

УКРАИНА

Падение "облаков". Украинские и российские дата-центры под ударами

Евгений Легалов

15 октября 2026



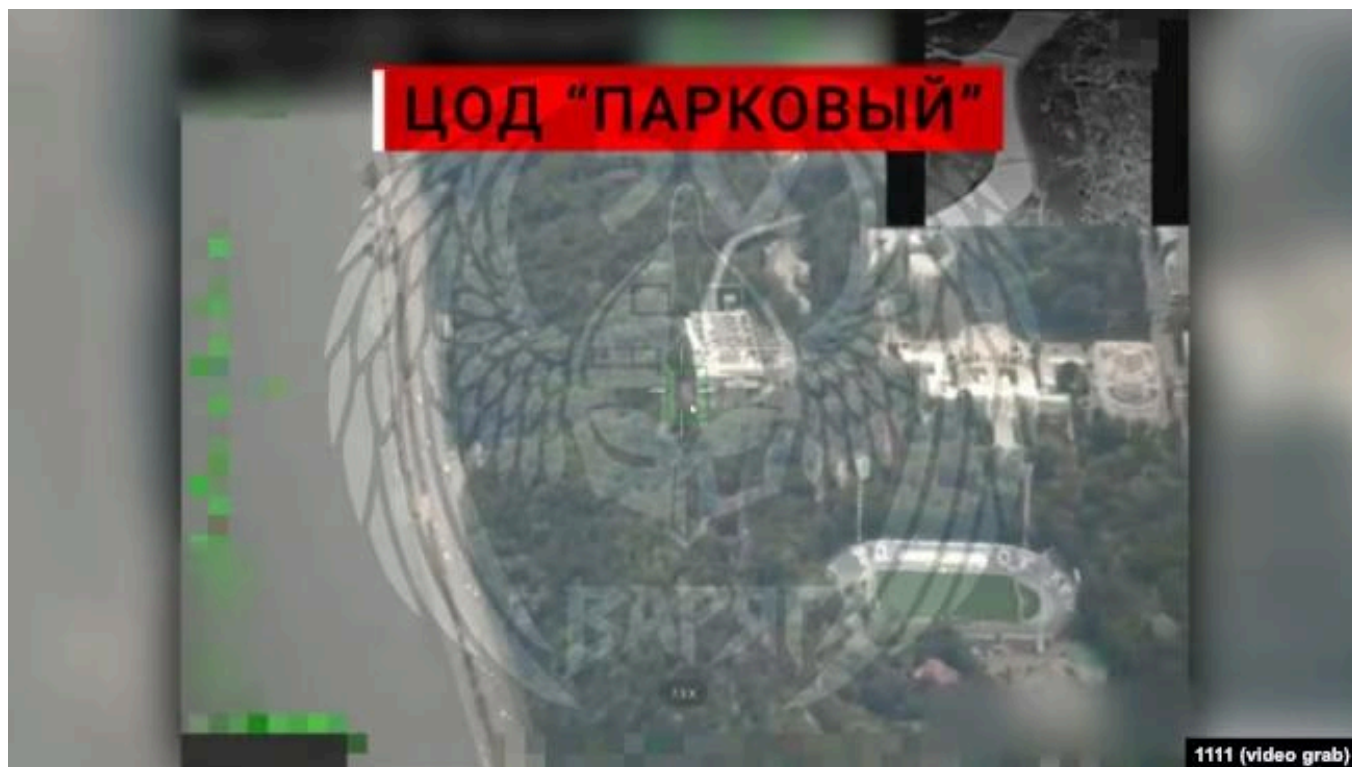
Дым над дата-центром "Яндекса" в Сасове Рязанской области

В конце сентября российская армия последовательно **нанесла серию ударов** по украинским **центрам обработки данных** **i** (ЦОД) и **узлам связи** **i**.

Минобороны России заявило, не приведя никаких доказательств, что украинские ЦОДы **используются** в военных целях. В официальном телеграм-канале российского военного ведомства **назвали** удары по дата-центрам и другой инфраструктуре "цифровым детоксом в принудительном режиме".

"Как можно бить по дата-центрам, по мобильной связи? Как Путин это делает? Как он не думает о том, что мобильной связью пользуются не только в Киеве, в Украине? В Москве тоже пользуются", – **отреагировал** на российские удары украинский президент **Владимир Зеленский**.

Спустя несколько дней под ударом оказались уже российские дата-центры компаний "Яндекс" и "Сбер" – из-за украинских атак в российском сегменте интернета наблюдалась масштабные сбои. Зеленский назвал это зеркальным ответом на действия России.



