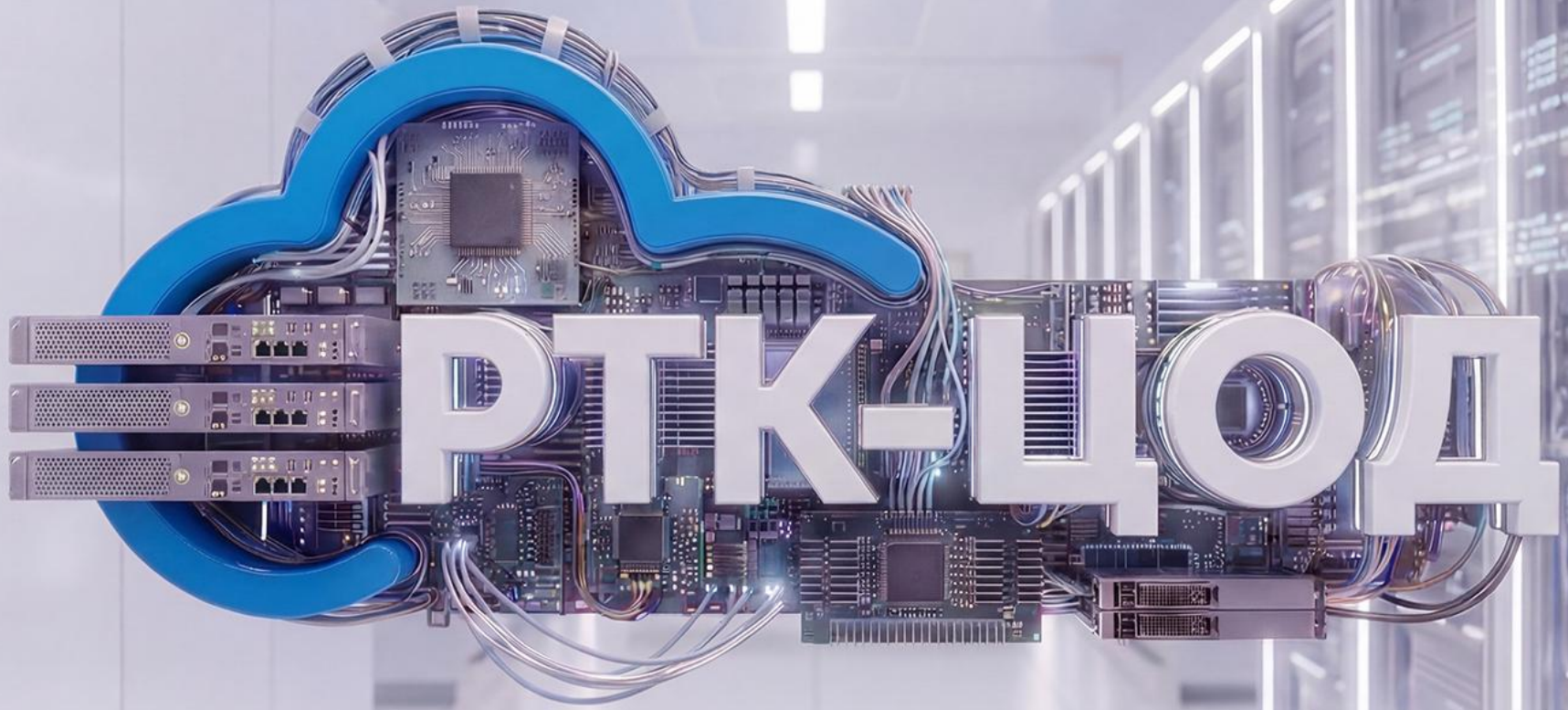


«Ковчег»

Архитектура хранения и восстановление данных в условиях комбинированных угроз

РТК-ЦОД

ОСНОВНОЙ РИСК

ЧТО ПРОИЗОЙДЁТ, ЕСЛИ ВАШИ РЕЗЕРВНЫЕ КОПИИ БУДУТ СКОМПРОМЕТИРОВАНЫ ИЛИ УНИЧТОЖЕНЫ ВМЕСТЕ С ИТ-ИНФРАСТРУКТУРОЙ?



