AXOFT

центр экспертизы и дистрибуции
цифровых технологий

Мишенев Федор

Менеджер отдела развития продаж решений инфраструктурного, прикладного, офисного, специализированного ПО

Fedor.Mishenev@axoftglobal.ru

Историческая справка СРК до 2022 года

Американская компания, разработчик программного обеспечения для управления хранением информации для организаций. Основана в 1983 году под названием Tolerant, переименована в Veritas в 1989 году

Частная компания, специализирующаяся на разработке программного обеспечения для резервного копирования виртуальных машин и мониторинга виртуальных сред на базе платформ VMware и Hyper-V. Основана в 2006 году

Основана в 1996 году. С момента своего основания она разрабатывает программное обеспечение для управления корпоративными данными и обеспечения их безопасности. Цель компании - помочь заказчику упорядочить все свои данные и извлекать из них максимальную пользу.

Швейцарская компания-разработчик, основанная в Сингапуре. Известна разработкой системных решений для корпоративных и домашних пользователей по работе с жёсткими дисками, резервным копированием, защитой и восстановлением данных, управлению загрузкой операционных систем, и защиты ОС от внешних угроз

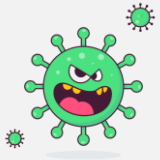
Основные задачи резервного копирования

Обеспечить сохранность данных

Сбой в работе

Несанкционированное проникновение

Случайная перезапись



Утеря по причине вирусной атаки

Удаление по ошибке

Российский ландшафт резервного копирования

В портфеле Axoft

КИБЕР Бэкап

RuBackup

MIND Software

Handy Backup

Нет в портфеле Axoft, но мы о них знаем

береста

хайстекс

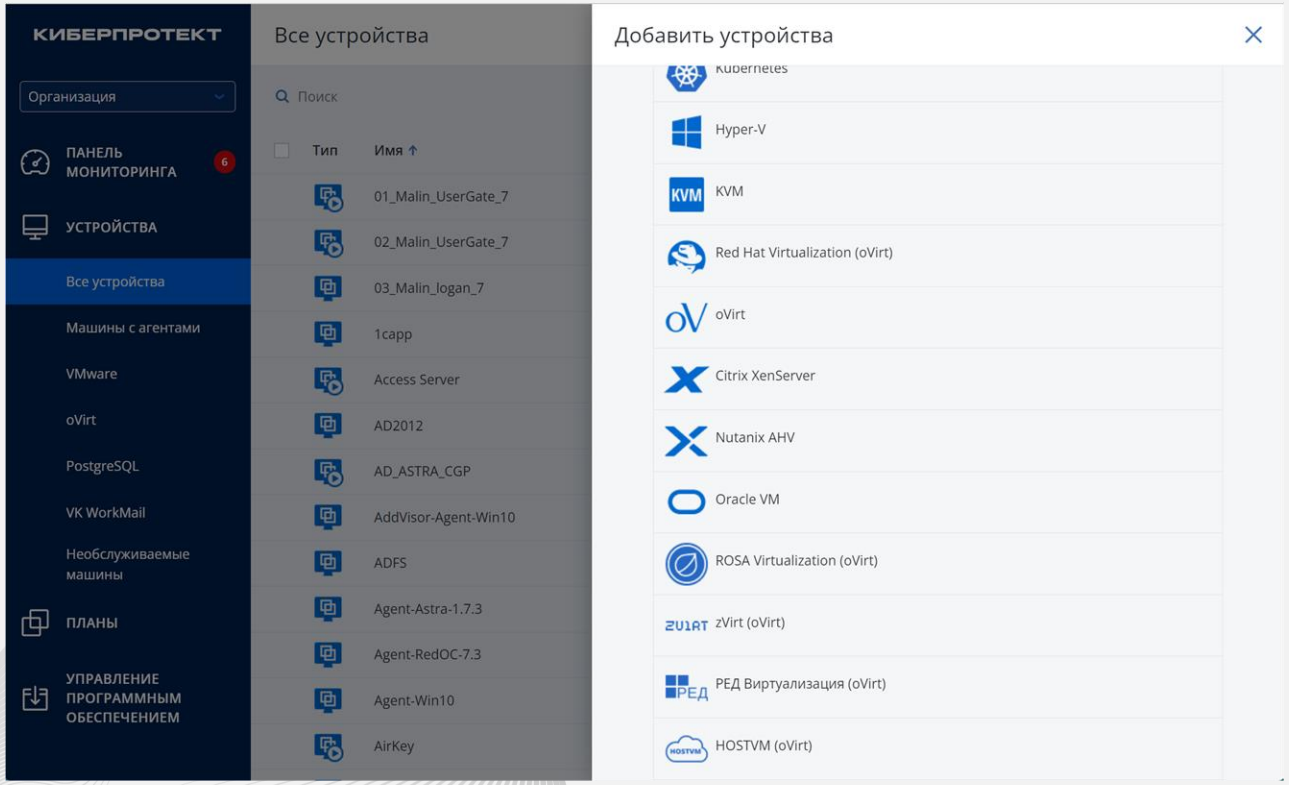
И другие.....

