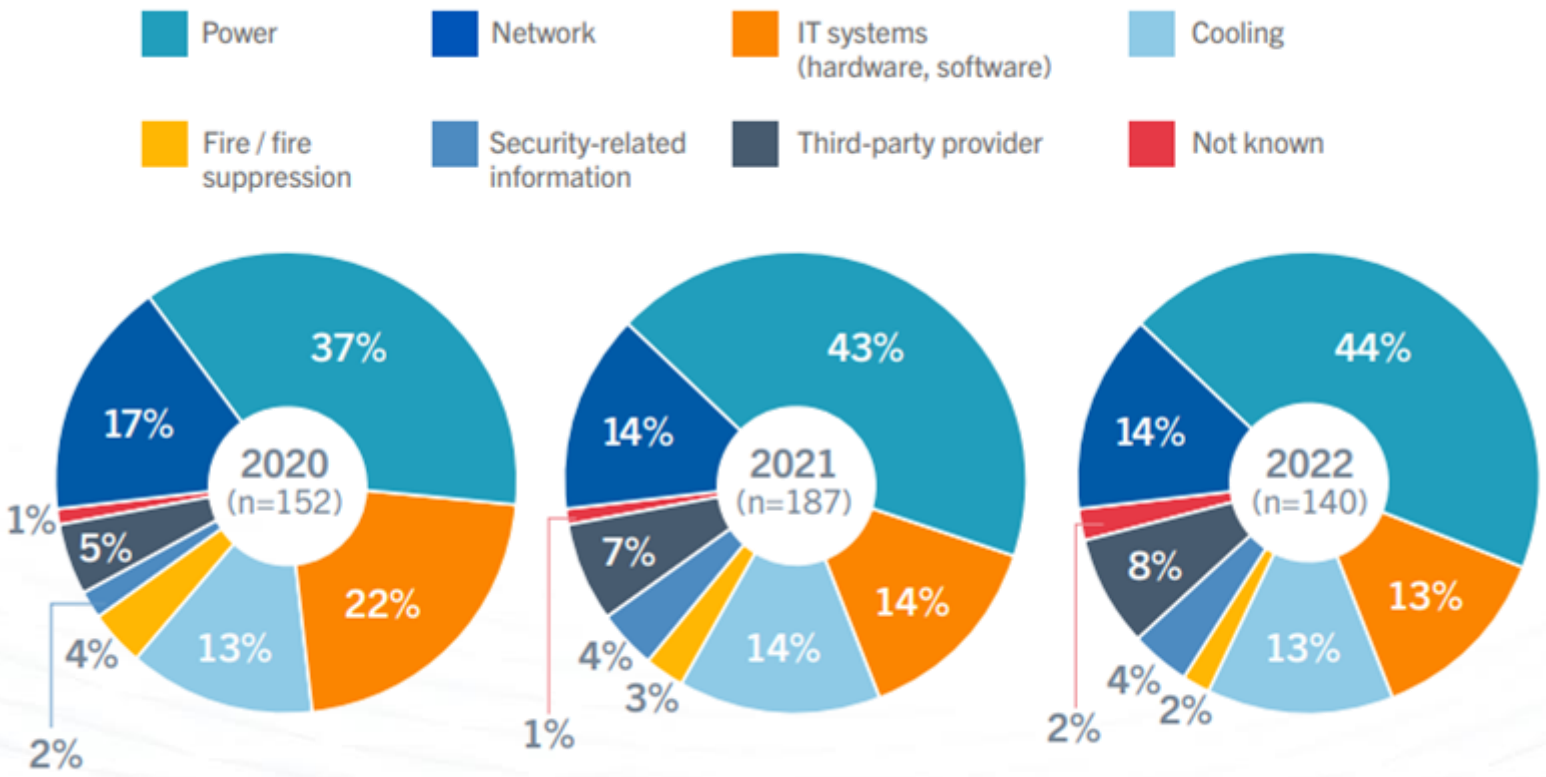


Несмотря на громкие пугающие случаи отказов, освещаемые в СМИ, число серьезных происшествий сокращается

Эта тенденция, вероятно, отражает рост использования облаков и распределенной инфраструктуры, смягчающих последствия отказов в ЦОД

uptime INSTITUTE

Что явилось причиной отказа сервисов в вашем ЦОД?

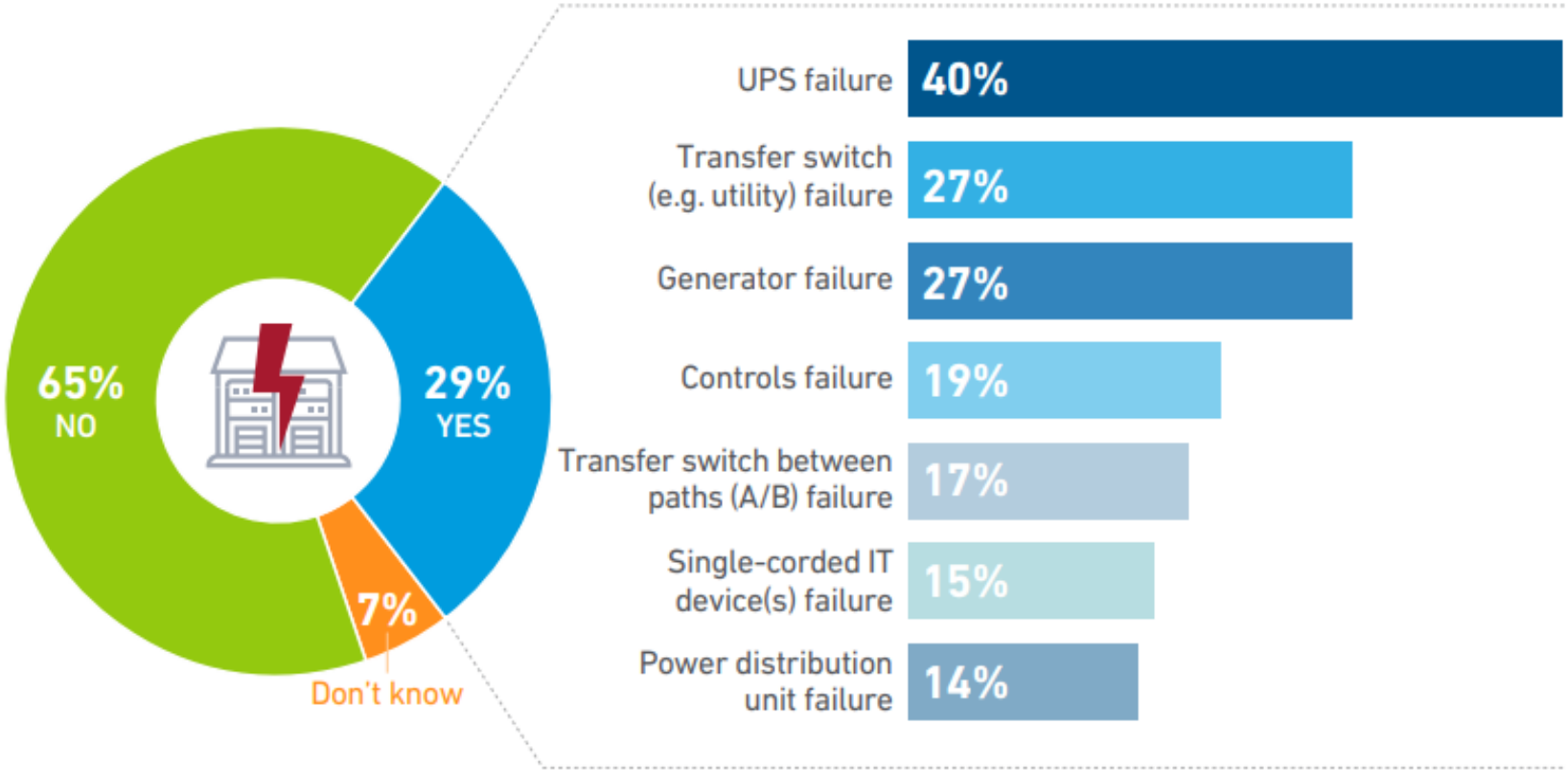


Самой проблемной остается система электропитания, за которой следуют система охлаждения, ИТ-системы и сети

Постепенно возрастает доля отказов по вине стороннего провайдера

uptime INSTITUTE

За последние три года сталкивались ли вы с отказом по причине системы электропитания и, если да, какие компоненты были причиной (выберите не более трех)?



