Ростелеком
ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ

Технологическая импортонезависимость

Облако КИИ

Решение для объектов критической информационной инфраструктуры

Забродин Алексей
Технический директор

Что такое Облако КИИ

Облако КИИ — это управляемая облачная инфраструктура, полностью отвечающая требованиям приказа ФСТЭК № 239 (для объектов II категории значимости). Обеспечивает легкое масштабирование и предоставляется как услуга.

Облако КИИ сочетает в себе вычислительные мощности, сети и системы хранения данных. Обеспечивает заданный уровень надёжности и безопасности.

Законодательство в сфере безопасности КИИ

Федеральный закон №187-ФЗ от 26.07.2017

«О безопасности КИИ РФ»

Федеральный закон №193-ФЗ от 26.07.2017

«О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ «О безопасности КИИ РФ»

Федеральный закон №194-ФЗ от 26.07.2017

«О внесении изменений в УК РФ и УПК РФ в связи с принятием ФЗ «О безопасности КИИ РФ»

Указ Президента РФ №569 от 25.11.2017

«О внесении изменений в Положение о ФСТЭК»

Приказ ФСТЭК России №227 от 06.12.2017

«Об утверждении Порядка ведения реестра значимых объектов КИИ РФ»

Приказ ФСТЭК России №229 от 11.12.2017

«Об утверждении формы акта проверки, составляемого по итогам проведения госконтроля в области обеспечения безопасности значимых объектов КИИ РФ»

Приказ ФСТЭК России №235 от 21.12.2017

«Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»

Приказ ФСТЭК России №236 от 22.12.2017

«Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости»

Приказ ФСТЭК России №239 от 25.12.2017

«Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»

Постановление Правительства РФ №127 от 08.02.2018

«Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»

Постановление Правительства РФ №162 от 17.02.2018

«Об утверждении Правил осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ»

Указ Президента РФ №166 от 30.03.202

«О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры РФ»

Постановление Правительства РФ от 20.12.2022 №2360

«Изменения в правилах категорирования ОКИИ и перечне показателей критериев значимости»

Законопроект №390902-8 от 28.06.2023

«О внесении изменения в статью 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»

Постановление Правительства РФ №1912 от 14.11.2023

«О порядке перехода субъектов КИИ РФ на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах КИИ РФ»

Постановление Правительства РФ от 20.12.2022 №2360

- создание перечней типовых отраслевых объектов КИИ
- обязанность мониторинга и проверок субъектов КИИ

Законопроект №390902-8 от 28.06.2023

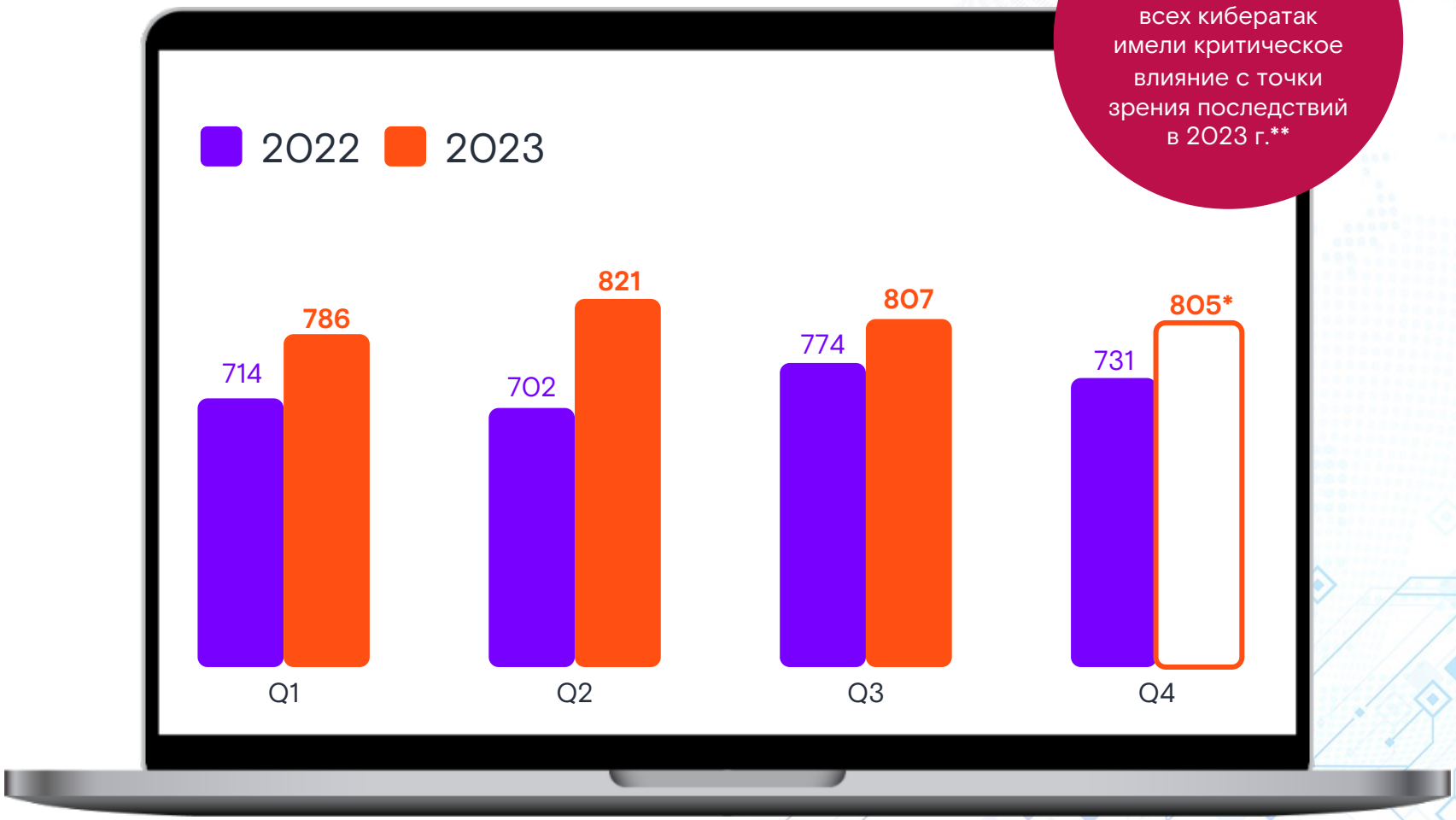
- расширение перечня субъектов КИИ
- добавление Образования и Социального обеспечения

