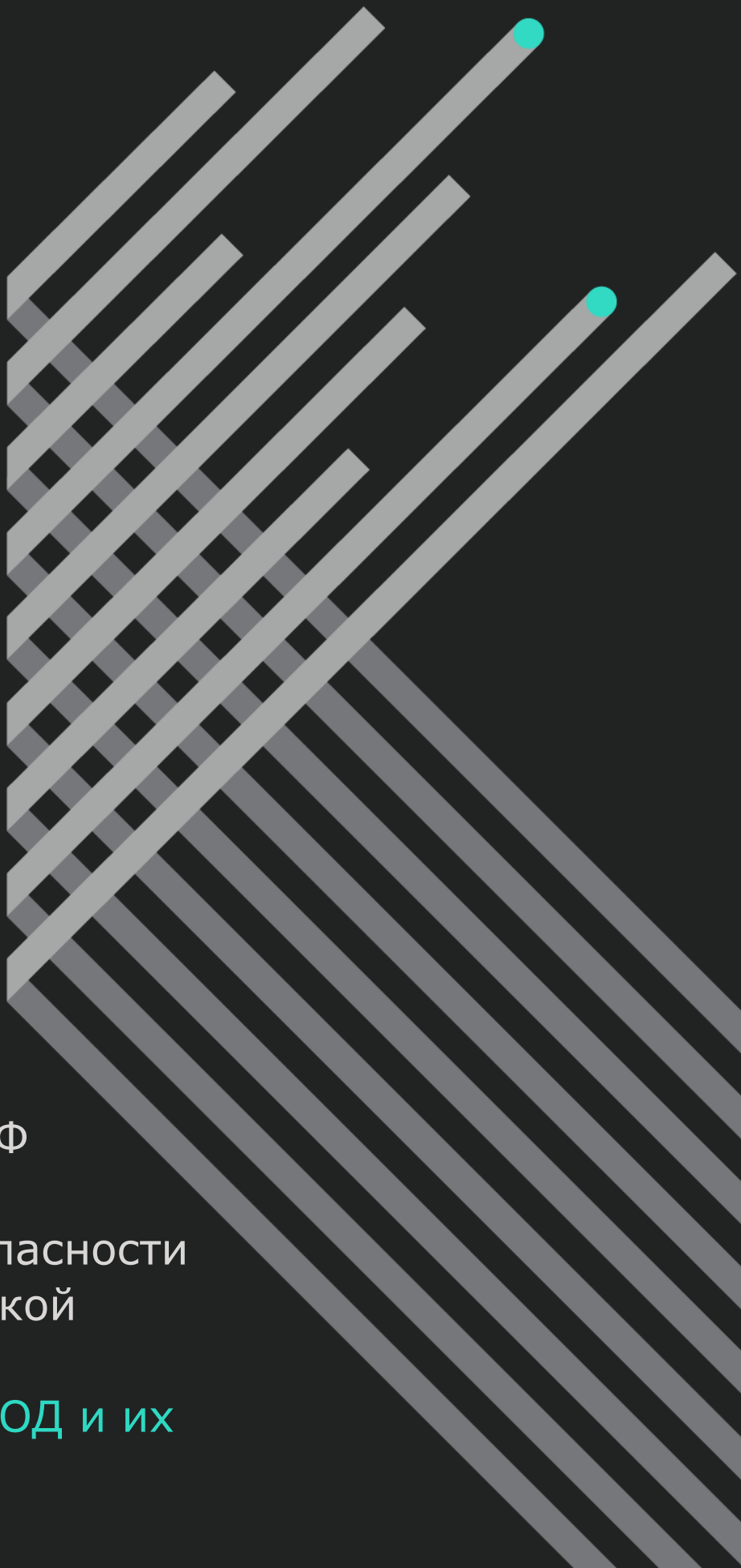
BGP LITIGATION | комплексная правовая поддержка

bgplaw.com



# Указ Президента РФ «О мерах по обеспечению безопасности объектов критической инфраструктуры»: как это затронет ЦОД и их клиентов?

