РОСКОНГРЕСС
Пространство доверия



Безопасность данных

Сравнение подходов к размещению и защите дата-центров

ИИМР
Институт Изучения Мировых Рынков

Ноябрь 2026

- В мире действует около 13 тыс. центров обработки данных. Их число продолжит активно расти по мере развития искусственного интеллекта и цифровых сервисов.

- До недавнего времени подходы к их размещению определялись прежде всего стоимостью электроэнергии, доступностью воды и близостью к сетям связи. Риски физического воздействия оставались на периферии внимания.

- В условиях геополитических конфликтов вычислительные мощности стали целями атак, учитывая, что каждый подобный инцидент наносит ущерб не только оператору дата-центра, но и всем организациям, которые его используют.

- Физическая уязвимость дата-центров повышает спрос на альтернативные варианты их размещения и защиты, включая подземные, подводные и орбитальные.

Подземное размещение

Дата-центры, расположенные под землей, занимают небольшую, но растущую нишу на мировом рынке. Вместо того чтобы создавать новые объекты с нуля, ряд операторов перепрофилирует уже существующие, такие как заброшенные шахты или бункеры. Этот подход развивается, в частности, в США и Северной Европе.

Так, центр обработки данных американской компании Iron Mountain в Западной Пенсильвании расположен на глубине около 67 метров в бывшей известняковой шахте. Он занимает площадь в 30,66 тыс. квадратных метров, обладает мощностью 15,5 МВт и геотермальной системой охлаждения, использующей подземный резервуар площадью 404,7 тыс. квадратных метров. Еще один подземный дата-центр компании площадью 4,6 тыс. квадратных метров расположен вблизи Канзас-Сити, штат Миссури, на глубине 33,5 метра. А компания Bluebird Fiber использует для размещения своего дата-центра известняковую пещеру в Спрингфилде, штат Миссури, на глубине около 26 метров.

Data Journey разместила центр обработки данных площадью более 3,7 тыс. квадратных метров в подземном бункере в Техасе, который изначально был построен как противорадиационное укрытие.

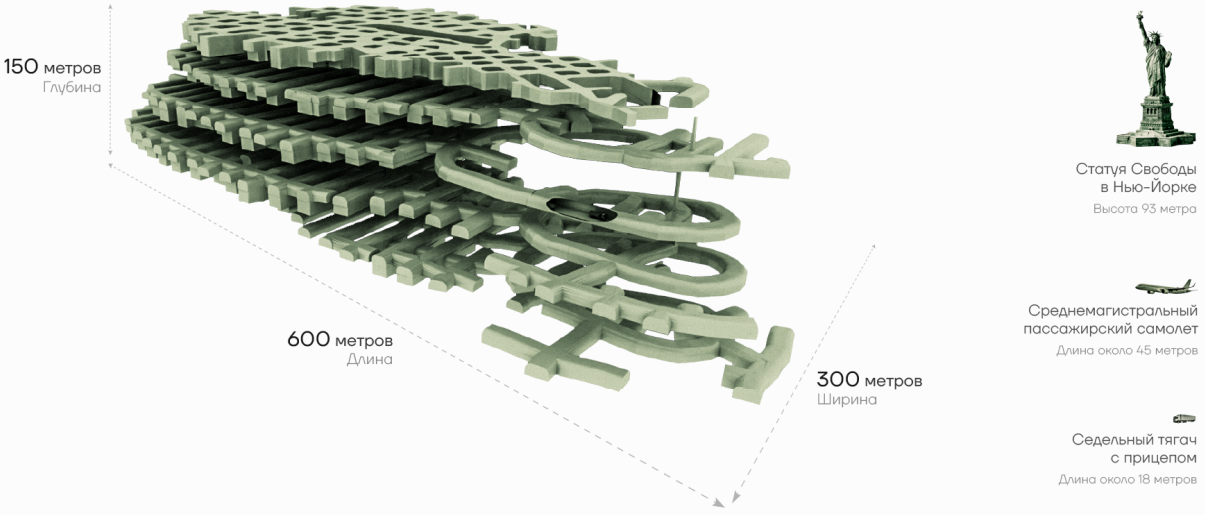
Шведский интернет-провайдер Bahnhof разместил вычислительные мощности на объекте Pionen — в бывшем бункере, построенном в 1940-х годах на глубине около 30 метров под Стокгольмом. Толстые гранитные стены не только обеспечивают безопасность оборудования, но и поддерживают стабильный температурный режим.

Компания Green Mountain в 2013 году переоборудовала под центр обработки данных бывшее хранилище боеприпасов НАТО в Реннесёе (Норвегия). Объект был спроектирован так, чтобы выдерживать ядерные удары и стихийные бедствия. Его основная часть включает шесть горных залов, в каждом из которых размещены двухэтажные бетонные сооружения, возведенные непосредственно внутри горы. Общая доступная площадь составляет около 23 тыс. квадратных метров. Расположение рядом с фьордом позволяет использовать естественное охлаждение, а для энергоснабжения применяется гидроэлектроэнергия.

Норвежская Lefdal Mine Data Centers переоборудовала старую шахту на западном побережье страны в подземный «город дата-центров». Он расположен на шести уровнях, разделенных на 75 залов, с потенциальной площадью свободного пространства до 120 тыс. квадратных метров. На каждом уровне есть центральная подъездная дорога — так называемая «авеню». Она обеспечивает прямой доступ к «улицам» — свободным помещениям на каждом уровне, глубина которых различается, но в среднем составляет 100 метров. Каждую «улицу» можно рассматривать как независимый центр обработки данных, использующий общую с другими центрами систему энергоснабжения и охлаждения. Комплекс работает практически полностью на возобновляемой гидроэлектроэнергии. Для охлаждения используются естественная температура горных пород и вода близлежащего фьорда.

Подземный дата-центр Lefdal Mine

Масштаб дата-центра в сравнении с другими объектами



Источник: Lefdal Mine Data Centers

Высокая степень защиты и пассивное охлаждение, которое позволяет сократить затраты на электроэнергию, составляют главные преимущества подземных ЦОДов. Поскольку земля обеспечивает изоляцию и более низкие температуры на глубине, подземные объекты работают в более стабильных и предсказуемых температурных условиях. Это предполагает защиту как от физических атак, так и от климатических угроз, включая аномальную жару, лесные пожары, ураганы, наводнения и т. д. Использование геотермальной энергии позволяет обеспечить дата-центр электричеством непосредственно на месте, снижая зависимость от внешней энергосети. Особенно привлекательным подземное размещение может быть в регионах с ограниченными земельными ресурсами, таких как Сингапур.