Большинство решений резервного копирования и аварийного восстановления (Disaster Recovery) находятся внутри того же контура, который должны защищать. В результате успешной атаки на контур они перестают быть защитой — **они становятся частью проблемы.**

Новая реальность: Комбинированные угрозы

ПРОВЕРЕНО НА ПРАКТИКЕ

Кибернетический вектор:

Компрометация хранилищ резервных копий
Целевые атаки начинаются с поиска и уничтожения резервных копий до шифрования основной среды.

Месяцы внутри инфраструктуры
До начала активной атаки злоумышленник может присутствовать внутри сети компании от нескольких недель до нескольких месяцев.

Удаление точек восстановления
В ходе кибератаки точки восстановления методично удаляются, сужая окно возможного отката.

Физический вектор

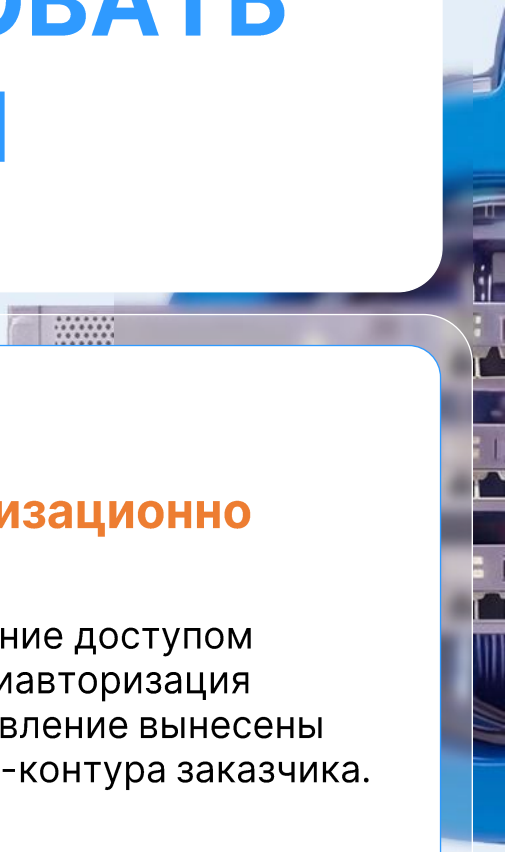
Риски повреждения или уничтожения ЦОД

Внешние деструктивные воздействия на объекты, техногенные аварии, диверсии, масштабные отключения. Если резервная площадка находится в том же здании или районе, она будет потеряна вместе с продуктивным контуром.

Резервные копии внутри продуктивного контура предприятия — это иллюзия защиты.

КЛЮЧЕВОЙ ИНСАЙТ

ВАШИ ДАННЫЕ ДОЛЖНЫ СУЩЕСТВОВАТЬ ВНЕ ВАШЕЙ ИНФРАСТРУКТУРЫ



Физически

Географически удаленная площадка, независимые контуры электропитания и охлаждения. Недостижима для локальных угроз.

Логически

Независимая сеть, отдельные учетные записи, отсутствие маршрутизации из основного периметра в хранилище.

Организационно

Управление доступом и мультиавторизация на восстановление вынесены за пределы ИТ-контура заказчика.

Концепция «Ковчег»: Архитектурный стандарт выживания

О СИСТЕМЕ

Изолированный контур хранения

Один сценарий — сохранить бизнес. Не резервная копия. Не система Disaster Recovery. Независимая инфраструктура выживания.

Однонаправленная архитектура

Данные поступают в «Ковчег», но не могут быть изменены или удалены извне

Изолированное хранение

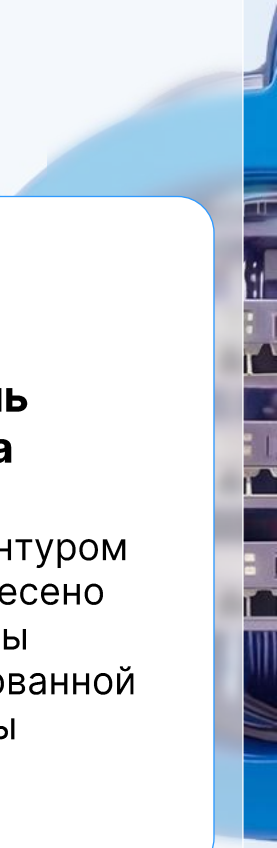
Физически и логически отделённый контур без прямых сетевых связей

Независимая среда восстановления

Инфраструктура восстановления, готовая к активации в случае чрезвычайной ситуации

Контроль доступа

Управление контуром хранения вынесено за пределы скомпрометированной ИТ-среды



Что происходит, если ИТ-инфраструктура потеряна

Управляемый цикл восстановления бизнеса:

ДЕНЬ X

Начало восстановления

Решение принято, изоляция подтверждена

Активация «Ковчега»

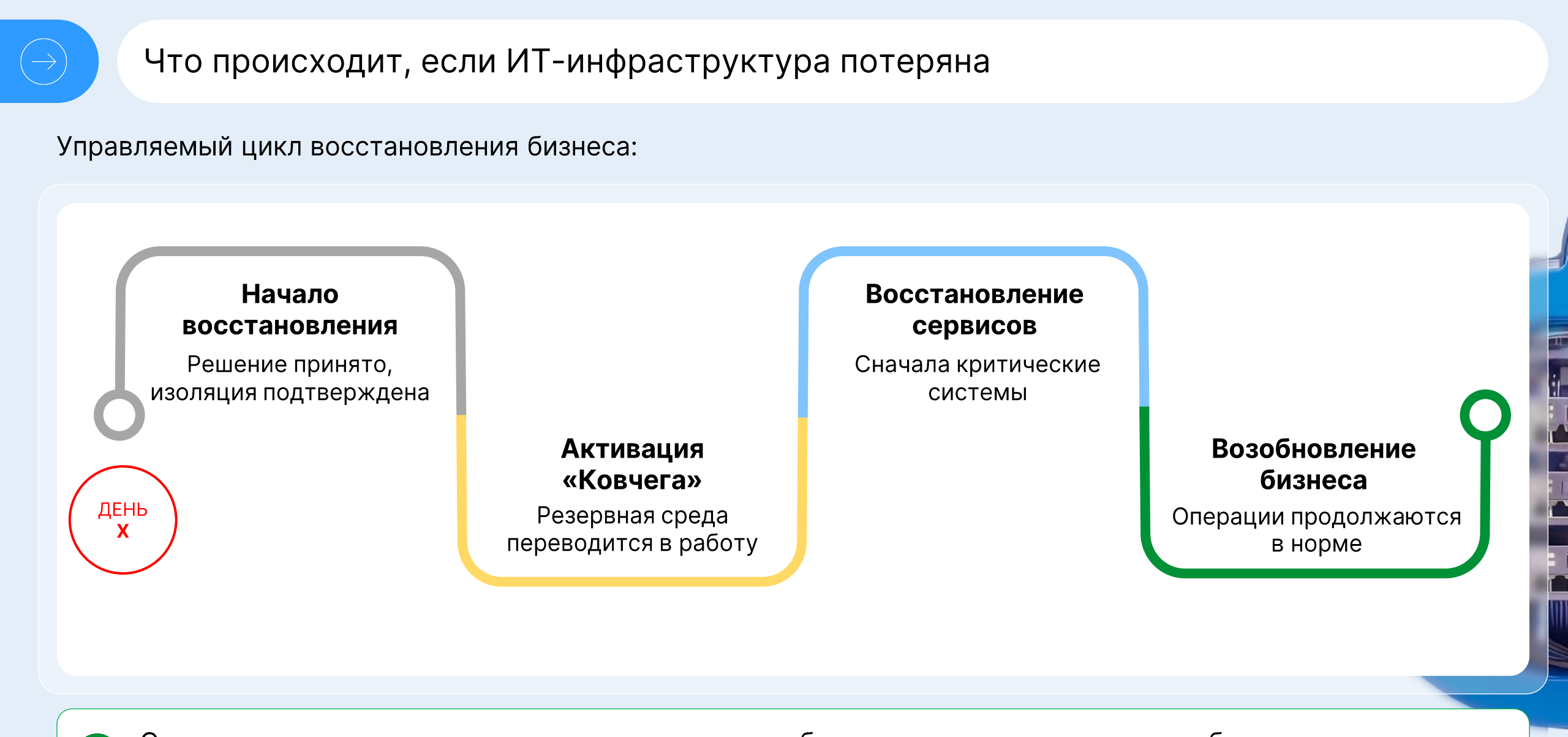
Резервная среда переводится в работу

Восстановление сервисов

Сначала критические системы

Возобновление бизнеса

Операции продолжаются в норме



Система проектируется для хранения данных, необходимых для восстановления бизнеса.
Полный цикл от инцидента до возобновления работы — управляемый и предсказуемый.

РТК-ЦОД

Варианты реализации

АРХИТЕКТУРА

Три модели развёртывания — под разные требования к изоляции, масштабу и мобильности.
Каждая реализация проектируется индивидуально под модель угроз заказчика.