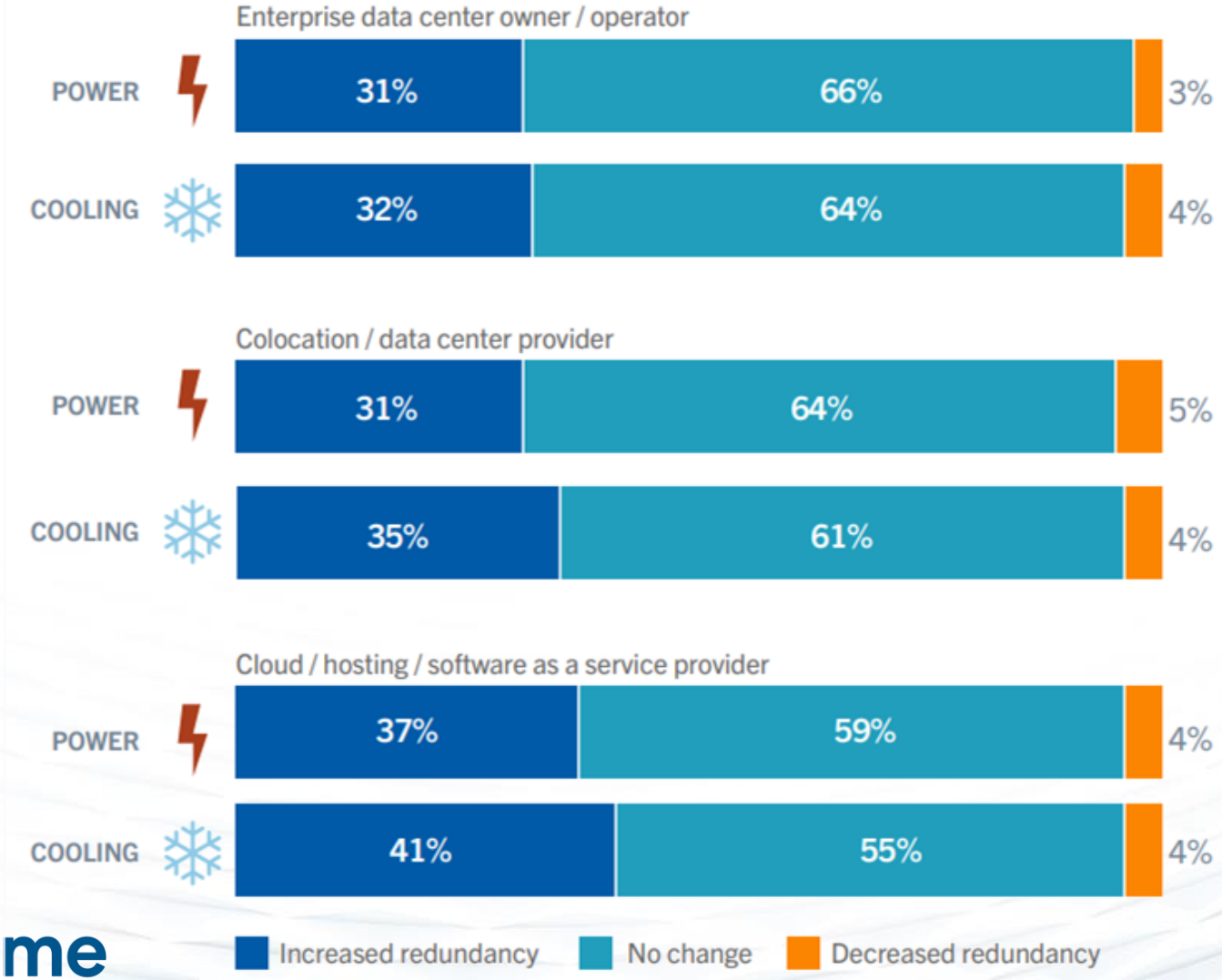
Самой частой причиной отказа является ИБП

Незапуск ДГУ и неудачное переключение АВР с «города» на ДГУ и обратно – также частый случай

Имеет ли смысл сокращение времени автономии ИБП, что стало частым явлением?

uptime INSTITUTE

Как изменились уровни резервирования критических подсистем в вашем ЦОД за последние 3-5 лет?

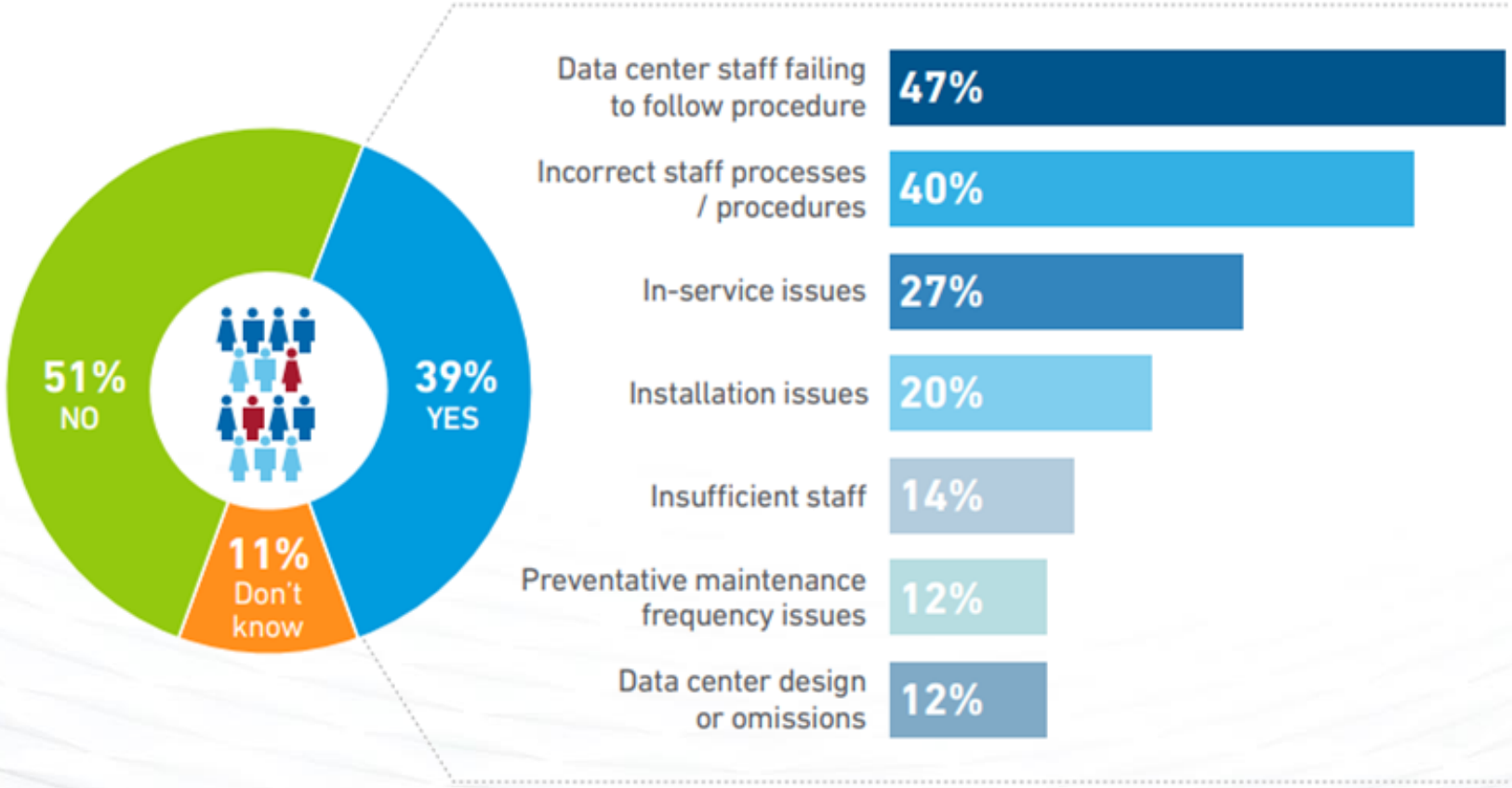


Обеспечение высокого уровня резервирования критических систем на уровне ЦОД не теряет востребованности, несмотря на переход к георасределенной инфраструктуре на базе нескольких ЦОД

Наибольшая актуальность высокого уровня резервирования предсказуемо наблюдается у поставщиков услуг ЦОД

uptime INSTITUTE

за последние три года сталкивались ли вы с отказом по причине «человеческого фактора» и, если да, что именно явилось причиной (выберите не более трех)?