Однако строительство совершенно нового подземного ЦОДа требует намного более масштабных инвестиций, чем возведение наземного объекта. Инженерные работы, выемка грунта и борьба с грунтовыми водами обходятся очень дорого и занимают гораздо больше времени по сравнению с возведением помещения на поверхности земли. Этот подход также требует стабильных геологических условий, как, например, в странах Северной Европы. Объекты, расположенные вблизи геологических разломов или источников воды, могут быть связаны с повышенными рисками землетрясений или проникновения воды.

Размещение ЦОДов в уже существующих подземных объектах сокращает первоначальные инвестиции и сроки введения в эксплуатацию, но все еще требует значительных операционных расходов. Логистика в подземных условиях нуждается в более сложном планировании. Особенность, которая обеспечивает безопасность — скрытность размещения и ограниченность доступа, — существенно усложняет транспортировку тяжелого оборудования и персонала через протяженные туннели или узкие шахты лифтов, монтаж и ремонт техники, а также аварийную эвакуацию. Прокладка оптоволоконных кабелей под землей может оказаться более сложной и дорогостоящей задачей, чем их размещение в траншеях на поверхности.

Хотя подземные сооружения требуют меньше энергии для охлаждения по сравнению с наземными объектами, они, как правило, потребляют больше энергии для поддержания надлежащего качества воздуха и уровня влажности. Для обеспечения их непрерывной работы необходимы сложные и дорогостоящие системы вентиляции, контроля влажности и передовые средства мониторинга. Все это приводит к росту финансовых и временных затрат на техническое обслуживание.

Кроме того, при перепрофилировании шахт или бункеров возможности масштабирования дата-центров меньше, чем при традиционном строительстве с нуля. Операторы физически ограничены существующей конфигурацией

горных пород, что не позволяет легко надстроить дополнительные уровни для удовлетворения растущих потребностей в обрабатывающих мощностях. Расширение подземного ЦОДа может потребовать масштабных буровых и взрывных работ, что создает риск сейсмической активности или обрушения. Наземные же объекты зачастую можно расширять или дополнять модульными блоками гораздо быстрее.

Особенности подземного размещения дата-центров

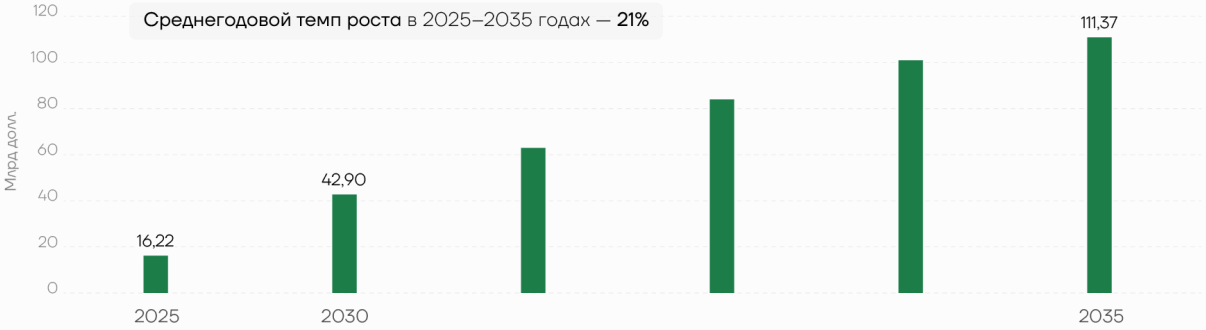
Параметры	**Закапывание дата-центров** (строительство новых подземных объектов)	**Размещение в существующих подземных объектах**
Технологическая сложность		
	Очень высокая. Требуются проектирование с нуля, инженерные изыскания, проходка, гидроизоляция и создание всей инфраструктуры.	**Средняя–высокая**. Основные сложности связаны с адаптацией старых объектов под нужды оператора и современные требования.
Экономическая эффективность		
Капитальные затраты	**Очень высокие**. Необходимы затраты на проектирование, земляные и горнопроходческие работы, инженерные системы, энергетику, связь и безопасность.	**Средние–высокие**. Расходы в целом ниже, но могут потребоваться значительные вложения в модернизацию инфраструктуры.
Операционные расходы	**Средние–высокие**. Ниже затраты на охлаждение, но выше расходы на вентиляцию, водоотведение и обслуживание.	
Функциональная эффективность по различным критериям		
Доступ к энергии	**Средний–высокий**. Энергоснабжение можно проектировать под потребности объекта, но требуется строительство линий, подстанций и резервных источников.	**Средний.** Зависит от расположения объекта; старые объекты могут иметь устаревшую энергетическую инфраструктуру.
Охлаждение	**Очень хорошее**. Подземная среда обеспечивает стабильную температуру и снижает нагрузку на системы охлаждения.	
Ремонт и эксплуатация	**Средняя сложность**. Объект проектируется под обслуживание, но доступ ограничен, а аварийные работы могут быть длительными.	**Средняя–высокая сложность**. Старые объекты могут иметь узкие проходы, ограниченную грузоподъемность, плохую вентиляцию и сложности с доставкой оборудования.
Возможности масштабирования	**Средние**. Масштабирование возможно, но требует дополнительных горнопроходческих или строительных работ.	**Ограниченные**. Масштабирование зависит от свободных площадей, состояния объекта и возможности расширения без нарушения его целостности.
Степень защищенности		
От физических угроз	**Очень высокая**. Подземное размещение затрудняет физический доступ, снижает уязвимость к ударам, обстрелам и диверсиям.	
От климатических угроз	**Высокая**. Подземные объекты защищены от большинства погодных явлений, но уязвимы к затоплениям, землетрясениям и повышению грунтовых вод.	**Средняя–высокая**. Защита зависит от состояния объекта; старые шахты особенно уязвимы к затоплению и влажности.
Когда подход предпочтителен		
	· При **стабильных геологических** условиях. · В условиях **повышенной физической угрозы**. · Для обработки **критически важных данных**. · Для **крупных долгосрочных** проектов.	· При наличии **готовых подземных объектов**. · В условиях **повышенной физической угрозы**. · Для обработки **критически важных данных**.

Модульные и контейнерные решения

Такие дата-центры составляют более быструю и гибкую альтернативу традиционным ЦОДам. Это заранее спроектированная инфраструктура, размещенная в стандартном транспортном контейнере размером около 3, 6 или 12 метров, которую можно развернуть там, где она необходима, а затем расширять по мере изменения потребностей.

По данным The Business Research Company, объем мирового рынка контейнерных дата-центров в 2025 году составил почти $16,22 млрд, продемонстрировав среднегодовой темп роста (CAGR) на уровне 22,7% в период с 2020 года. Ожидается, что показатель увеличится до $42,9 млрд в 2030 году, а к 2035 году достигнет $111,37 млрд.