ЦОД "Парковый" в объективе российского беспилотника

"Результат заблаговременного планирования". Удары по украинским дата-центрам

Алексей Семеняка, специалист по сетевой инфраструктуре с опытом проектирования сетей и строительства дата-центров, отмечает в комментарии Радио Свобода, что следует различать удары по дата-центрам и атаки на узлы , обеспечивающие связность сети.

"Связность – это то, как данные проходят из точки А в точку Б: сколько существует маршрутов и можно ли перераспределить трафик, если какой-то из этих маршрутов перегружен или недоступен. Есть крупные узлы, где маршруты пересекаются и где операторы взаимодействуют друг с другом. Дата-центр – конечная точка, куда приходят данные, или начальная, откуда они отправляются пользователю", – поясняет он.

Специалист вспоминает, что в начале полномасштабного вторжения украинские узлы связи подвергались ударам, но местные операторы быстро координировались, чтобы восстанавливать соединение.

"Они помогали друг другу, причём зачастую бесплатно. Сейчас горизонтальные связи в операторском сообществе ещё крепче, чем тогда", – говорит Семеняка.

Семеняка отмечает, что предсказать последующую тактику российских ударов и, следовательно, масштаб угрозы связности сети в краткосрочной перспективе сложно, но уже в среднесрочной операторы способны быстро восстанавливать связь.

Об этом говорит и то, как украинские операторы справились с последствиями недавних российских ударов: 23 сентября ВС РФ повредили в Киеве сетевую инфраструктуру нескольких провайдеров, в том числе узловое оборудование UTELS, а также оборудование и линии связи компании "Паутина"; у ста тысяч домохозяйств в Киеве и области **возникли** проблемы с подключением к сети. Уже спустя пару часов после аварии UTELS **сообщил** о восстановлении связи для большинства своих абонентов, а "Павутина" – о возобновлении работы почти всей сети на резервном оборудовании.



СМОТРИ ТАКЖЕ

Разведданные и Starlink для ВСУ. Сомнения на фоне ударов по Киеву

Говоря о дата-центрах, Семеняка отметил, что в последние годы украинские проекты развивались с учётом возможной необходимости экстренно перенести свои данные и сервисы.

"Идея заключалась не в том, чтобы поставить вокруг каждого объекта несколько систем ПВО, а в стандартном для отрасли подходе: географическом резервировании и возможности миграции на другую площадку. Скорость такого переноса зависит от потребностей сервиса и бюджета: не всем нужно самое дорогое решение с немедленным переключением", – говорит телеком-эксперт.

С конца сентября под ударом **оказались** не менее восьми украинских центров обработки данных. Многие помещения были разрушены, но работа самих сервисов в большинстве случаев продолжилась, пусть **не сразу** и с определенными перебоями.

По **словам** **Александра Ольшанского**, основателя хостинг-провайдера MiroHost, чей дата-центр был уничтожен российскими ударами, около 95% клиентов компании

продолжили работу благодаря мощностям в Польше и Чехии. Полностью прекратил работу и дата-центр "Парковый", но данные клиентов удалось развернуть на резервных площадках в ЕС. ЦОД компании Data Group тоже пострадал, но сами сервисы, находившиеся на серверах, продолжили работу благодаря заблаговременному резервированию.

Из-за роста рисков и затрат провайдеры, однако, предупреждают о предстоящем подорожании тарифов на домашний интернет в Украине.

В целом же, по словам замминистра цифровой трансформации Украины **Виталия Балашова**, перебои носили локальный и временный характер, в большинстве случаев клиентские данные сохранились, а компании восстанавливали работу на резервных площадках.

Семеняка называет реакцию украинских компаний на российские атаки "результатом заблаговременного планирования". "С начала войны было понимание, что такое может случиться", – поясняет собеседник.

"Поэтому я оцениваю эти действия России так же, как удары по гипермаркетам "Эпицентр" или складам "Новой почты" – как попытку запугать, а не достичь каких-то военных целей", – продолжает специалист.



СМОТРИ ТАКЖЕ

"Враг разносит Киев". Украинская столица под российскими ударами

Обратный "цифровой детокс". ВСУ наносят ответный удар

С 8 по 11 октября украинская армия поразила дата-центры "Яндекса" в Калуге, Сасове (Рязанская область) и Владимире – три из пяти основных центров обработки данных компании. В калужском центре пострадала часть инфраструктуры, а два других полностью остановили работу.