«Человеческий фактор» продолжает быть основной причиной происшествий в ЦОД

Разработка четких рабочих процессов, детальное следование процедурам и развитие персонала продолжают быть на недостаточном уровне

Недостаток навыков и отсутствие регулярных учений негативно отражаются на работе службы эксплуатации

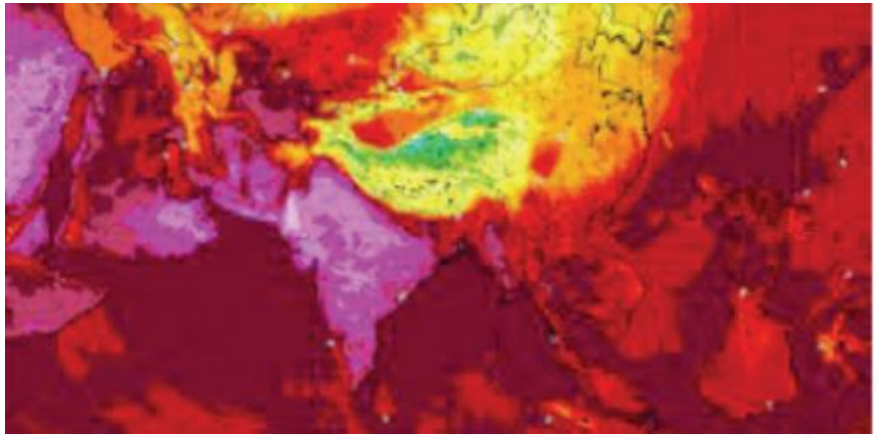
uptime INSTITUTE

Глобальное потепление

- Погодные аномалии последних лет вызывали серьезные отказы. Их причиной становилось то, что ЦОДы не были спроектированы для работы в тех условиях, в которых оказывались
- **70%** операторов ЦОД проводят анализ работоспособности систем в условиях, ранее не свойственных данной территории
- **50%** ЦОД, проводя данный анализ, следуют внутренним или внешним требованиям проведения данного анализа
- Целесообразно проводить подобный анализ для существующих ЦОД, а для проектируемых учитывать условия более тяжелые, нежели приведены в статистических данных

uptime INSTITUTE

2022 год показал, что погода бывает непредсказуемо опасна для ЦОД



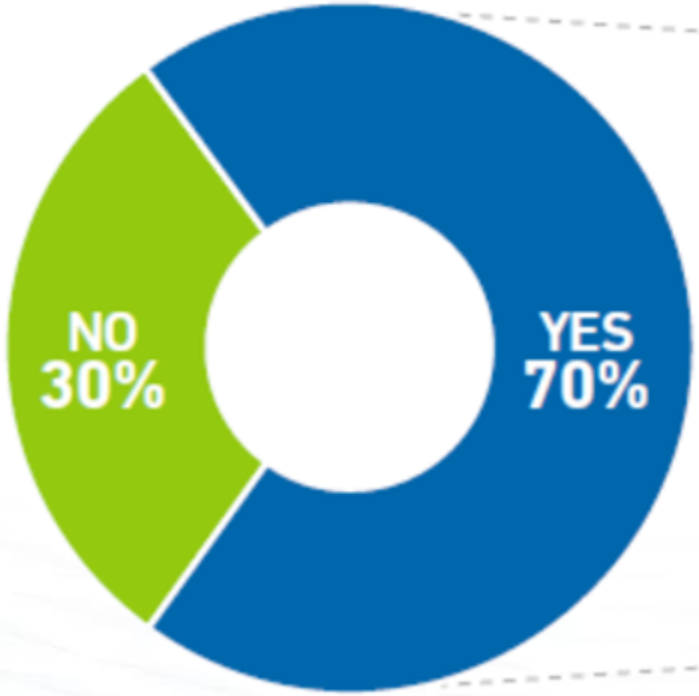
Июль 2022: Небывалая жара в Лондоне вызвала отключение ресурсов Google и Oracle в коммерческом ЦОД.
Это произошло из-за отключения обеих независимых взаиморезервирующих систем охлаждения, рабочие параметры которых были заметно ниже температуры в 39°C

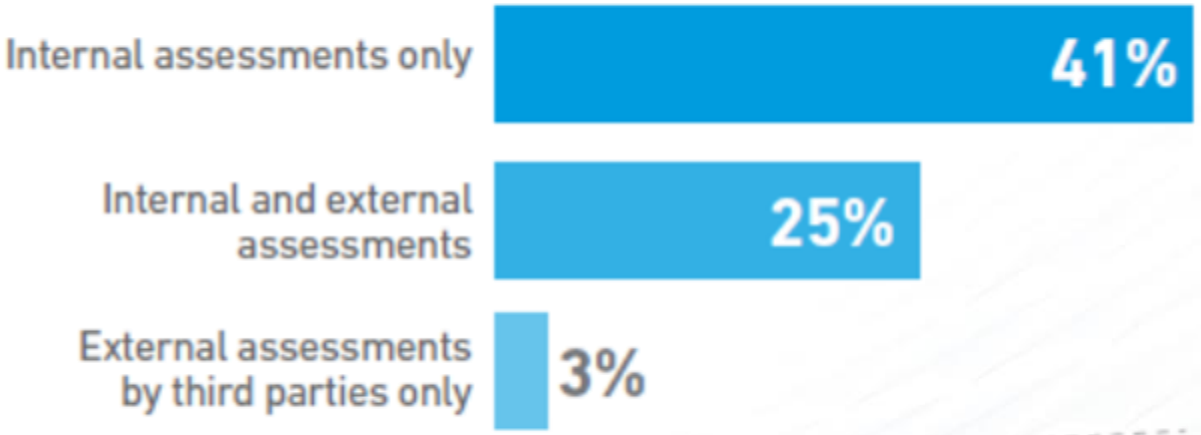
Тогда же, там же отключился ЦОД сети больниц, что повлекло убытки в 115M$.

В Сакраменто, США, произошло отключение ЦОДа Twitter, также по причине экстремальной жары.

Многие ЦОДы, в том числе некоторые в России, не испытывали отключения, но переходили в аварийные режимы работы.