Прогнозируемый рост рынка контейнерных ЦОД



Источник: The Business Research Company

Мировой рынок контейнерных центров обработки данных довольно фрагментирован, на нем работает большое количество игроков, включая американские Google, Microsoft, IBM, Hewlett Packard Enterprise и Dell Technologies, китайскую Huawei Technologies, тайваньскую Delta Electronics, южнокорейскую LG, немецкую Rittal, ирландскую Eaton и т. д.

Компании предлагают различные решения:

- **стандартный контейнерный дата-центр** — готовый блок в стандартной комплектации, который можно развернуть в кратчайшие сроки, но возможности его адаптации ограничены заранее предусмотренными вариантами;
- **модульное решение по индивидуальному заказу** — этот вариант дает больше гибкости для удовлетворения потребностей конкретного заказчика — специальных сертификатов, интеграции с существующим оборудованием, строгих нормативных ограничений, но кастомизация стоит дороже и требует больше времени для внедрения.

Если на создание традиционных центров обработки данных может уйти от 12 до 24 месяцев, то модульные зачастую можно поставить и ввести в эксплуатацию за 12–20 недель — в зависимости от сложности проекта.

Контейнер поставляется в полной комплектации: системы электроснабжения и кондиционирования, серверные стойки, кабельная инфраструктура, средства пожарной безопасности. Поскольку основные инженерные системы уже содержатся внутри модуля, оператору остается подготовить площадку и обеспечить электропитание и сетевое подключение.

Специфика таких дата-центров позволяет легко масштабировать их. Оператор может заказать дополнительный контейнер и разместить его рядом с имеющимся, наращивая количество стоек, мощность и охлаждение именно тогда, когда это потребуется, без необходимости сложного планирования. С этим же связано удобство ремонта и замены модулей. Кроме того, контейнерные ЦОД мобильны, их можно перевезти на другую площадку, что эффективно для разовых проектов, временных производственных площадок и создания резервной инфраструктуры.

Особенности модульных и контейнерных решений

Параметры	Стандартизированные решения	Кастомизированные решения
Технологическая сложность		
	Низкая–средняя. Используются серийные, заранее спроектированные модули с проверенными инженерными решениями.	**Средняя**. Требуется индивидуальное проектирование, адаптация к специфическим потребностям компании.
Экономическая эффективность		
Капитальные затраты	**Низкие–средние**. Ниже стоимость проектирования, производства и монтажа за счет серийности и унификации.	**Средние**. Затраты выше из-за индивидуального проектирования и меньшего эффекта масштаба.
Операционные расходы	**Средние**. Предсказуемые расходы на обслуживание благодаря типовым компонентам и доступности запчастей.	**Средние–высокие**. Расходы могут быть выше из-за уникальных компонентов, более сложного обслуживания и зависимости от узкого круга поставщиков.
Функциональная эффективность по различным критериям		
Доступ к энергии	**Средний**. Модули рассчитаны на стандартные схемы подключения, но могут требовать адаптации к местной сети.	**Средний-высокий**. Энергосистема может быть спроектирована под конкретный источник: АЭС, ГЭС, газовую генерацию, ВИЭ или гибридную схему.
Охлаждение	**Среднее**. Используются типовые системы охлаждения; эффективность зависит от климата.	**Среднее-хорошее**. Охлаждение можно оптимизировать под климат, плотность размещения оборудования и конкретные вычислительные задачи.
Ремонт и эксплуатация	**Высокая** степень удобства. Стандартизированные компоненты легко заменяются.	**Средняя–высокая** сложность. Ремонт может быть несколько дольше и дороже.
Возможности масштабирования	**Очень высокие**. Мощности наращиваются путем добавления однотипных модулей.	
Степень защищенности		
От физических угроз	**Средняя**. Стандартные контейнеры обеспечивают базовую защиту, но не рассчитаны на высокие угрозы без дополнительных мер.	**Средняя-высокая**. Возможна интеграция усиленных корпусов, систем контроля доступа, защиты от БПЛА и специализированных систем безопасности.
От климатических угроз	**Средняя**. Стандартные решения подходят для умеренного климата, но могут требовать доработки в суровых климатических условиях.	
Когда подход предпочтителен		
	· **При быстром росте бизнеса** и потребностей в вычислительных мощностях. · При **ограниченных финансовых ресурсах**. · Для **временных/пилотных проектов**, **для расширения** существующих дата-центров, **для создания резервной инфраструктуры**. · Для работы на удаленных площадках **без развитой инфраструктуры**. · Для **периферийных вычислений** (edge computing): приближение вычислительных мощностей к источнику данных (Интернет вещей, интеллектуальное видеонаблюдение и т. д.).	

Однако для масштабных задач, которые требуют тысяч стоек, традиционный формат дата-центров остается более удобным вариантом. Использование большого

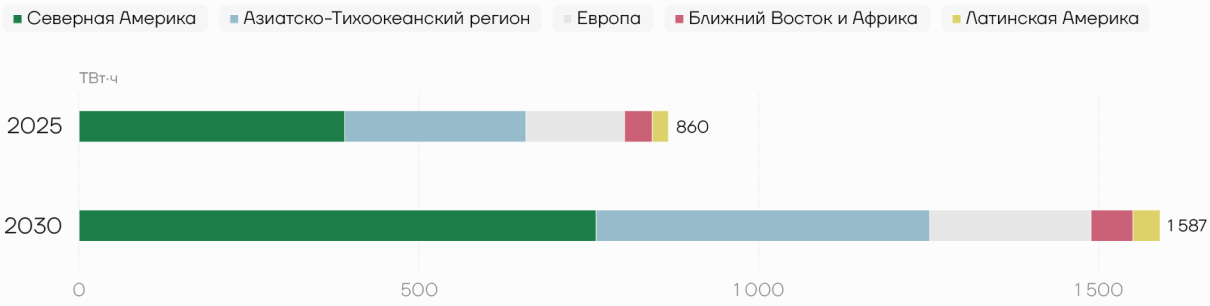
количества контейнеров влечет за собой сложности, связанные с их объединением в цельную систему и обеспечением согласованной работы. Контейнеры также дают ограниченную защиту: они уязвимы как к атакам, так и к неблагоприятным погодным явлениям.

Размещение вблизи источников энергии

Центры обработки данных становятся одним из самых быстрорастущих источников потребления электричества. Согласно консервативному прогнозу подразделения S&P Global Market Intelligence 451 Research, мировой спрос на электроэнергию со стороны дата-центров увеличится почти вдвое — с 860 ТВт·ч в 2025 году до 1587 ТВт·ч к 2030 году.