В результате украинских ударов сервисы "Яндекса" – от такси и доставки еды до электронной почты и сервисов оплаты – работали с перебоями или не работали вовсе. Атаки коснулись и сторонних компаний: пользователи жаловались на сбои в

работе сервисов РЖД, "Авито", "Циан", "Т-Банка", а также сайтов ряда СМИ – РБК, РИА Новости и "Ведомостей".

"Приложение не работает и пишет, что деньги в безопасности, что должно скоро заработать. Но пока не работает", – рассказывает АРР житель Москвы Семен.

Станислав из Москвы не мог внести платеж по кредитной карте другого банка, поскольку все его деньги в момент сбоя находились на накопительном счете в Яндексе".

"Пришлось занимать у знакомых, чтобы не попасть на проценты. Другому банку ведь не объяснишь, почему ты не можешь заплатить", – [рассказал](#) он "Медузе".

Жительница столицы Инна рассказала изданию, что сервис "Собака гуляла" отменил поездку её пожилой собаки к реабилитологу: из-за сбоя компания не могла просмотреть уже принятые заказы.



Последствия удара по дата-центру "Яндекса" во Владимире

В Ростове-на-Дону таксисты выстроились в очередь у офиса местного оператора такси, чтобы [подключиться](#) к агрегатору.

Как [отметил](#) в разговоре с "Би-би-си" знакомый с инфраструктурой "Яндекса" собеседник, "большинство сервисов компании "жило" в трех атакованных центрах". Это утверждение касается и сильно пострадавшего облачного хранилища Yandex Cloud: платформа была [размещена](#) в разных зонах доступности,

чтобы в случае выпадения одной из зон сервис мог продолжить работу в штатном режиме. Ударам, однако, подверглись сразу все ЦОДы, отвечающие за эти зоны доступности – к такому система оказалась попросту не готова.

Например, во Владимире находятся сразу два независимых друг от друга дата-центра, в каждом из них находилось по одной зоне ответственности, и в компании просто не предполагали, что остановка работы сразу двух "владимиров" возможна, рассказал собеседник "Би-би-си".

Алексей Семеняка считает, что культура регулярных учебных отключений дата-центров также могла деградировать в ходе реорганизации "Яндекса": раньше компания проводила экстренные учения раз в одну-две недели. "Яндекс" и сейчас заявляет, что регулярно тестирует отказоустойчивость систем, но не уточняет, насколько часто.

Сразу же после украинских ударов Yandex Cloud договорилась с Selectel, K2Cloud и VK Cloud об ускоренном размещении клиентских данных и сервисов на их мощностях. Хотя найти место для хранения данных относительно легко, гораздо сложнее восстановить работу сервисов, отмечает Семеняка: каждый из них состоит из множества связанных компонентов.

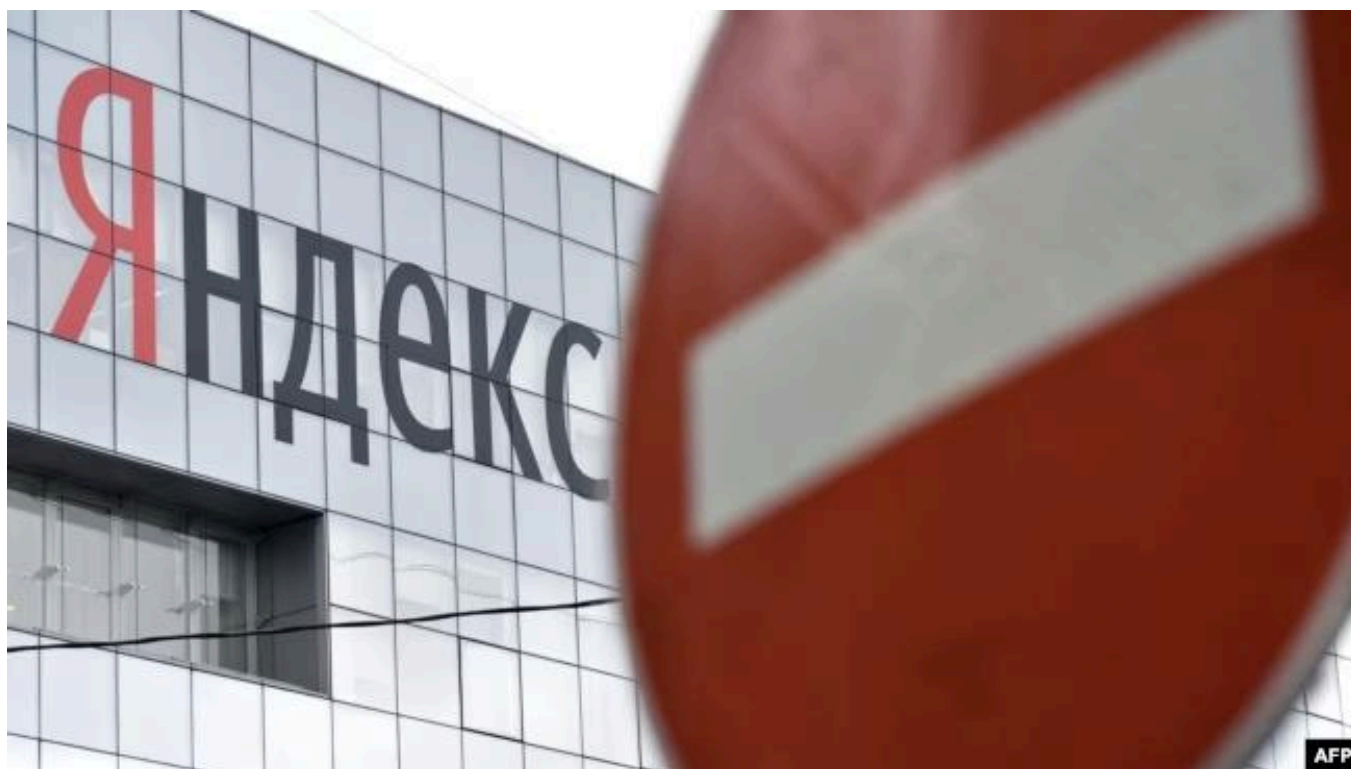
"Это сложная, "дышащая" система. Одна из главных трудностей восстановления — заставить её снова "дышать". Недостаточно включить оборудование и сказать: "Работай". Нужно восстановить все уровни этой системы и взаимодействие между ними", – поясняет он.