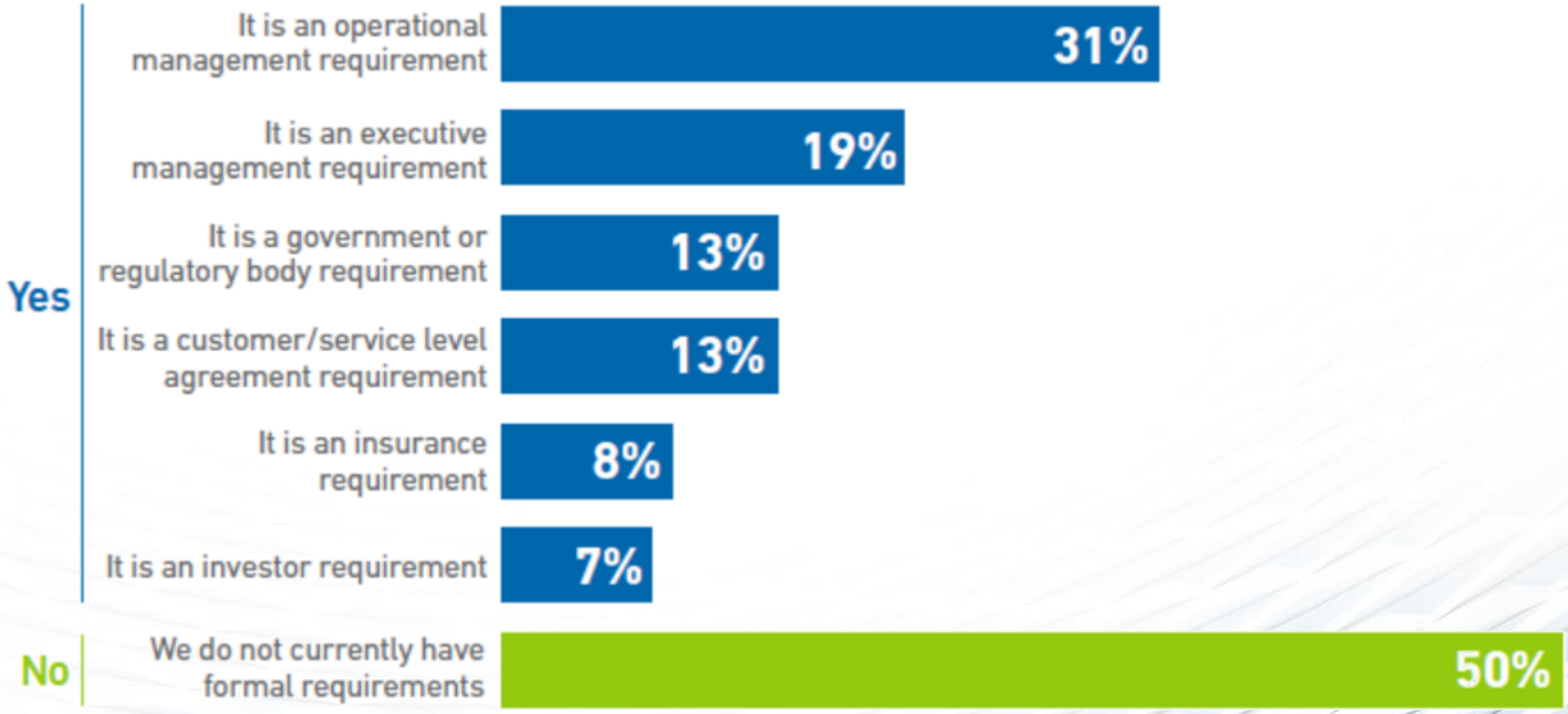
Проводится ли в вашей организации анализ устойчивости ЦОД к изменениям климата?





uptime INSTITUTE

Есть ли у вас формальное требование к проведению анализа устойчивости ЦОД к изменениям климата?



uptime INSTITUTE

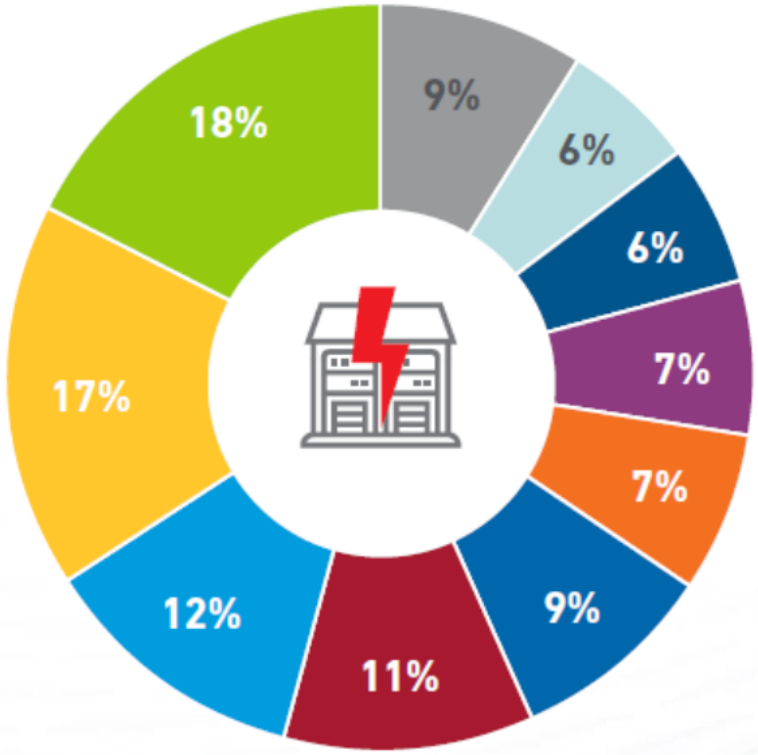
Кибербезопасность

- Один из десяти случаев отказов сервисов ЦОД связан с информационной безопасностью (**DDoS**, **ransomware** и пр.)
- Хотя кибератакам обычно подвергаются ИТ системы, мы наблюдаем рост случаев атак на ОТ-ресурсы, особенно **ransomware**
- Целями атаки могут быть шпионаж, завладение информацией об обслуживании объекта, перехват контроля за различными системами, получение данных о персонале или взаимодействии с третьими лицами и пр.
- Разработать и внедрить соответствующие меры защиты

uptime INSTITUTE

Причины серьезных отказов сервисов в ЦОД, объявленные публично в 2022 году

- IT (software / configuration)
- Fiber
- Network (software / configuration)
- Cyberattack / ransomware
- Power
- Fire
- Provider / partner issue
- Capacity / demand
- Cooling
- Network (cabling)



(n=103)

(Category 1, negligible, outages omitted.)

11% всех серьезных отказов сервисов в ЦОД, о которых объявлялось публично, вызваны кибератаками

Хотя кибератакам обычно подвергаются ИТ системы, мы наблюдаем рост случаев атак на ОТ-ресурсы

uptime INSTITUTE

Пример из новостей – 13.04.2023

11:57 ФСБ зафиксировала свыше 5000 кибератак на российскую инфраструктуру за год

Всего с начала 2022 года специалисты зафиксировали более пяти тысяч хакерских атак против критической инфраструктуры России.

развернута беспрецедентная киберкампания по выведению из строя информационной структуры. Большое количество цифровых атак в 2022 году было направлено на хищение информации и нарушение технологических процессов, а также вмешательство в работу объектов, которые могут иметь общественный резонанс.

uptime INSTITUTE

Operational Technologies (OT) – новая цель

Новыми целями киберпреступников становятся различные системы управления, составляющие OT-ресурсы:

- **DCIM**
- **BMS**
- **Системы управления электропитанием, охлаждением**
- **Системы физической безопасности**
- **Контроль доступа**
- **Видеонаблюдение**
- **Освещение**
- **Водоснабжение**
- **PLC**
- **CMMS**
- **Различные удаленные системы**

Operational Technologies (OT) – новая цель

Для снижения рисков атак на OT необходимо:

- **Оценить подверженность OT атакам**
- **Сегментировать сети, ограничивать доступ извне / наружу или физически разделять сети**
- **Ограничивать удаленный доступ**
- **Разработать и внедрить жесткие политики обращения с чувствительной информацией**
- **Обязательно делать копии , в т.ч. автономные, всей чувствительной информации**
- **Проводить обучение и тренинги персонала**
- **Использовать средства защиты**
- **Проводить анализ инцидентов**
- **Осуществлять строгий контроль за работой с подрядчиками**
- **Разработать программу нейтрализации последствий утечки данных**