Глобальный спрос на электроэнергию со стороны дата-центров

Консервативный прогноз



Источник: S&P Global Market Intelligence 451 Research

Стремительный рост потребления опережает развитие сетевой инфраструктуры. Как отмечал Институт изучения мировых рынков (ИИМР), недостаток пропускной способности электросетей становится критическим узким местом энергосистем во многих регионах. Очереди на подключение к электросетям достигли рекордных уровней по всему миру (подробнее об этом — в обзоре «Погоня за гигаваттами. Наращивание генерации как ключ к экономическому росту»). В этих условиях близость вычислительных мощностей к источнику генерации становится конкурентным преимуществом.

В докладе, опубликованном Министерством энергетики США, отмечается, что атомные электростанции, работающие непрерывно и практически не зависящие от погодных условий, представляют собой технически жизнеспособный вариант стабильного энергоснабжения ЦОДов с низким уровнем выбросов углерода.

В исследовании представлены различные подходы к сопряжению центров обработки данных с атомными энергообъектами — от традиционных схем до более интегрированных моделей:

- **подключение через сеть**: АЭС подает электроэнергию в общую энергосеть, к которой подсоединен ЦОД, без прямой связи между этими двумя объектами;
- **подключение за счетчиком** (behind the meter, BTM): объект конечного потребителя подключается к АЭС до точки, в которой сама станция подсоединяется к общей энергосети и в которой производится учет вырабатываемой ею электроэнергии, предназначенной для подачи в сеть общего пользования; это позволяет АЭС продавать электроэнергию для ЦОД напрямую;
- **прямое подключение**: АЭС и ЦОД соединены напрямую, без существенного подключения к энергосети, хотя такое подключение может потребоваться в качестве резервного источника питания на случай чрезвычайных ситуаций.

Схема вариантов сопряжения атомной электростанции с дата-центром



Примечание: градирня — специализированное инженерное сооружение, предназначенное для охлаждения большого количества воды.

Источник: Stauff, Nicolas E., Zhou, Jia, Mann, W. Neal, Sehloff, David, Cho, So-Bin, Kim, Taek K., Jenson, William, Hannah, Botros N., Omitaomu, Femi, Miller, Brandon, & Adeniyi, Abiodun (2025). Preliminary Analysis of Nuclear-Powered Data Center Scenarios.

Интеграция АЭС с дата-центрами требует тщательной инженерной проработки. ЦОДы современных гиперскейлеров — крупнейших операторов вычислительной инфраструктуры — как правило, имеют мощность от 50 до более 300 МВт на кампус, и уже анонсируются проекты кампусов мощностью в несколько гигаватт.

Ядерные объекты включают:

- микрореакторы мощностью до 50 МВт — подходят для небольших или периферийных центров обработки данных;
- малые модульные реакторы (ММР) мощностью 50–600 МВт — оптимальны для средних и крупных кампусов дата-центров;
- большие реакторы мощностью свыше 600 МВт — подходят для региональных хабов ЦОД.

Расположение дата-центров в непосредственной близости от электростанций снижает стоимость энергии и дает ряд эксплуатационных преимуществ. Оно позволяет сократить потери при передаче энергии, повысить надежность системы и снизить затраты, связанные с перегрузкой сети.

Несмотря на потенциальные преимущества, существует ряд препятствий для широкого внедрения этого подхода. Атомные проекты, как правило, сопряжены с высокими первоначальными капитальными затратами, жесткими регуляторными требованиями и длительными сроками строительства, что может сдерживать быстрое развертывание центров обработки данных. Возможность размещения вычислительных мощностей рядом с АЭС во многом зависит от наличия подходящих площадок. Они должны одновременно соответствовать критериям, действующим для обоих типов инфраструктуры, таким как стабильные геологические условия, достаточная площадь территории и доступ к воде для охлаждения. Дополнительные требования включают наличие оптоволоконных сетей. Количество таких площадок ограничено, и за них идет конкурентная борьба.

Перепрофилирование инфраструктуры, например, бывших угольных электростанций, может обеспечить экономические и логистические преимущества, позволяя сократить расходы на строительство и сроки его реализации. Выводимые из эксплуатации угольные электростанции подходят для размещения малых модульных реакторов, и на этих же площадках можно разместить ЦОД, поскольку там уже имеются необходимые подключения к электросетям и доступ к источникам водоснабжения.

Операторы также рассматривают возможность размещения дата-центров возле объектов газовой генерации. Близость к таким электростанциям снижает зависимость от ограниченных мощностей энергосети и повышает надежность электроснабжения. Тем не менее остаются проблемы, связанные с колебаниями цен на газ и углеродным следом.

В регионах, богатых гидроэнергией, центры обработки данных могут размещаться вблизи ГЭС. Это также дает преимущество в виде более низких затрат на электричество, но создает сильную географическую привязку: нельзя построить новую плотину специально под конкретный проект там, где это требуется оператору ЦОД.

Еще один вариант размещения — близость к источникам возобновляемой энергии. Мощности солнечной и ветровой энергетики имеют преимущества в виде относительно низкой стоимости и быстрого развертывания. Однако нестабильный характер ВИЭ-генерации становится главным препятствием для обеспечения устойчивого питания дата-центра. Такие системы требуют либо значительного резервирования мощностей, либо наличия дополнительного источника энергии для стабилизации электроснабжения.