Кибер Бэкап

КИБЕР
Бэкап

Сертификация

- ФСТЭК 4 класса



Преимущества решения:

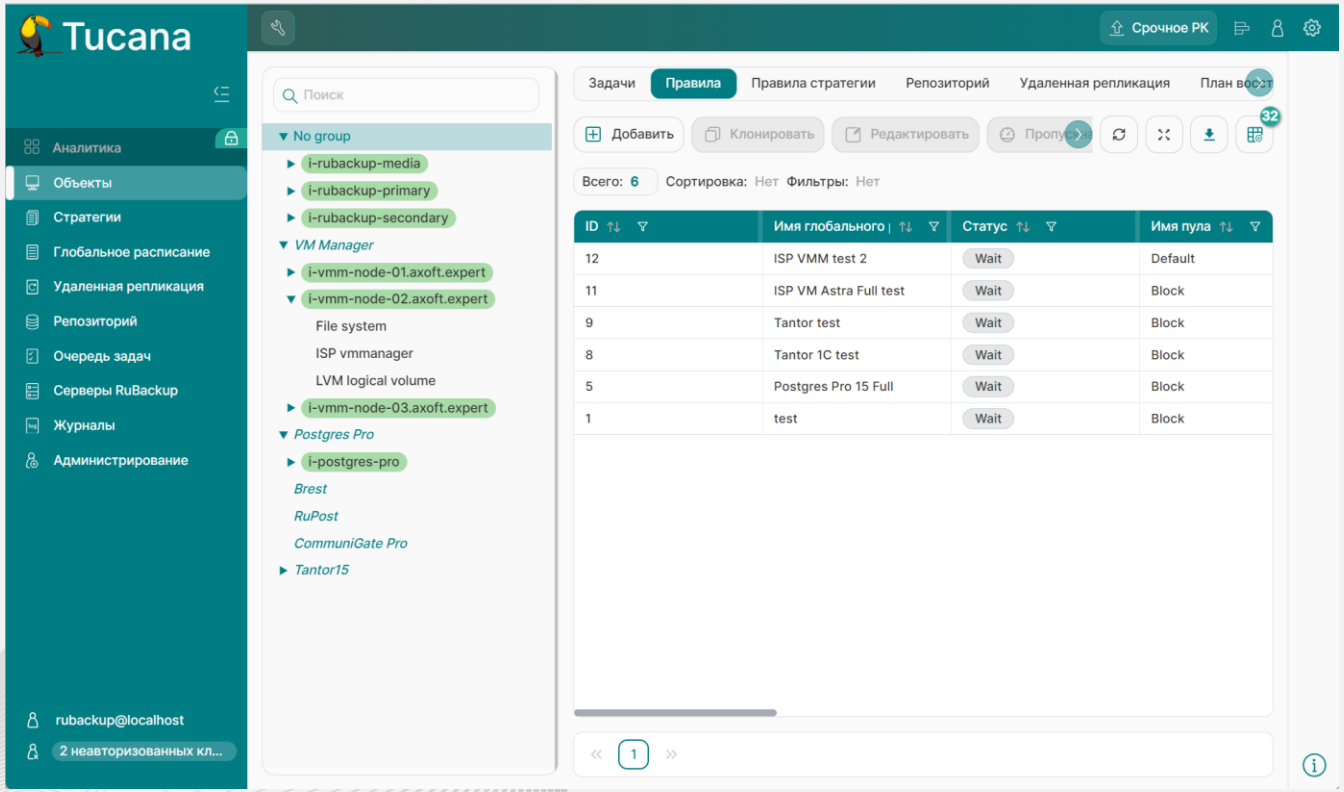
- Простота установки и администрирования
- Поддержка виртуализации Hyper-V
- Поддержка виртуализации Vmware
- Широкая поддержка семейства Windows серверов и рабочих станций
- Моментальное восстановление Hyper-V и VMware
- Работа с LTO устройствами
- Защита от вирусов шифровальщиков и угроз в Windows средах
- Встроенные механизмы сжатия и дедупликации