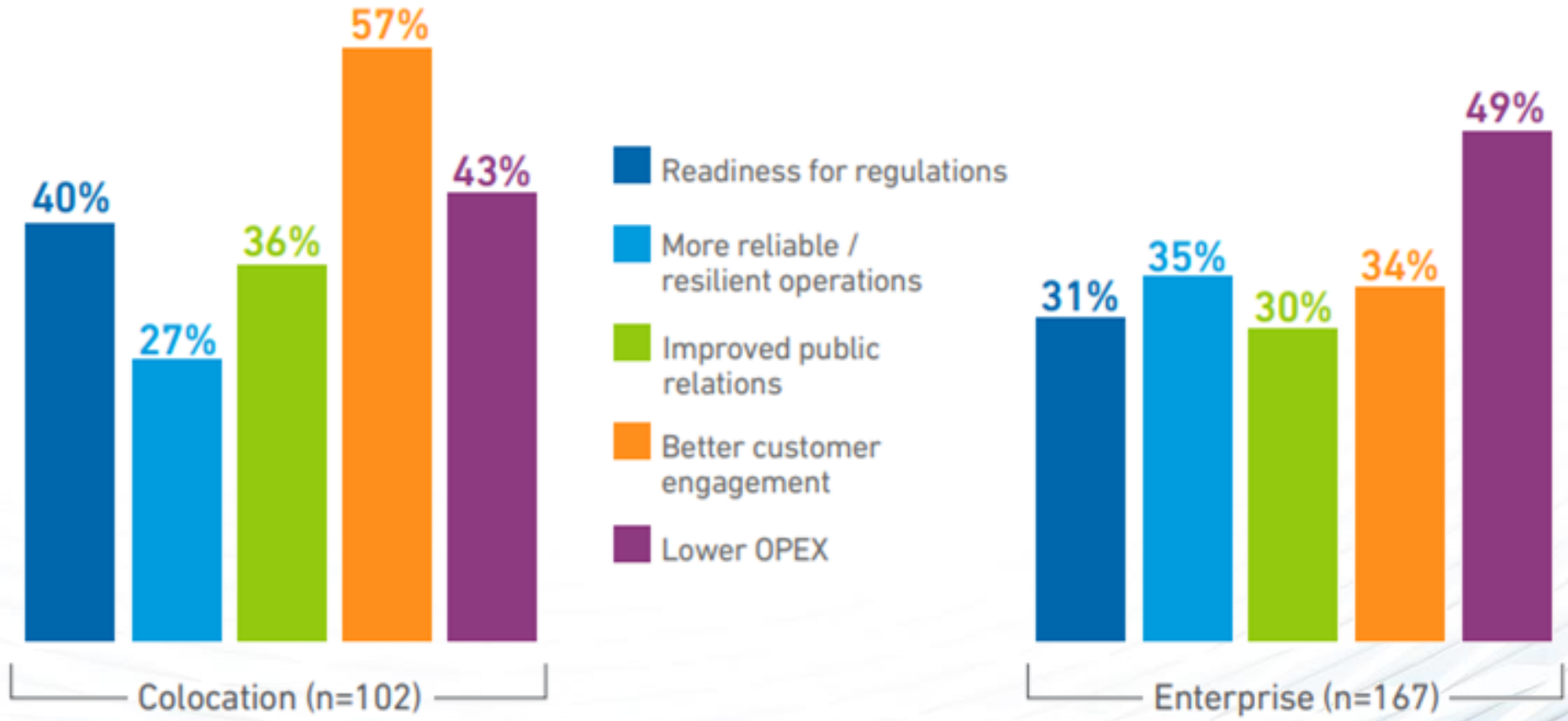
uptime INSTITUTE

Sustainability. «Устойчивое развитие»

- Если отбросить долю хайпа, то суть – в повышении эффективности и экологической ответственности
- Тема востребована преимущественно в Европе, где регулируется рядом протоколов и директив
- Основные драйверы – более эффективное охлаждение, повышение утилизации ИТ-ресурсов и возобновляемые источники энергии
- Основная сложность – снижение углеродного следа как от ИТ-оборудования, так и от ЦОД в целом, а также доступ к возобновляемым источникам

uptime INSTITUTE

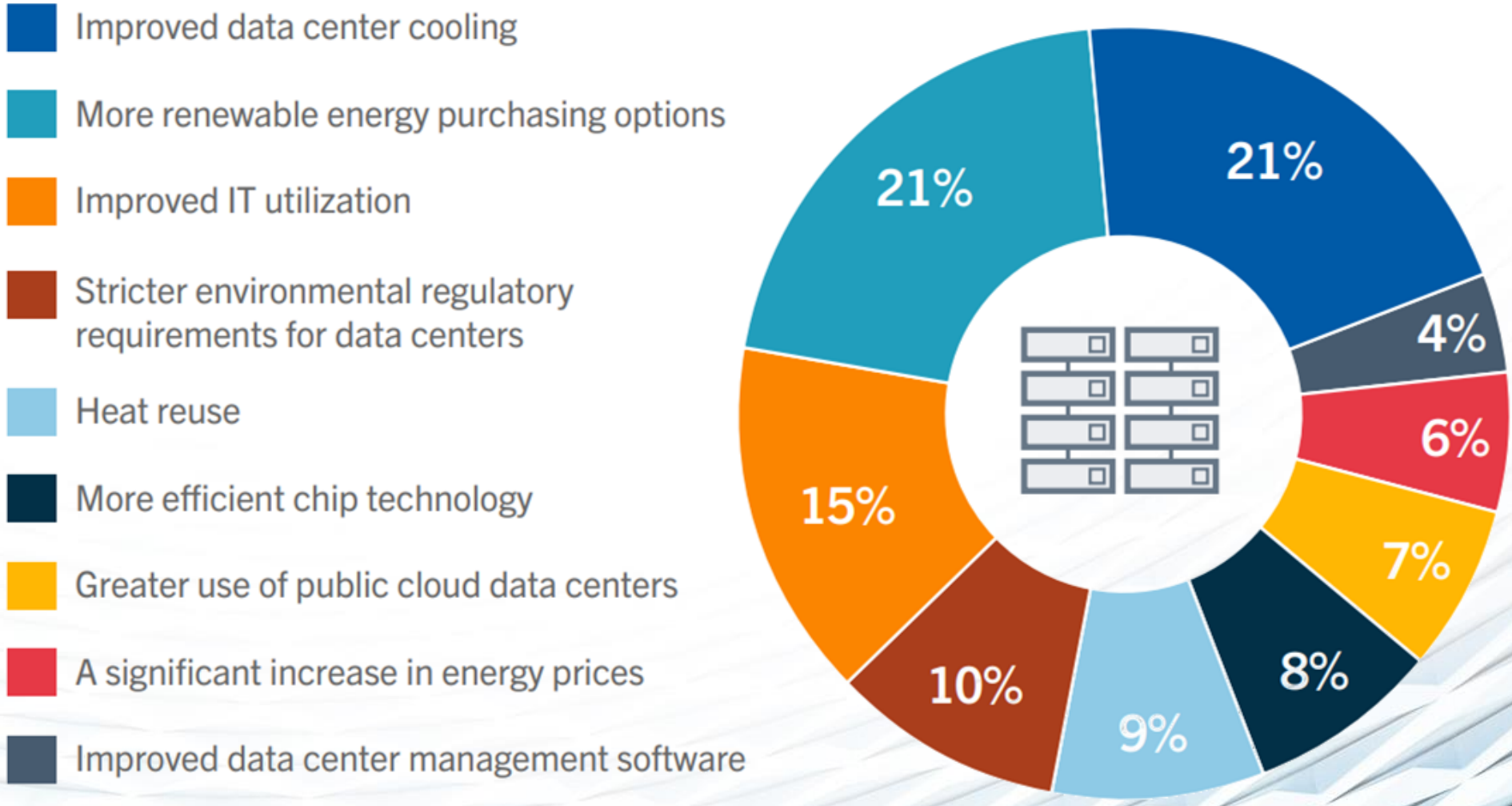
основные преимущества инициатив в области sustainability? Выберите не более двух вариантов