Особенности размещения дата-центров вблизи источников энергии

Параметры	Вблизи АЭС	Вблизи объектов газовой генерации	Вблизи ГЭС	Рядом с объектами солнечной / ветровой энергетики
Технологическая сложность				
	Очень высокая; строгие требования к безопасности, длительные сроки согласования.	**Средняя**.	**Высокая**.	**Средняя–высокая**; требуются накопители, резервные мощности и интеллектуальное управление нагрузкой.
Экономическая эффективность				
Капитальные затраты	**Очень высокие**.	**Средние**.	**Высокие**; зависят от состояния ГЭС, необходимости расширения инфраструктуры.	**Средние–высокие**.
Операционные расходы	**Низкие–средние**. Низкая стоимость электроэнергии, но высокие расходы на безопасность, обслуживание и страхование.	**Средние**; стоимость газа может быть волатильной.	**Низкие** за счет стоимости электроэнергии.	**Средние**.
Функциональная эффективность по различным критериям				
Доступ к энергии	**Очень высокий**. АЭС обеспечивает стабильную базовую нагрузку и предсказуемую генерацию.	**Высокий**. Газовая генерация гибкая и может быстро подстраиваться под нагрузку дата-центра.	**Очень высокий** при стабильной базовой генерации ГЭС.	**Средний**. Солнечная и ветровая генерация зависят от погоды и времени суток.
Охлаждение	**Среднее**. Возможности охлаждения зависят от водных ресурсов и климатических условий.	**Среднее**. Возможности охлаждения зависят от климата и доступности воды.	**Очень хорошее**. Возможность использования воды для охлаждения.	**Среднее**. В солнечных регионах часто жарко и сухо, что увеличивает нагрузку на системы охлаждения.
Ремонт и эксплуатация	**Средняя сложность**. Работы требуют высокой квалификации и строгого соблюдения регламентов безопасности.	**Высокая доступность**.	**Средняя сложность**. Объекты могут быть удаленными, а доступ осложнен рельефом и сезонными ограничениями.	**Средняя–высокая доступность**.
Возможности масштабирования	**Ограниченные**.	**Высокие**.	**Ограниченные**.	**Высокие**.
Степень защищенности				
От физических угроз	**Очень высокая** при наличии охраны, но объект становится критической целью.	**Средняя**. Газовая инфраструктура уязвима к диверсиям, пожарам и атакам на трубопроводы.	**Средняя–высокая**. ГЭС защищены удаленностью, но уязвимы к диверсиям и повреждению плотин.	**Средняя**. ВИЭ-объекты распределены, что снижает риск единой точки отказа, но отдельные элементы уязвимы к атакам.
От климатических угроз	**Высокая**.	**Высокая**.	**Средняя**. ГЭС зависят от засух, паводков, ледовых явлений.	**Низкая–средняя**; генерация зависит от погоды.
Когда подход предпочтителен				
	Для крупных дата-центров с постоянной высокой нагрузкой, где критичны **стабильность и низкая стоимость энергии** в долгосрочном периоде.	**Для быстрого наращивания мощностей**, в регионах с доступным газом.	**Для крупных дата-центров** в регионах **с избытком гидроэнергии**.	**Для распределенных вычислений**, в сочетании с накопителями и резервной генерацией.

Орбитальные дата-центры

ЦОДы требуют не только колоссальных объемов энергии, но и больших земельных участков, они могут занимать площадь в несколько футбольных полей. Это подтолкнуло ряд операторов к идее размещения дата-центров в космосе. Такой подход не только решил бы проблему нехватки свободных площадок, но и открыл более широкий доступ к солнечной энергии, поскольку в космосе нет облачности и внутрисуточных или сезонных колебаний освещения.

Первый коммерческий спутник — дата-центр был запущен в конце 2025 года, а ряд компаний заявили о планах развертывания в общей сложности более миллиона спутников. Очередной шаг в этом направлении был сделан в октябре 2026 года, когда Alphabet вывела на орбиту свои ИИ-чипы на борту ракеты SpaceX Falcon 9.

Китай намерен создать к 2030 году целое «космическое облако». Пекин планирует развернуть сеть из 2800 спутников, обеспечивающих вычислительную инфраструктуру для ИИ, на орбитах высотой от 500 до 1000 километров. Вопрос заключается уже не в том, можно ли разместить дата-центры в космосе, а в том, возможно ли обеспечить их развертывание в таких масштабах, по такой стоимости и таким уровнем надежности, которые необходимы для широкого внедрения.

Запуск является одним из основных факторов, влияющих на стоимость космических ЦОДов. При нынешних затратах, составляющих примерно $1,5 тыс. за килограмм, для вывода на орбиту 1 ГВт вычислительной мощности потребуется около $30 млрд, что делает крупномасштабное развертывание экономически нецелесообразным. Однако, по оценкам Boston Consulting Group (BCG), стоимость запуска значительно снизится, возможно, до $100 за килограмм, благодаря полностью многоразовым системам запуска большой грузоподъемности, таким как Starship от SpaceX. Расширение инфраструктуры запусков должно еще больше увеличить частоту полетов, что даст экономию за счет масштаба.

В то время как эффективность запусков приближается к уровню, необходимому для полноценной эксплуатации, вопросы охлаждения и технического обслуживания на орбите остаются основными узкими местами. Поэтому для полноценной реализации концепции необходим ряд серьезных технологических прорывов.

Наземные центры обработки данных используют как воздушное, так и жидкостное охлаждение серверов. В таких системах тепло передается от микросхем к жидкому

хладагенту, а затем — в окружающую атмосферу. Для дата-центра, расположенного в космическом вакууме, подобный подход неприменим, поскольку там отсутствует атмосфера, способная поглощать тепло. Единственным способом отвода тепла от орбитального дата-центра может быть тепловое излучение. Однако, согласно расчетам некоторых ученых, для эффективного рассеивания тепла от одного такого объекта потребовались бы радиаторы общей площадью 2,15 млн квадратных футов (199,7 тыс. квадратных метров).

Из-за отсутствия атмосферы объекты в космосе подвергаются воздействию гораздо более высоких доз солнечного ультрафиолетового излучения. Уровень радиации на низкой околоземной орбите примерно в 20–30 раз выше, чем на поверхности Земли, из-за чего незащищенная электроника может выйти из строя всего за 30–50 дней. Применение микросхем космического класса, а также направленного экранирования из многослойных материалов позволяет продлить срок службы оборудования, но увеличивает стоимость проекта.

Объекты в космосе также уязвимы для ракет, средств создания помех, кибератак и оружия направленной энергии, а их защита будет весьма дорогостоящей. Существует риск вспышек на Солнце и других факторов, способных нарушить работу оборудования, а также столкновений на орбите.

Современные спутники обычно эксплуатируются от пяти до семи лет, после чего их сводят с орбиты. Такая модель — замена вместо ремонта — приводит к росту как эксплуатационных расходов, так и объема космического мусора. Использование роботизированных спутников для технического обслуживания могло бы увеличить срок службы аппаратов в 2–3 раза, а применение более долговечных компонентов — настолько же сократить частоту их замены.

Проблема заключается в том, что масштабного спроса на подобные технологии пока нет, что сдерживает инвестиции. При этом скорость технического прогресса так высока, что запущенный в космос ценой огромных затрат ЦОД может устареть уже через пару лет. Кроме того, передача больших объемов данных обратно на Землю остается сложной задачей. Чем выше орбита, на которой находится объект, тем больше риск проблем со связью и задержек передачи данных.

Наиболее вероятно, что размещение дата-центров в космосе в значительных масштабах станет технически осуществимым не ранее, чем через 5–10 лет. Но даже тогда они вряд ли смогут конкурировать с наземной инфраструктурой по стоимости. При текущих условиях размещение дата-центров на орбите обойдется в 2,5–3 раза дороже традиционных вариантов. Исходя из реалистичных сценариев развития технологий, этот разрыв в стоимости в течение следующего десятилетия

сократится примерно до 1,5 раз, но не исчезнет. Поэтому орбитальные центры обработки данных следует рассматривать не как замену наземной инфраструктуре, а лишь как потенциальное дополнение к ней. По оценкам BCG, спутники к 2040 году смогут занять от 10% до 15% мирового рынка центров обработки данных для нужд искусственного интеллекта.