К тому же, отмечает бывший гендиректор "Яндекс.Украина" **Сергей Петренко** в интервью Настоящему времени, сервисы компании уже долго время работают на своем собственном специфическом оборудовании.

"Нужен именно "яндексовский" сервер, чтобы безболезненно развернуть все то программное обеспечение, которое должно бы работать и чтобы обеспечивать те сервисы "Яндекса", которые нужны", – говорит он.

Алексей Семеняка отмечает, что восстановление поврежденных и замена уничтоженных вычислительных мощностей компании займет много времени: российской компании придется закупить большое количество серверов в условиях санкций, дефицита памяти и ее дороговизны. Так, по данным газеты

"Коммерсант", на замену вышедшего из строя оборудования может уйти до шести месяцев.



В Сасове и Владимире также расположены три суперкомпьютера  компании – "Галушкин", "Червоненкис" и "Ляпунов". Пострадали ли они в результате украинских ударов, неизвестно.

Впрочем, даже если они уцелели, перенести их в новое место или распределить мощности по другим дата-центрам будет довольно трудно, отмечает Семеняка. Если обычные сервисы спроектированы так, чтобы они могли автоматически переноситься на удаленную площадку, – с минимальным перерывом в работе и незначительной потерей данных, – то для таких крупных вычислительных комплексов важна физическая близость оборудования, и просто распределить его элементы между разными центрами не выйдет.

"Например, в кластере может быть множество ускорителей компании Nvidia, использующих удаленный прямой доступ к памяти. Если эта память окажется за тысячу километров, задержки настолько снизят производительность, что система не сможет нормально работать", – объясняет эксперт.

Если же компьютеры уничтожены, восстановить их возможно: у компании уже есть опыт, проект и документация, отмечает эксперт. Основная трудность, как и в случае с другими вычислительными мощностями, – закупка и доставка оборудования, значительная часть которого не производится в России.

Что касается языковых моделей, которые обучались на суперкомпьютерах, – они, вероятно, не пострадали, предполагает собеседник: у "Яндекса", скорее всего, были резервные копии. Если же результаты обучения утрачены, после восстановления оборудования модель придется обучать заново: хотя компания уже умеет это делать, повторное обучение потребует значительных вычислительных ресурсов и времени.

"Трудность в том, чтобы снова собрать и запустить всё необходимое в условиях дефицита оборудования и санкций. При этом остаётся вопрос физической уязвимости. Если восстановить комплекс в другом месте, он всё равно останется отдельной установкой, уязвимой для физического воздействия", – подчеркивает специалист.