(Only the top 5 response categories are shown in the chart.)

uptime INSTITUTE

Что вы считаете основным драйвером «устойчивого развития» отрасли ЦОД в ближайшие 3-5 лет?



uptime INSTITUTE

Что вы считаете вашими основными вызовами в «устойчивом развитии» ваших ЦОД в ближайшие 3-5 лет? Выберите не более двух

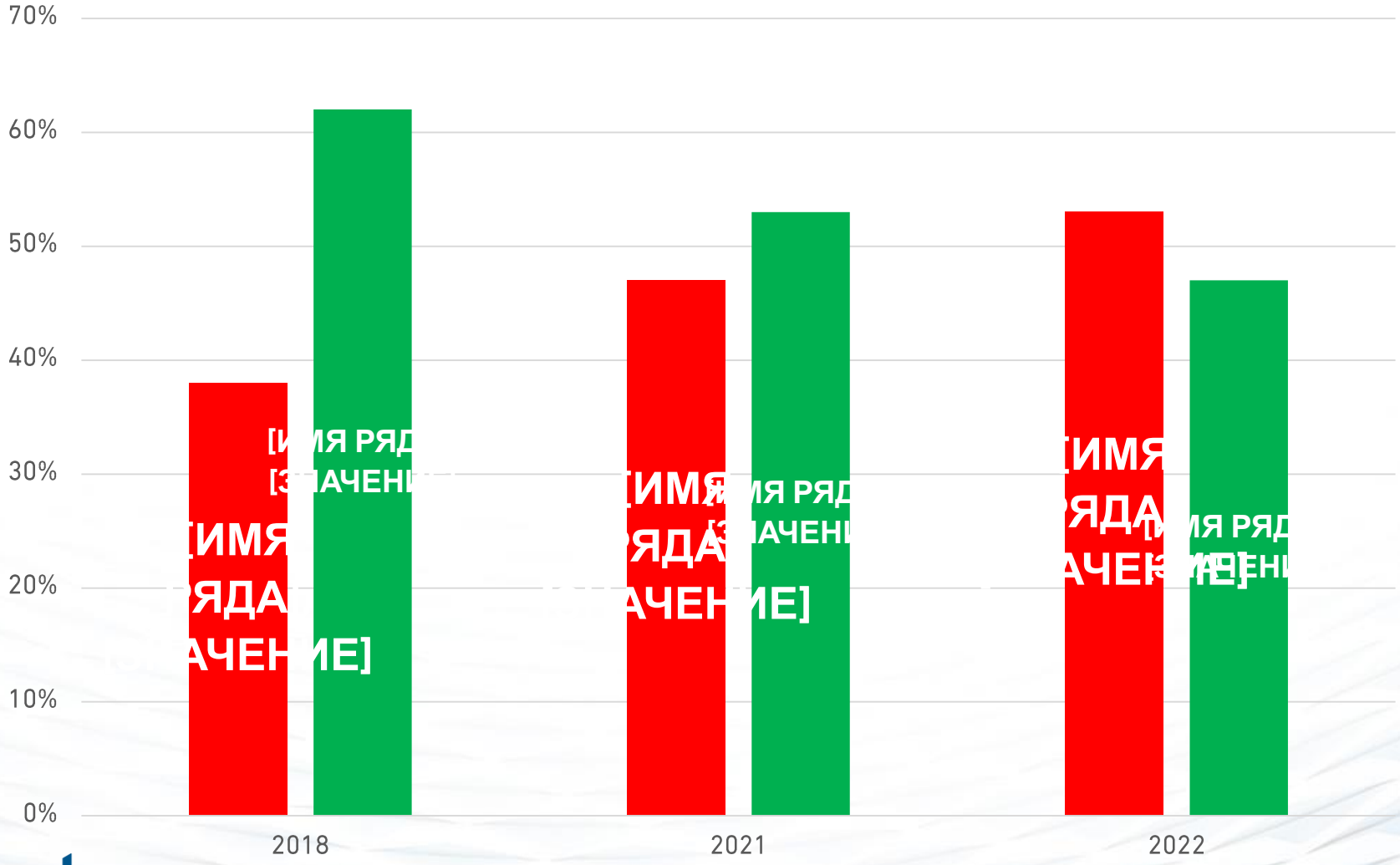
uptime INSTITUTE

Персонал ЦОД

- Нахождение специалистов и их привлечение в службу эксплуатации ЦОД – одна из ключевых задач отрасли по всему миру
- Проблема усугубляется возрастом специалистов. Скоро они массово будут выходить на пенсию, унося с собой не переданные достаточному числу преемников знания и опыт
- Перекупка кадров стала как частой практикой, так и большой проблемой
- Недостаток кадров и переработки ведут к недостаточности обучения и тренировок и далее – к снижению профессиональных навыков и росту рисков отказов в ЦОД

uptime INSTITUTE

при найме персонала в службу эксплуатации?



Привлечение и удержание специалистов – огромная проблема по всему миру

Проблема имеет нарастающий характер и усугубляется старением участников отрасли, что влечет потерю знаний и навыков

uptime INSTITUTE

Приходится ли вам испытывать трудности, связанные с перекупкой сотрудников службы эксплуатации?

Перекупка сотрудников стала как распространенным способом привлечения кадров, так и большой проблемой для их удержания

Имеет краткосрочный эффект, повышая уровень оплаты труда и затрат на привлечение и содержание персонала

uptime INSTITUTE

Недостаток специалистов пагубно отражается на работе ЦОД, самих специалистах и отрасли в целом

Недостаток кадров на рынке и опережение ростом отрасли притока новых кадров негативно сказывается на работе отрасли

Недостаток специалистов в ЦОД влечет вынужденные переработки, отложенное техническое обслуживание и нехватку рабочего времени для обучения и повышения квалификации сотрудников

Передача и распространение наборов навыков становится все менее достаточным

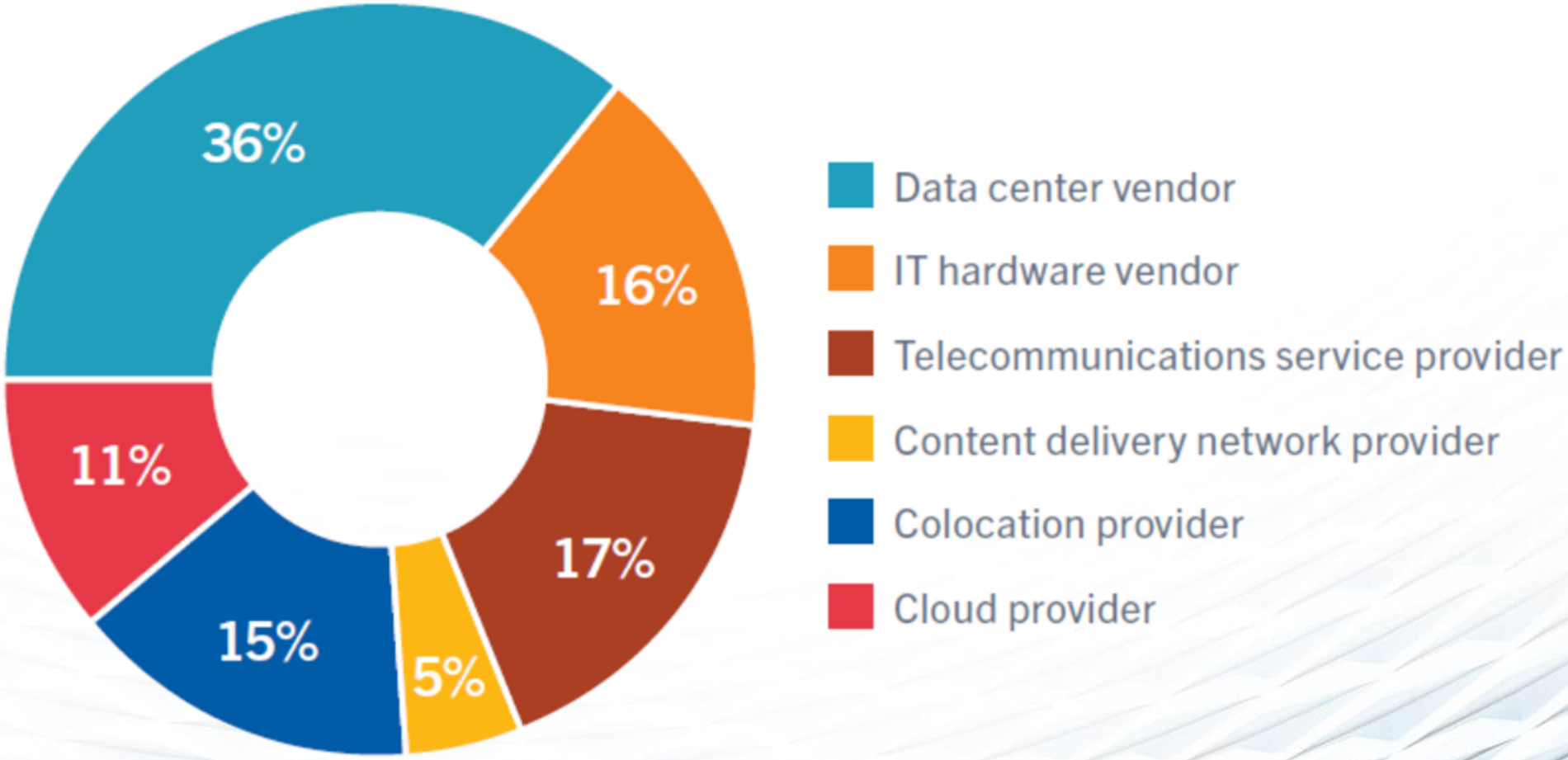
Недостаток профессиональных навыков и опыта у специалистов ставит под угрозу как эксплуатацию самого ЦОД, так и предоставляемые им сервисы