RuBackup

RuBackup

Сертификация

- ФСТЭК на версию 2.4

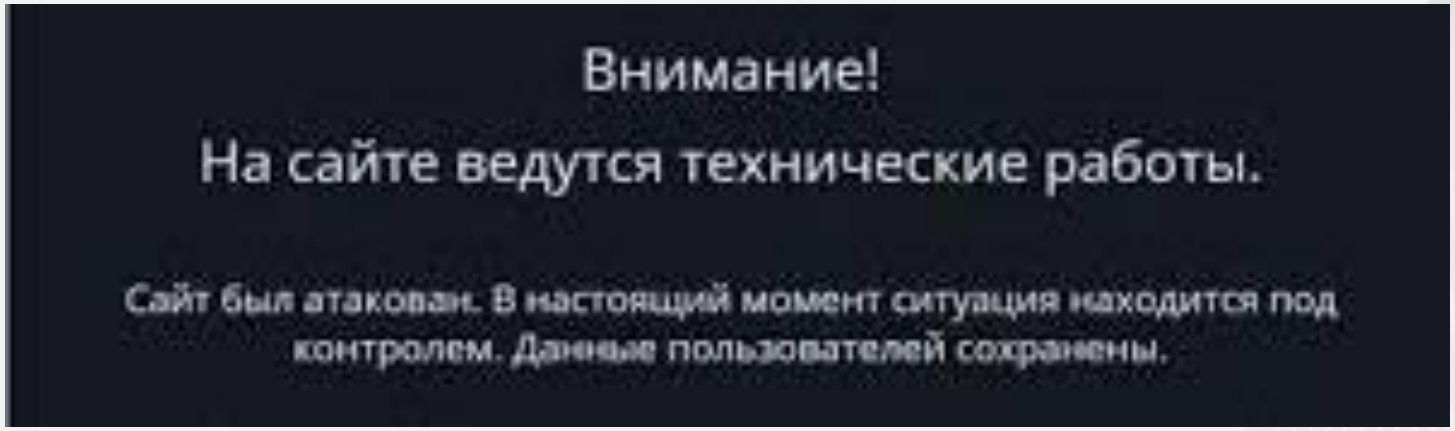


Преимущества платформы:

- Модульная система поставки
- Развитие модулей независимо от платформы
- Поддержка виртуализации Брест
- Поддержка виртуализации ISP VMmanager
- Разработка с «0» – 100% отечественное решение
- Управление системой через Web-консоль и приложение
- Возможность управления на хостах с агентами
- Работа с LTO устройствами
- Встроенные механизмы сжатия и дедупликации

Случай из жизни

9 мая 2022 г один из видеосервисов пережил крупнейшую в истории компании кибератаку. Она поразила более 75% инфраструктуры основной версии и 90% резервных копий. Спустя 10 дней после атаки видеосервис все еще не восстановился. Сложившаяся ситуация как нельзя лучше иллюстрирует предмет сегодняшнего обзора — что должно быть у бизнеса для восстановления данных после мощной DDoS-атаки.