Особенности размещения дата-центров в космосе

Параметры	**Размещение на орбите**
	Технологическая сложность
	Очень высокая. Требуются устойчивая к радиации электроника, легкие и надежные вычислительные модули, системы энергоснабжения, охлаждения, спутниковой связи, автономного управления.
	Экономическая эффективность
Капитальные затраты	**Очень высокие**. Основные статьи затрат: производство спутников или орбитальных платформ, запуск, радиационная защита, системы связи, резервирование, страхование и наземная инфраструктура управления.
Операционные расходы	**Сравнительно низкие** (затраты на электроэнергию и эксплуатацию практически исключены).
	Функциональная эффективность по различным критериям
Доступ к энергии	**Высокий**. В космосе возможен практически непрерывный доступ к солнечной энергии, особенно на орбитах с минимальным затенением Землей.
Охлаждение	**Сложное** в условиях вакуума, несмотря на низкую температуру космического пространства.
Ремонт и эксплуатация	**Очень сложные**. Обычный ремонт невозможен; замена компонентов требует миссии обслуживания, роботизированных систем или вывода нового аппарата. Время реакции на отказ может составлять месяцы.
Возможности масштабирования	**Ограниченные** в краткосрочной перспективе; требуется запуск дополнительных модулей, расширение орбитальной группировки, увеличение пропускной способности связи и развитие наземной инфраструктуры.
	Степень защищенности
От физических угроз	**Высокая** от наземных физических атак в силу удаленности и труднодоступности объекта, но есть **риски столкновений** с космическим мусором, преднамеренных **атак на спутники** и **перехвата каналов связи**.
От климатических угроз	**Высокая** от земных климатических явлений: ураганов, наводнений, засух, пожаров и экстремальных температур на поверхности. Но существуют **специфические риски**: солнечные вспышки, космическая радиация, метеориты и т. д.
	Когда подход предпочтителен
	· В перспективе **5–10 лет**. · Для **масштабных долгосрочных проектов**. · Для обработки данных в **удаленных регионах**, **наблюдения за Землей**.

Плавучие дата-центры

Потенциальным решением проблем нехватки земли и водных ресурсов для охлаждения служит перенос вычислительных мощностей в моря и океаны. Оборудование может размещаться вблизи прибрежной инфраструктуры, где энергоснабжение, подключение к сетям связи и охлаждение организовать проще. Этот вариант особенно актуален для районов, где ощущается нехватка территории, включая островные государства.

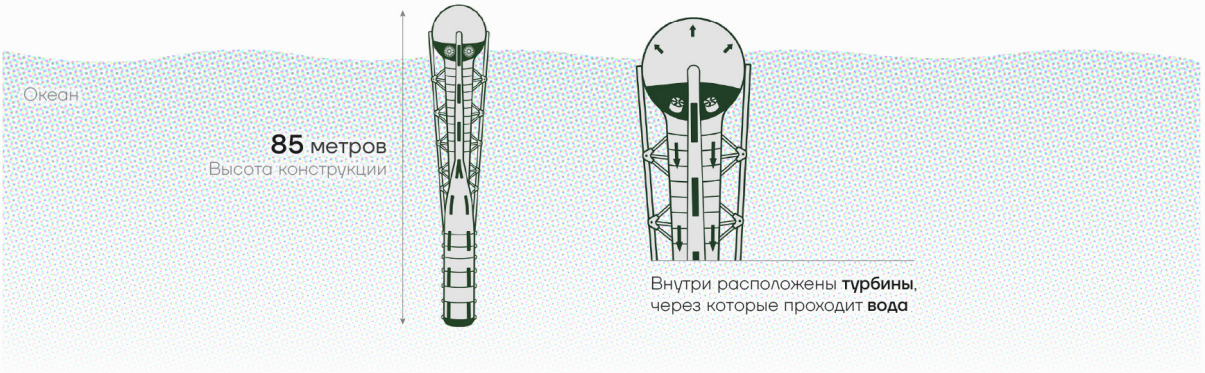
Для индустрии ЦОД работа в водной среде — относительно новое явление. Концепция плавучих дата-центров уже вышла за пределы чисто теоретических

разработок, но большинство проектов пока находятся на стадиях проектирования, утверждения или на демонстрационном этапе.

Препятствия остаются существенными: высокие затраты на морское строительство, экологическая экспертиза, суровые климатические условия и ограниченное количество экономически привлекательных площадок для размещения. Инженерные и эксплуатационные проблемы включают необходимость защиты оборудования от воздействия морской среды, зависимость от подводных кабелей, сложности организации технического обслуживания и стабильного электропитания большой мощности для судна или платформы, которые не вырабатывают энергию самостоятельно.

Американский стартап Panthalassa для решения этих проблем разработал плавучие стальные конструкции высотой 85 метров, большая часть которых находится под поверхностью океана. Они вырабатывают электроэнергию за счет движения волн, которые проталкивают воду через встроенные турбины. Полученная энергия используется для ИИ-чипов, размещенных внутри герметичного модуля, который охлаждается морской водой.

Схема устройства плавучих дата-центров Panthalassa



Источник: Panthalassa

Вместо подключения к наземным телекоммуникационным сетям плавучие ЦОД Panthalassa используют спутниковую связь SpaceX Starlink. В результате создается полностью автономная морская вычислительная платформа.