uptime INSTITUTE

Edge-ЦОДы

- В качестве поставщика **Edge**-ЦОДа **36%** видят производителя ЦОДов, а каждый шестой – телеком-провайдера, ИТ-производителя или колокейшн
- **2** из **5 Edge**-ЦОДов принадлежат самой компании, в то время как каждый шестой предоставляется коло- / клауд-провайдером. Их доля удвоится через два года. Каждая пятая организация использует смешанную модель
- Основными драйверами **Edge**-ЦОДов станут требования к пропускной способности и сокращению задержек и приложения **IoT** и **AI**
- Основным уровнем резервирования останется **N+1**, а большинство **Edge**-ЦОДов будут использовать ДГУ, батареи и солнечные панели для

Какой тип организации вы рассматриваете как основного поставщика Edge?

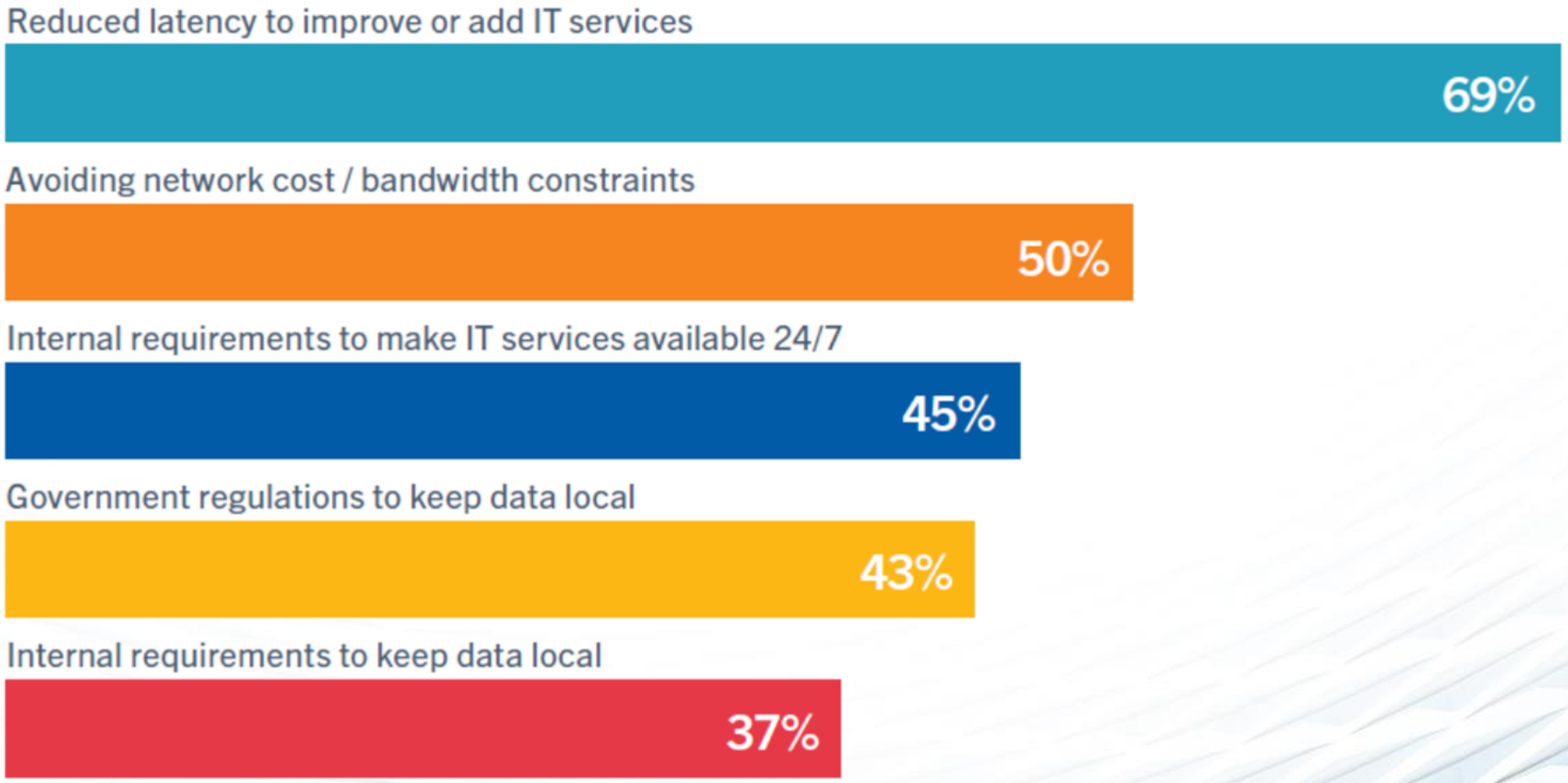


uptime INSTITUTE

Какие Edge-ЦОДы вы используете сегодня и как это изменится через 2-3 года?