Бэкап, каким он должен быть

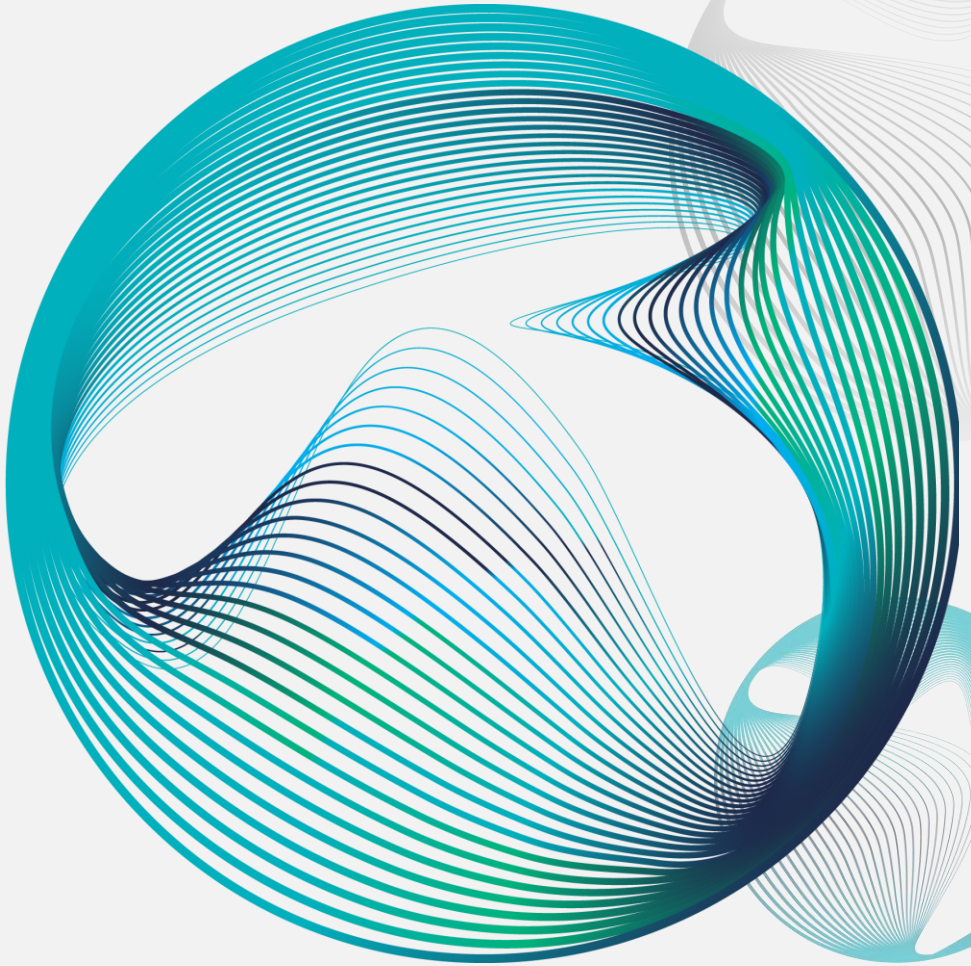
- Делайте бэкапы сервера и не забывайте про отдельный бэкап баз данных. Не во всех решениях получится развернуть систему с нуля и просто импортировать в нее бэкапы.
- Дополнительно к облачным создавайте офлайновые серверные бэкапы. Они выручат в ситуации, когда программа-вымогатель зашифровывает данные, доступные по сети.
- Тестируйте резервные копии. Нередко после тестирования оказывается, что бэкапилось не то, что нужно.
- Следите за настройками бэкапов сервера, выполненными заданиями и местом под хранение копий. Иначе в один непрекрасный день компании понадобится бэкап, а его не получится развернуть из-за ошибки резервного копирования.
- Выделите для резервного копирования виртуальных машин отдельное хранилище. Держать резерв на той же СХД, где хранится основная информация — не лучшая идея.

Важно!

Бэкап должен быть у каждого бизнеса. Но не каждому достаточно бэкапа. У классического резервного копирования RTO и RPO составляют несколько часов. Это значит, что резервные копии виртуальных машин и копии баз данных сохраняются, например, каждые 3, 6, 9, 12 или 24 часа. Соответственно после распаковки бэкапов система восстановится без данных за последние 3, 6, 9, 12 или 24 часа.

AXOFT

центр экспертизы и дистрибуции
цифровых технологий



Действуй вместе с нами

В компетенции инженерного блока АО «Аксофт» входит плавный переход с зарубежных решений резервного копирования на импортонезависимые.