Особенности размещения ЦОД в море

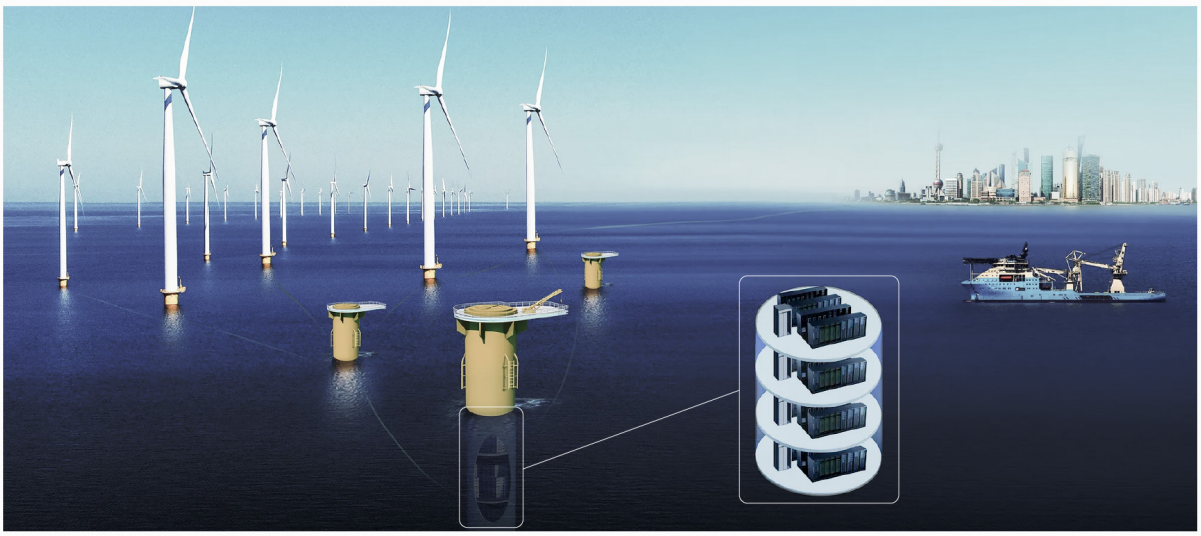
Параметры	Плавучие дата-центры
	Технологическая сложность
	Средняя–высокая. Требуются морская инженерия, герметизация, системы стабилизации, защита от коррозии, надежное электроснабжение и связь.
	Экономическая эффективность
Капитальные затраты	**Высокие**.
Операционные расходы	**Средние–высокие**.
	Функциональная эффективность по различным критериям
Доступ к энергии	**Средний**. Возможна связь с прибрежными сетями, ВИЭ или плавучими электростанциями, но надежность зависит от погоды и морской логистики.
Охлаждение	**Хорошее** за счет доступа к воде.
Ремонт и эксплуатация	**Средняя сложность**. Доступ возможен, но зависит от погоды и морской логистики.
Возможности масштабирования	**Высокие**. Можно добавлять модули и платформы.
	Степень защищенности
От физических угроз	**Средняя**. Платформа уязвима для диверсий, столкновений судов и других угроз.
От климатических угроз	**Средняя**. Уязвимость к штормам, ураганам, волнам, ледовым условиям и повышению уровня моря.
	Когда подход предпочтителен
	Для прибрежных регионов с **дефицитом земли**, рядом с энергетической и сетевой инфраструктурой.

Подводные дата-центры

Еще один вариант использования морей и океанов в качестве масштабного, стабильного и бесплатного источника охлаждения — размещение дата-центров под водой. Задает этот формирующийся тренд главным образом Китай. Хотя Microsoft запустил пилотный проект в акватории Оркнейских островов (Шотландия) еще в 2018 году, впоследствии компания отложила его, поскольку прогресс в этом направлении остановился.

Первый в мире коммерческий подводный дата-центр был запущен в 2023 году китайской HiCloud Technology на Хайнане. А в 2026 году в КНР начал работу первый в мире подводный центр обработки данных на энергии ветра. Проект реализуется совместно компаниями HiCloud Technology и China Communications Construction и имеет мощность 24 МВт. Дата-центр расположен более чем в 10 километрах от побережья Шанхая, на глубине 10 метров, и снабжается энергией от расположенной неподалеку морской ветряной электростанции. По сравнению с традиционными наземными центрами обработки данных он потребляет на 22,8% меньше энергии благодаря естественному охлаждению в морской воде, а также позволяет сократить использования воды и земельных ресурсов — на 100% и более чем на 90% соответственно.

Схема подводного дата-центра у побережья Шанхая, работающего на энергии ветра



Источник: Shanghai Hailanyun Technology

К зонам риска подводных дата-центров относятся инженерные проблемы, такие как необходимость герметизации модулей, коррозионное воздействие морской воды, высокое давление на глубине, а также сложность технического обслуживания, которое может потребовать подъема целых модулей на поверхность.

Особенности размещения ЦОД под водой

Параметры	Подводные дата-центры
	Технологическая сложность
	Очень высокая. Необходимы глубоководные корпуса, защита от давления, коррозии, сложные системы связи и дистанционного обслуживания.
	Экономическая эффективность
Капитальные затраты	**Очень высокие**.
Операционные расходы	**Высокие**. Основные расходы связаны с дистанционной диагностикой, редкими, но сложными ремонтами, морскими операциями и страхованием.
	Функциональная эффективность по различным критериям
Доступ к энергии	**Средний**.
Охлаждение	**Очень хорошее**.
Ремонт и эксплуатация	**Очень сложные**. Ремонт требует подъема модуля, водолазных или роботизированных операций; время восстановления может быть длительным.
Возможности масштабирования	**Ограниченные**. Масштабирование возможно, но требует новых подводных модулей, кабелей и сложной логистики монтажа.
	Степень защищенности
От физических угроз	**Высокая**. Глубина и удаленность затрудняют физический доступ, но объект уязвим к атакам на кабели и подводную инфраструктуру.
От климатических угроз	**Высокая**. Подводная среда защищает от большинства погодных явлений.
	Когда подход предпочтителен
	Для задач с высокими требованиями к **скрытности и защите от наземных угроз**.

В то время как такой тип размещения предполагает высокую защищенность от наземных угроз, источником уязвимости служит зависимость от подводных

кабелей, которые остаются уязвимым местом критически важной информационной инфраструктуры. Большинство повреждений кабелей носит случайный или природный характер, но геополитические конфликты повышают вероятность целенаправленных атак, которые обычно предполагают более дорогостоящий ремонт и значительные последствия.

Дата-центры в регионах с холодным климатом

Еще одним потенциальным решением проблем с доступом к энергии и воде является размещение дата-центров в регионах с холодным климатом. Естественные низкие температуры в таких районах снижают нагрузку на системы охлаждения, сокращая потребление электричества. При этом температура должна оставаться достаточно низкой на протяжении всего времени, вне зависимости от сезона предотвращая перегрев оборудования за счет циркуляции воздуха между помещением и внешней средой.

Подходящие условия можно найти за полярным кругом или вблизи него, но пока объекты в таких районах встречаются нечасто. В Арктике создано около трех десятков центров обработки данных. В Антарктиде, которая сильнее удалена от населенных пунктов и инфраструктуры, крупных центров обработки данных нет, однако там функционируют небольшие ИТ-объекты, обеспечивающие работу местных исследовательских групп.

Примеры размещения дата-центров в регионах с холодным климатом:

- скандинавский оператор **atNorth** управляет центрами обработки данных в Исландии, Норвегии, Дании, Швеции и Финляндии;
- дата-центр **Google** располагается на бывшей бумажной фабрике в Хамине (Финляндия) и использует для охлаждения морскую воду из Финского залива;
- кампус ЦОД **Verne Global** в Исландии мощностью более 140 МВт использует преимущества холодного климата страны и ее возобновляемых источников энергии, включая геотермальную и гидроэнергию.

- дата-центр британской технологической компании **Nscale** расположен в Гломфьорде — небольшом населенном пункте на севере Норвегии, чуть выше Северного полярного круга, где также имеется гидроэлектростанция.