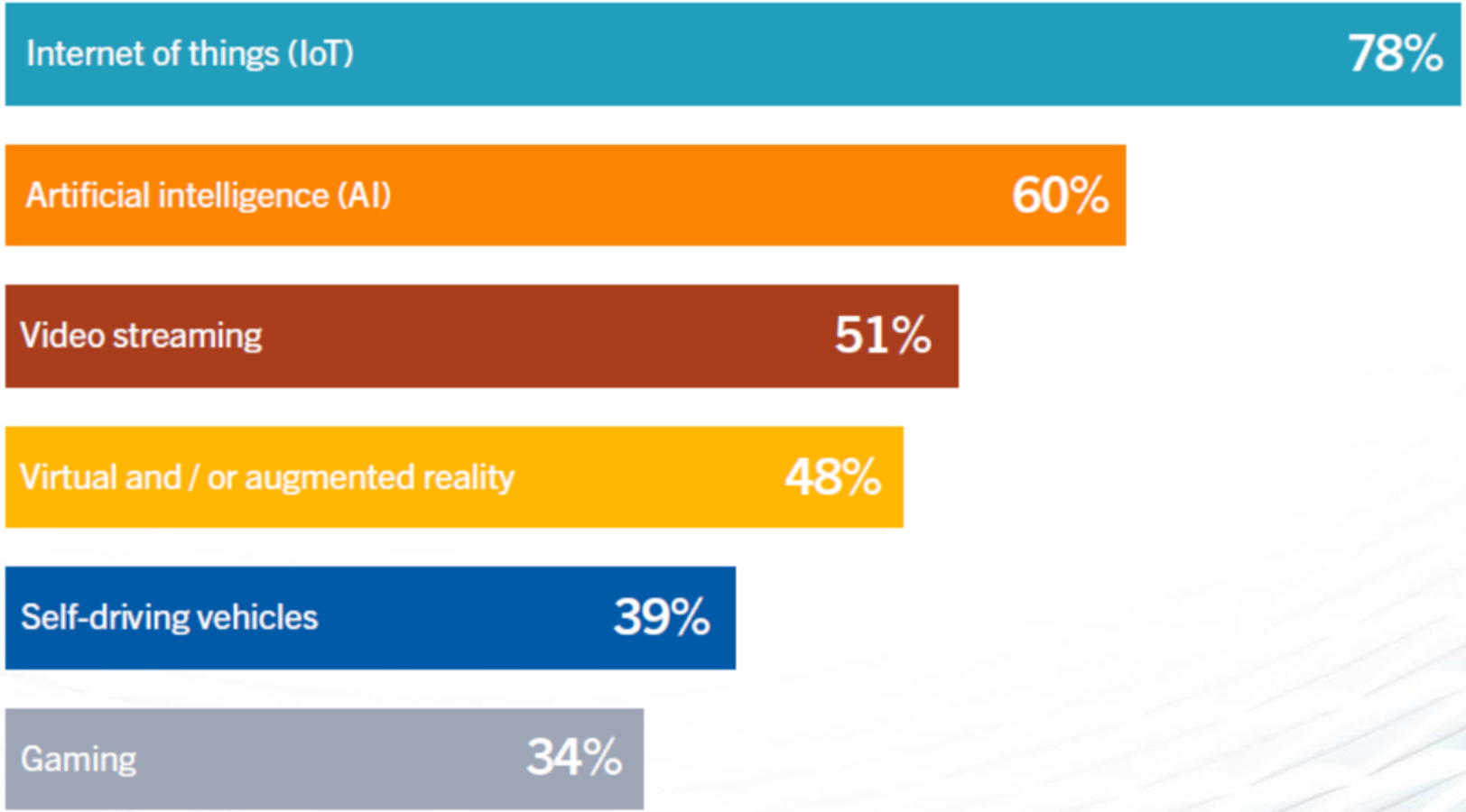
uptime INSTITUTE

Какие требования будут драйверами использования Edge в ближайшие 2-3 года?



uptime INSTITUTE

Какие приложения будут драйверами использования Edge в ближайшие 2-3 года?

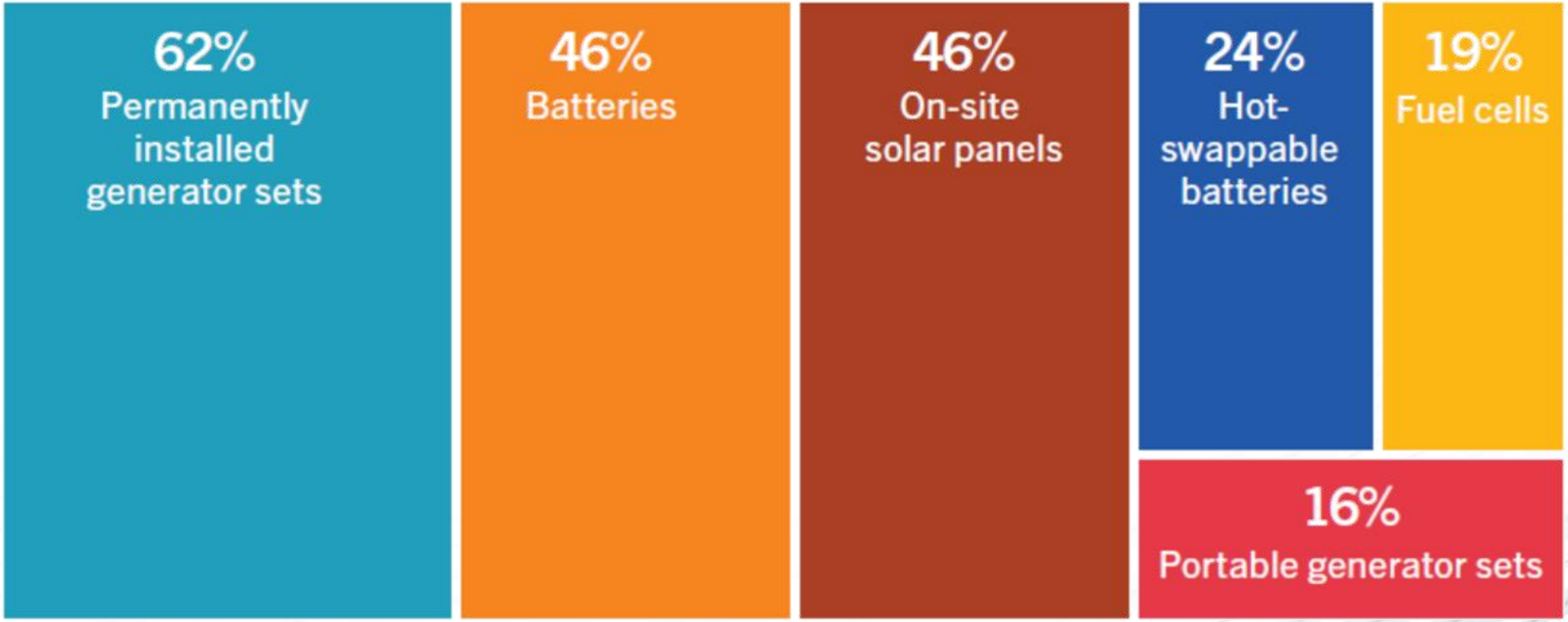


uptime INSTITUTE

Какой уровень резервирования будет типичен для Edge-ЦОДа в ближайшие 2-3 года?

uptime INSTITUTE

Какие источники электроэнергии (помимо электрических сетей) будут типичны для Edge-ЦОДа в ближайшие 2-3 года?



Модели развертывания Edge-ЦОДов

Market activity
Significant
Some
Limited

Edge deployment models

	Provider	Facility	Servers / IT	Networks	
Metro/City	Cloud*	Leased from colo/other (below)	Bare metal, XaaS	Local fiber (telco), cloud on-ramps	
	Colo	MW-scale, staffed, Tier III or higher	Leased (incl. Bare metal) or provided by client	Access to many telco networks, service interconnection, etc.	
Far edge (Near premises)	Cloud	Leased from colo/telco (below)	XaaS (limited offering)	4G/5G, local telco, cloud on-ramps	
	Colo/ Telco	Tens to a few hundred kW, unstaffed, varying redundancy. Single or no engine generator.	Leased (incl. Bare metal) or provided by client	Focus on last mile fiber / 5G incl. local breakout. Network can be part of the service.	
On premises	Cloud (IT)	Provided by enterprise (below)	Cloud extension SW/HW (e.g., AWS Outposts)	Local fiber (telco) and cloud on-ramps	
	Owned	<10 to a few hundred kW. Retrofitted rooms or MDC/ prefab. Owned or leased. Varying redundancy and staff expertise.	Owned or leased (e.g., HPE Greenlake)	Local fiber (telco), 4G/5G, WiFi, Ethernet	
	On-device	N.A.	Embedded + cloud service	4G/5G, WiFi, Ethernet	

uptime INSTITUTE

uptime INSTITUTE

Konstantin Korolev

Director, Business Development

+7 916 642 6603

kkorolev@uptimeinstitute.com

Uptime Institute
405 Lexington Avenue
New York, NY 10174