Специализированные ПАК для резервного копирования

- Максимальная эффективность хранения (глубокая дедупликация и компрессия);
- Оптимизация трафика (экономия WAN-канала);
- Нативная защита от изменений (WORM) на уровне файловой системы.

Программно-определяемые хранилища (SDS)

- Линейная масштабируемость и гибкость;
- Независимость от производителей оборудования;
- Единая поддержка блочных, файловых и объектных (S3) интерфейсов.

Модульные ЦОД и высокопроизводительные массивы

- Высокие показатели IOPS и низкие задержки;
- Максимальная скорость чтения при восстановлении;
- Инфраструктура для сценариев, требующих развёртывания на любой площадке.

Позиционирование

Это не система резервного копирования

Резервное копирование — это инструмент операционной защиты.
«Ковчег» — это архитектура выживания бизнеса в условиях комбинированных угроз .

Изолированная инфраструктура хранения
Вне вашего контура, вне досягаемости атаки

Независимый слой восстановления
Независимый слой восстановления
с собственной средой

Управляемый процесс восстановления
Управляемый и верифицированный процесс
восстановления

Архитектура для устойчивости бизнеса
Решение уровня стратегической
непрерывности бизнеса



Когда всё остальное перестаёт работать — остаётся только то, что было изолировано заранее.

Для организаций, которые не могут позволить себе потерю данных

ЦЕЛЕВЫЕ ЗАКАЗЧИКИ

«Ковчег» проектировался для компаний и структур, где остановка бизнеса измеряется не часами — а репутационными, финансовыми и регуляторными последствиями катастрофического масштаба.

Банки и финансовые институты

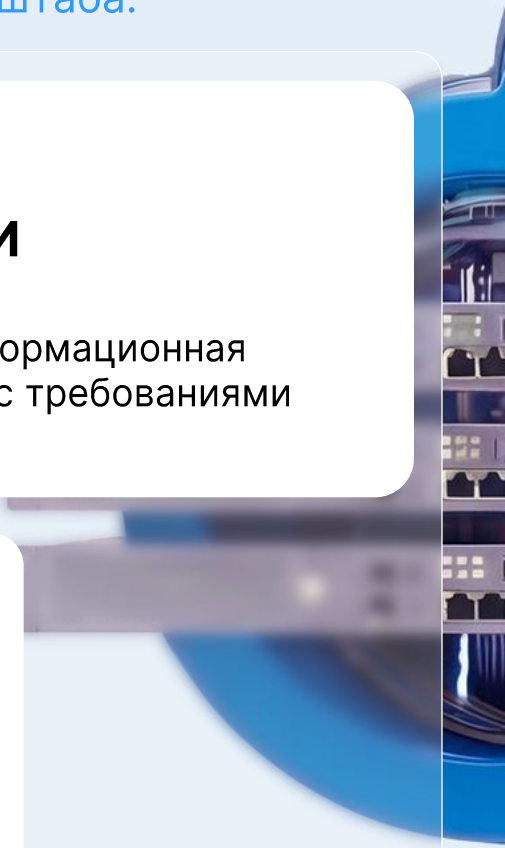
Требования ЦБ, непрерывность расчётов, защита клиентских данных

Государственные системы

Суверенность данных, непрерывность государственных функций

Объекты КИИ

Критическая информационная инфраструктура с требованиями 187-ФЗ



Телеком-операторы

Операторы связи с требованиями к непрерывности сервиса

Крупные корпорации

Компании с распределённой инфраструктурой и высокими ставками

СЛЕДУЮЩИЙ ШАГ

ОБСУДИМ, КАК БУДЕТ ВЫГЛЯДЕТЬ ВОССТАНОВЛЕНИЕ ВАШЕГО БИЗНЕСА

Архитектурная сессия — это закрытая встреча с нашей командой, на которой мы разбираем вашу модель угроз, анализируем уязвимости контура и проектируем индивидуальную схему изоляции и восстановления.

Запросить архитектурную сессию

Каждая реализация проектируется индивидуально под требования инфраструктуры и модель угроз заказчика. Все материалы сессии — конфиденциальны.

Контакты

Алексей Забродин

Технический директор РТК-ЦОД

+7 (985) 774-65-45
A.Zabrodin@rtk-it.ru



РТК-ЦОД

Спасибо за внимание!

РТК-ЦОД