Широкое распространение подобных объектов сдерживается рядом факторов:

- **удаленность от населенных пунктов**: регионы с холодным климатом часто отличаются низкой плотностью населения, что может увеличивать задержки при передаче данных между ЦОДами и пользователями, которые находятся на значительном расстоянии от них;
- **ограниченный доступ к энергетической инфраструктуре**: хотя дата-центры в холодном климате не требуют значительных энергозатрат на охлаждение, им все равно нужно электричество для работы серверов. Однако в таких регионах энергосети, как правило, менее развиты, а точек подключения меньше;
- **ограниченный доступ к сетевой инфраструктуре**;
- **повышенные логистические издержки**: сложности с доступом к дата-центрам дополнительно усугубляются при неблагоприятных погодных условиях, например, при сильных снегопадах. Это затрудняет строительство таких объектов, транспортировку ИТ-оборудования и техническое обслуживание.

Особенности размещения ЦОД в регионах с холодным климатом

Параметры	**Дата-центры в регионах с холодным климатом**
	Технологическая сложность
	Средняя. Требуются адаптация к климатическим условиям, надежная логистика и устойчивая связь.
	Экономическая эффективность
Капитальные затраты	**Средние–высокие**. Затраты на строительство в труднодоступной местности, транспортировку оборудования, дороги, энергетику и связь.
Операционные расходы	**Средние**. Ниже расходы на охлаждение, но выше затраты на логистику, персонал, отопление вспомогательных помещений.
	Функциональная эффективность по различным критериям
Доступ к энергии	**Средний–высокий**. Возможен доступ к гидроэнергетике или ветровой генерации, но инфраструктура может быть ограничена.
Охлаждение	**Очень хорошее**.
Ремонт и эксплуатация	**Средняя сложность.** Доступ возможен, но осложняется удаленностью и погодными условиями.
Возможности масштабирования	**Средние**. Масштабирование возможно при наличии свободных площадей, энергии и транспортной доступности.
	Степень защищенности
От физических угроз	**Средняя–высокая**. Удаленность и сложный рельеф затрудняют доступ, но объект может быть уязвим к диверсиям и атакам на линии электропередачи.
От климатических угроз	**Высокая** при правильном проектировании.
	Когда подход предпочтителен
	Для обработки данных с **умеренными требованиями к низкой задержке**.

Защита дата-центров

Выработка альтернативных подходов к размещению дата-центров не отменяет необходимости их защиты от физических и цифровых угроз. Требования к безопасности могут существенно варьироваться в зависимости от конкретного объекта. Тем не менее существуют общие подходы к защите дата-центров, включая следующие:

- **защита периметра**: интеллектуальные системы видеонаблюдения и наземные радары способны идентифицировать и отслеживать людей, транспортные средства и другие объекты, а интегрированные системы обнаружения вторжений и контроля доступа могут обеспечить усиленную защиту внешних границ;
- **контроль доступа в помещение**: внедрение различных уровней доступа для разных категорий персонала, а также посетителей, системы мониторинга, камеры видеонаблюдения и т. д.;
- **обеспечение безопасности зон повышенного риска и критически важных активов**: многофакторная аутентификация, непрерывное видеонаблюдение, фиксация всех попыток доступа к серверным помещениям, стойкам и хранилищам данных.

Необходимым элементом стратегии безопасности также стала защита от дронов. К пассивным методам защиты относятся:

- **физические средства защиты**: создание физических барьеров (защитных сеток, решетчатых или бетонных ограждений) вокруг критически важных узлов; системы обнаружения, которые активируют меры физической защиты; перемещение уязвимых элементов с открытых участков в защищенные зоны за ограждениями или барьерами;
- **укрытие и маскировка**: физическая маскировка, использование ложных целей, расширение периметра для увеличения просматриваемого изнутри воздушного пространства, сокращение числа мест с беспрепятственным обзором объекта извне;
- **системы резервирования и отказоустойчивости**: создание на территории объекта дублирующих подсистем охлаждения и электроснабжения, резервирование каналов связи для сохранения непрерывности работы; регламенты переключения между объектами, позволяющие быстро переносить рабочие нагрузки в другие центры обработки данных.

Кроме того, существуют активные методы защиты, направленные на идентификацию и нейтрализацию угрозы. Возможности нейтрализации беспилотника в воздушном пространстве ограничиваются регуляторным режимом, действующим на территории объекта.

Применение средств физического воздействия, систем направленной энергии, подавления или подмены сигналов может быть прерогативой исключительно государственных структур. Тем не менее в мире ведутся разработки дронов-перехватчиков для защиты ЦОДов.

К примеру, стартап из Сан-Франциско Impact Drones разрабатывает беспилотники-перехватчики различных моделей, предназначенные для защиты критически важной гражданской инфраструктуры. Самоуправляемые дроны-перехватчики размещаются в специальных контейнерах на территории объекта. Враждебные БПЛА отслеживаются с помощью датчиков, и при обнаружении угрозы производится автоматический запуск перехватчика. Подобная объектовая система защиты не может заменить рубежную, но потенциально может служить дополнением к ней.

Принцип работы дрона-перехватчика Weaver от Impact Drones



Источник: Impact Drones

Затраты на реализацию этих мер относительно низки по сравнению с потенциальными убытками от атаки. Они быстро окупаются при высоком уровне угроз. Наиболее велика потребность в них для критической инфраструктуры, объектов с высокой концентрацией данных, наземных дата-центров в зонах повышенного риска.

Выводы

— По мере строительства новых дата-центров вычислительные мощности в мире будут перераспределяться из геополитически нестабильных областей в регионы, где риск физического воздействия ниже.

— Спрос на подземные дата-центры будет расти благодаря высокой степени защиты от внешних угроз, но ограниченные возможности масштабирования будут сдерживать распространение этого подхода.

— Простота и скорость развертывания делает модульные и контейнерные решения эффективными для большинства задач. Они могут лежать в основе гибридных моделей, позволяя операторам размещать модули под землей, рядом с источниками энергии и дополнять их активной защитой.

— Подводные дата-центры, в отличие от наземных, решают проблемы доступности земли и воды. При этом они обеспечивают лучшее охлаждение и высокую скрытность и не требуют столь сложной инфраструктуры, как орбитальные.

— Однако подводные кабели находятся под угрозой, поэтому отдельным пунктом в стратегии размещения дата-центров будет выяснение топологии сети связи, обеспечивающей обмен информацией.

— Орбитальные вычисления в значительных масштабах станут возможны в 2030-х годах, но останутся нишевым и дорогостоящим направлением.

— Наиболее устойчивой моделью представляется георасределенная инфраструктура вычислительных мощностей в сочетании с развитием активной защиты и резервированием энергоснабжения.