14 октября украинские беспилотники атаковали центр обработки данных "Сбера", расположенный в городе Балаково Саратовской области, – власти планировали сделать его крупнейшим в Европе к 2030 году; на площадке также хотели разместить к 2027 году новый суперкомпьютер. И хотя в компании заявили, что "все системы и сервисы компании работают штатно", в российском интернете вновь произошел масштабный сбой, затронувший экосистемы самого "Сбера", а также "Яндекса", "ВКонтакте", маркетплейса Ozon и еще ряда компаний.



Последствия удара по дата-центру "Сбера"

От расчетов ПВО до ЦОДов "судного дня". Как российские компании хотят защищаться от беспилотников

Проблему защиты ЦОД от дронов в отрасли начали обсуждать еще в 2025 году. Компания "Синергия Интегратор", предоставляющая услуги по защите объектов от БПЛА, предлагала скрывать объекты при помощи маскировочных сетей, защищать их при помощи троссов, защитных сеток и других конструкций, а также использовать радары для раннего обнаружения беспилотников и средства радиоэлектронной борьбы для их подавления.

24 августа 2026 года **Владимир Путин** подписал указ, позволяющий вводить временное государственное управление объектами критической инфраструктуры, которые не обеспечили надлежащую защиту от БПЛА.

В начале сентября гендиректор CorpSoft24 **Константин Рензев** отметил в комментарии "Коммерсанту", что все крупные ЦОДы давно обеспечены системами информбезопасности различного уровня, а гендиректор хостинг-провайдера RUVDS **Никита Цаплин** рассказал изданию, что "ряд российских дата-центров уже начал модернизацию систем защиты внешнего инженерно-технологического оборудования под требования современных вызовов". Уже после ударов по "Яндексу" Цаплин сообщил "Коммерсанту", что "некоторые игроки уже начали закупать оборудование для защиты от атак БПЛА".



Мобильные группы ПВО в преддверии Парада Победы в Москве. 9 мая 2026 года

12 октября глава Минцифры **Максут Шадаев** заявил, что ведомство решает вопрос о защите дата-центров после украинских атак совместно с Минобороны.

"Атаки по масштабу – мы все это в режиме реального времени отслеживали – были беспрецедентными. И, конечно, сейчас вся отрасль помогает решать [проблемы]", – заявил он.

В качестве одного из решений обсуждается перенос центров под землю, а "Ростелеком" предлагает создать ЦОД "судного дня", который позволит восстанавливать работу критически важных цифровых сервисов после атак и масштабных сбоев.

Тем временем "Росатом" удалил со своего сайта страницы всех своих дата-центров или с информацией о них, так же поступил и "Сбербанк", обратило внимание Радио Свобода.

Могут ли удары по дата-центрам привести к серьезным последствиям?

По словам Алексея Семеняки, последствия атак на децентрализованную инфраструктуру зависят от их масштаба. В краткосрочной перспективе удары могут существенно нарушить работу сервисов и доступ в интернет, а также затронуть энергосистему на отдельных территориях.

Долгосрочные последствия оценить сложнее. Эксперт напоминает, что от дата-центров зависят не только общедоступные интернет-сервисы, но и внутренние информационные системы железных дорог и авиации. Они необходимы, в частности, для согласования международных перевозок.

Если Россия продолжит политику “суверенной сети”, она, по мнению Семеняки, может оказаться в менее выгодном положении, чем Украина, которая ещё в 2022 году начала переносить некоторые критические системы на мощности зарубежных партнёров.

"Восстановление каналов связи – непростая работа, но она выполнима и не требует каких-то безумных затрат. При этом сами критические информационные системы могут оставаться в безопасности за пределами страны. Если же они находятся внутри неё и тоже подвергаются ударам, приходится восстанавливать не только доступ к ним, но и сами системы. Это гораздо сложнее", – объясняет эксперт.

Военный эффект ударов по ЦОДам и узлам связи специалист считает прежде всего косвенным. В качестве аналогии эксперт приводит Wildberries: по его словам, компания напрямую не работает на российские вооружённые силы, однако на площадке продавались товары военного назначения.



Люди смотрят на догорающий склад Wildberries в Коледино, Московская область. 16 августа 2026 года

Он считает, что, если удары по российским дата-центрам продолжатся, они могут повлиять на российскую экономику, а это, в свою очередь, может сказаться на военной составляющей.

"Прямой связи "ударили по дата-центру – рухнул участок фронта" не будет. Но это касается финансирования военной кампании, устойчивости экономики и настроений в обществе — всего, что косвенно влияет на войну", – говорит он.



Евгений Легалов

Журналист. Выпускник факультета социальных наук Карлова университета в Праге

В России

Выбор Свободы

Мир

Украина