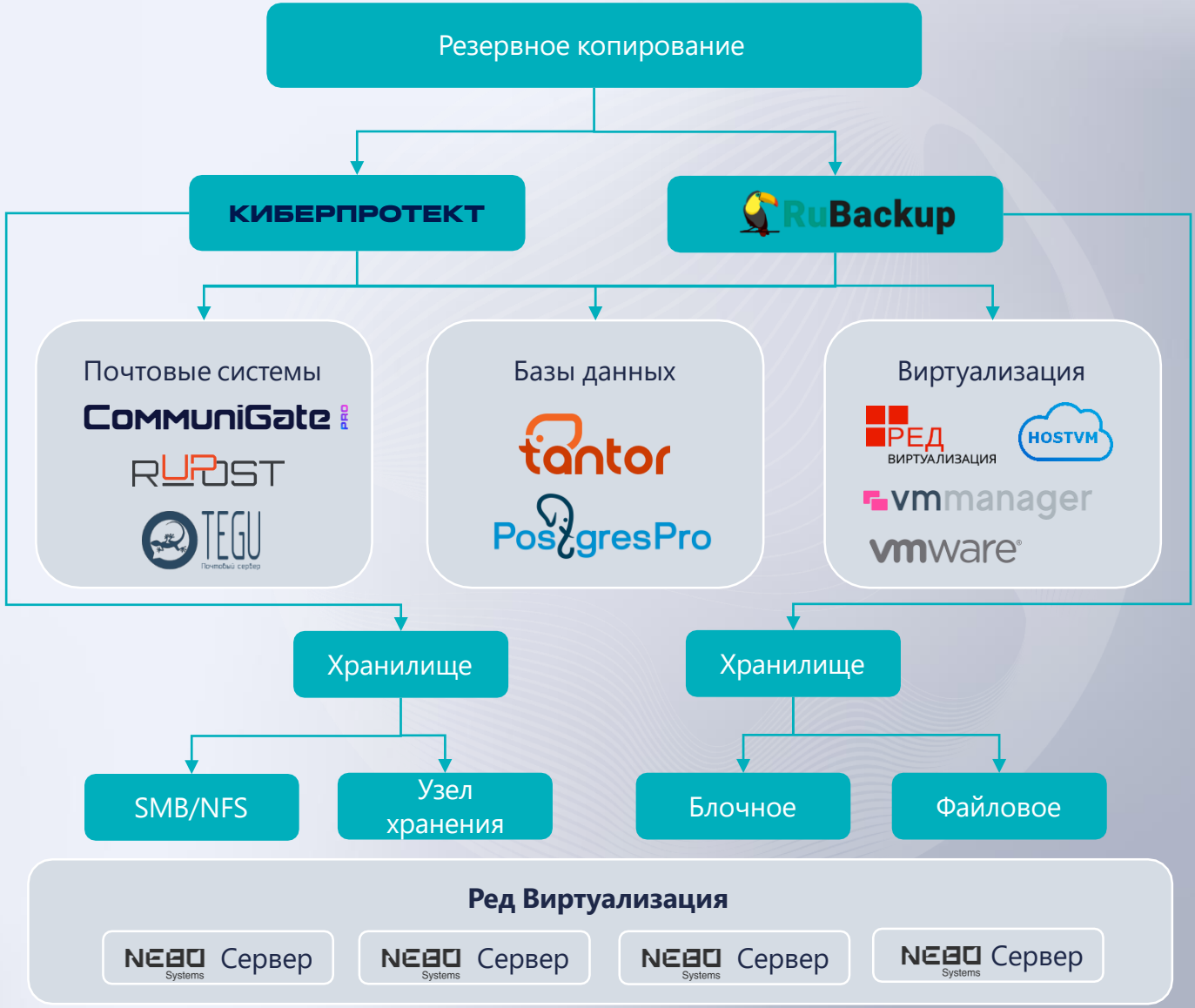
Так как не существует средств и методов конвертации резервных копий из зарубежных решений в отечественные, возникает обязательная необходимость поддержания «старой» системы резервного копирования параллельно с «новой» в режиме хранения и восстановления резервных копий.

Стенд: Системы Резервного Копирования

Централизованные системы Резервного Копирования:

- Поддержка отечественных систем виртуализации.
- Гранулярная работа с почтовыми серверами.
- Отказоустойчивые решения.
- Работа с Postgres и его производными.
- Продукты из реестра.

- Полностью российский софт и железо
- Решения сертифицированы ФСТЭК*
- Подходит для КИ и компаний с гос. уч.



Отечественное программное обеспечение

Полный цикл внедрения продуктов

ПРЕСЕЙЛ

Проводится профильной командой.

ДЕМОНСТРАЦИЯ

Демостенд наполненный данными и сценариями использования.

ПИЛОТЫ

Возможность проведения базового или расширенного по функционалу пилотного проекта.

АУДИТ И РАЗРАБОТКА АРХИТЕКТУРЫ

Аудит существующей инфраструктуры. Проектирование инфраструктуры. Разработка различной документации к проекту.