6 ноября 2026 г. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – «Минцифры») провело совещание с операторами центров обработки данных (далее – «ЦОД»). Основное заявление: операторы коммерческих ЦОД обязаны резервировать 10% своих мощностей, чтобы при необходимости выделить их сервисам из т.н. «белого списка»[1]. Если оператор не исполняет эту обязанность, то в отношении ЦОД власти смогут ввести временное управление.

**1. Чем обусловлено заявление Минцифры.**

24 августа 2026 г. Президент РФ подписал Указ № 604 «О мерах по обеспечению безопасности объектов критической инфраструктуры Российской Федерации» (далее – «Указ 604»).

**Суть Указа 604:** государство может временно взять объект критической инфраструктуры (далее – «объект КИ») под свой контроль, т.е. ввести временное управление[2] на нем, если собственник объекта не обеспечивает его безопасность, а именно:

- не принимает или несвоевременно принимает меры для обеспечения безопасности объекта КИ;
- не соблюдает требования по обеспечению безопасности объекта КИ;
- создает угрозу безопасности или работе объекта КИ, в том числе принимает неэффективные меры для предотвращения нападения с помощью БПЛА;
- не восстанавливает или несвоевременно восстанавливает работу объекта КИ.

К объектам КИ относятся объекты топливно-энергетического комплекса, промышленные объекты, объекты связи, объекты коммунальной, транспортной и логистической инфраструктуры, объекты энергетики, объекты жизнеобеспечения, и другие объекты, которые имеют особо важное значение для обеспечения безопасности, экономической стабильности и жизнедеятельности населения. При этом, ЦОД также относятся к объектам КИ.

2 ноября 2026 г. Президент РФ подписал Указ № 802 «О временных мерах по обеспечению поддержки функционирования на территории Российской Федерации информационных ресурсов» (далее – «Указ 802»).

**Суть Указа 802:**

- Операторы коммерческих ЦОД обязаны резервировать 10 % мощностей и по решению Подкомиссии по обеспечению бесперебойного функционирова-

[1] Ресурсы из «белого списка» — это перечень российских ресурсов, которые продолжают работать при временных ограничениях или отключениях мобильного интернета. Перечень формируется Минцифры. В него входят государственные порталы, банковские сервисы, маркетплейсы, социальные сети, сервисы связи, транспорта и пр.

[2] Временное управление означает, что право собственности сохраняется за собственником объекта КИ, но имуществом будет владеть и пользоваться Федеральное агентство по управлению государственным имуществом. При этом к имуществу относится движимое и недвижимое имущество, ценные бумаги и доли в уставных капиталах компаний, имущественные права.

ния объектов в сфере информационных технологий и связи по обеспечению (далее – «Подкомиссия»)[3] предоставлять их в течение суток для «обеспечения поддержки функционирования на территории РФ информационных ресурсов», т.е. для восстановления работы сервисов из «белых списков».

- Операторы коммерческих ЦОД могут временно использовать вычислительные мощности за рубежом по решению Подкомиссии, согласованного с Федеральной службой безопасности РФ (далее – «ФСБ»).

При этом, срок реализации этих требований для операторов ЦОД более чем сжатый – не позднее 11 ноября 2026 г. включительно.

**Важно:**

- Указ не коснется корпоративных ЦОД, предназначенных исключительно для внутренних нужд, а также пострадавших ЦОД. Однако он распространится на те коммерческие ЦОД, которые как используются для собственных нужд, так и сдаются третьим лицам в аренду.
- Операторы ЦОД могут продолжать использовать зарезервированные мощности, в т.ч. предоставлять их клиентам. Однако они должны быть готовы оперативно их освободить по решению Подкомиссии.
- На текущий момент не разработаны ни Положение о Подкомиссии, ни порядок принятия ей решений, ни методика расчета резервных мощностей. И хотя сам Указ уже вступил в силу, когда начнет работать предусмотренный им механизм – неясно.
- Если у оператора ЦОД что-то выйдет из строя, то самого по себе этого факта недостаточно для того, чтобы начать использовать ЦОД зарубежом – на это нужно разрешение Подкомиссии и ФСБ.
- Возможность использовать зарубежные ЦОД не отменяет требований о локализации баз персональных данных и правил трансграничной передачи персональных данных, предусмотренных ст. 12, ч. 5 ст. 18 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – «152-ФЗ»).

**2. Последствия для бизнеса.**

Ключевой риск заключается в том, что оператор ЦОД должен предоставить мощности по решению Подкомиссии в течение суток, даже если они уже используются клиентами по действующим договорам. Чтобы освободить эти ресурсы, нужно переносить виртуальные серверы, перераспределять нагрузку и перемещать оборудование, а некоторых клиентов – вынуждено отключать от используемых ими мощностей.

[3] Постановление Правительства РФ от 07.09.2018 № 1065 «О Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности».

Вместе с тем, Указ 802 не устанавливает специального порядка изменения или расторжения договоров, как и не предусматривает особого порядка возмещения убытков. На текущий момент Минцифры лишь высказало предложение о том, что отключение от мощностей действующих клиентов могло бы признаваться форс-мажором по п. 3 ст. 401 ГК РФ. Таким образом, исполнение решения Подкомиссии может потенциально приводить к нарушению обязательств перед клиентами, финансовым и репутационным потерям для операторов ЦОД.

Более того, само резервирование мощностей не оплачивается: операторы ЦОД получат плату только за фактически предоставленные ресурсы по предельным тарифам, которые будут установлены Подкомиссией. При этом расходы на содержание инфраструктуры останутся на операторах ЦОД.

Ключевой риск для клиентов заключается в том, что они в любой момент могут потерять доступ к оплаченной инфраструктуре из-за восстановления работы более приоритетных сервисов из «белых списков».

### 3. Что нужно сделать уже сейчас?

**Операторам ЦОД рекомендуем:**

- Определить состав резервных площадей и мощностей и подготовить план их предоставления в течение суток: какие ресурсы освобождать, куда переносить клиентские системы и кто отвечает за выполнение работ. Документально зафиксировать меры по исполнению Указа 802.
- Проверить договоры с клиентами и SLA, а для новых договоров - предусмотреть порядок уведомления, переноса ресурсов и распределения расходов при исполнении решения Подкомиссии. Такие условия помогут снизить договорные риски, связанные с предоставлением зарезервированных мощностей.
- Проверить выполнение применимых требований безопасности и готовность к восстановлению работы ЦОД. Необходимо фиксировать выявленные недостатки, сроки их устранения и принятые меры, т.к. нарушения безопасности и несвоевременное восстановление объекта входят в основания для временного управления по Указу 604.
- Подготовить порядок безопасного переноса персональных данных: ограничить доступ, защитить резервные копии и проверить удаление данных с освобождаемых ресурсов. Если ЦОД обрабатывает данные клиента по соглашению о поручении обработки персональных данных, то такие изменения необходимо согласовать с клиентом и отразить в этом соглашении с учетом требований ч. 3 ст. 6, ст. 19 152-ФЗ.

**Клиентам ЦОД рекомендуем:**

- Уточнить у оператора ЦОД, могут ли используемые мощности потребоваться для исполнения Указа 802, какие альтернативные ресурсы доступны и как будет организован перенос. Закрепить порядок уведомления, оказания помощи с переносом и расчетов при ограничении доступа в договоре.

- Заранее определить, куда можно перенести критически важные сервисы при отключении ЦОД, подготовить актуальные резервные копии данных и проверить, что на новой площадке удастся быстро восстановить работу.
- Закрепить в договоре с оператором ЦОД обязанность заранее уведомлять о смене площадки обработки персональных данных, а также согласовывать перенос данных зарубеж.

BGP LITIGATION

комплексная
правовая
поддержка

ДЦ «Империя», Пресненская наб., д. 6, стр. 2
г. Москва, Россия 123112

+7 (495) 777 28 20 office@bgplaw.com bgplaw.com



## Арсений Топадзе

Советник, адвокат
Защита данных и цифровое регулирование

arseniy.topadze@bgplaw.com



## Мария Константинова

Младший юрист
Защита данных и цифровое регулирование

mariia.konstantinova@bgplaw.com