ВНЕДРЕНИЕ

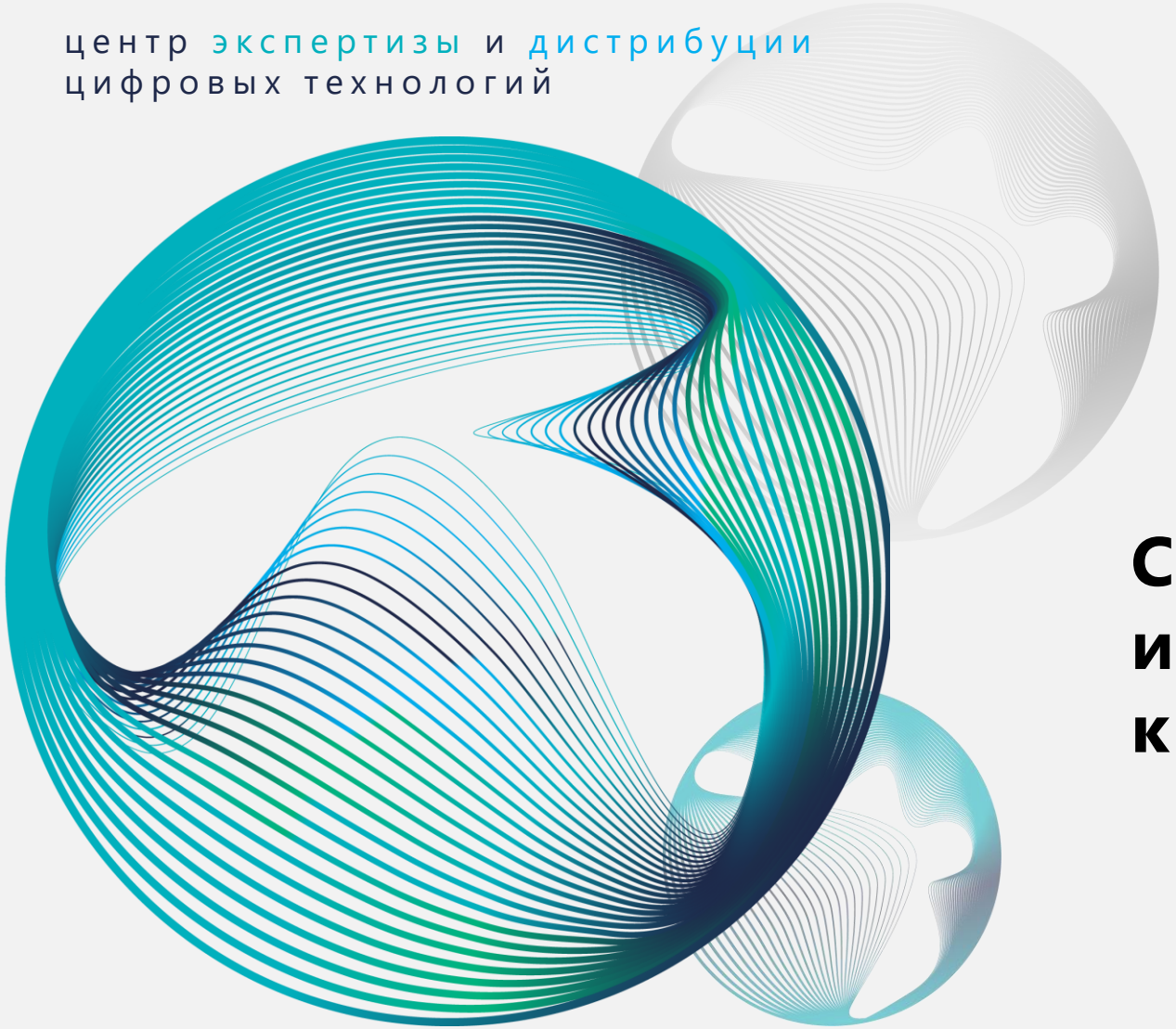
Берёмся за сложные, комплексные проекты с внедрением сразу нескольких продуктов.

СОПРОВОЖДЕНИЕ

Поддерживаем систему после внедрения и оказываем первую линию технической поддержки.

AXOFT

центр экспертизы и дистрибуции
цифровых технологий



Спасибо за внимание
и успехов на пути
к цифровому суверенитету!