Постановление Правительства РФ №1912 от 14.11.2023

- Переход к использованию доверенных ПАКов на объектах КИИ до 1 января 2030 года
- С 1 сентября 2024 года не допускается использование ПАКов, не являющихся доверенными, за исключением случаев отсутствия произведенных в РФ аналогов

Вызовы: рост угроз ИБ и импортозамещение

22%
всех кибератак имели критическое влияние с точки зрения последствий в 2023 г.**



Количество значимых кибератак в 2022 и 2023 годах (по кварталам)

▪ прогноз (официальных данных нет)

*по информации Positive Technologies.

**по информации МТС RED.

Россия оказалась в пятерке стран, которые за последний год чаще других подверглись кибератакам. В 2023 году было совершено 6 000 атак только на объекты КИИ, в основном на государственные, промышленные и финансовые организации и предприятия. Ежедневно более 170 кибератак направлено на российские компании с целью дестабилизировать их деятельность.

В 2023 году в публичный доступ попали данные почти 400 российских компаний и более 220 млн телефонных номеров российских абонентов. В прошлом году хакерские атаки на российские структуры отличались деструктивным характером: атаки были нацелены на то, чтобы вывести из строя инфраструктуру объекта и уничтожить данные. По оценке экспертов, этот тренд сохранится в 2024 году.

Распределение организаций-жертв по отраслям:
Госучреждения — 25%
Промышленность — 24%
Финансы — 12%

Состояние рынка

Неготовность к реализации требований

01 Реестр КИИ является неполным, так как не все организации* предоставили данные о своих информационных системах

02 Большое количество организаций* до сих пор не приняло всех необходимых мер для обеспечения безопасности объектов КИИ

03 Ужесточение законодательства в части расширения требований по защите объектов КИИ

Необходимость в модернизациях

01 Сложный, трудоемкий и затратный процесс создания Облака КИИ

02 Нехватка внутри организаций специалистов, готовых реализовать необходимый перечень работ для выполнения требований для КИИ

03 Технический долг компаний не позволяет своевременно выполнить требования для ОКИИ

* Государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, относимые к объектам КИИ.

* Государственные компании из перечня №91-р и их дочерние компании, если прямая или косвенная доля участия в их уставных капиталах превышает 50%

Облако КИИ «Ростелеком-ЦОД»: что вы получите?

Аттестованную инфраструктуру

Соответствует требованиям приказа ФСТЭК №239 на уровне IaaS и PaaS. С ней вы сможете пройти проверку регуляторов

Подбор, настройку и администрирование

средств защиты для вашей ИС КИИ

Услуги в рамках IaaS и PaaS

- Вычислительные ресурсы и ресурсы хранения данных
- Платформенные сервисы
- Управляемые кластеры контейнеров
- Защищенное размещение криптографического оборудования
- Резервное копирование
- ПО и программно-аппаратные комплексы (ПАК)
- Информационная безопасность с учетом требований к ОКИИ
- Конфигурирование и сопровождение
- Основная и резервная площадка ЦОД

Помощь в подготовке документов

для контролирующих органов: модель угроз, технический проект, организационная документация

Отказоустойчивое и катастрофоустойчивое облако

на базе отечественного оборудования и ПО с вендорской поддержкой и заданным уровнем обслуживания

Основные отличия Облака КИИ «Ростелеком-ЦОД»

	Облако КИИ	Облака на рынке
Серверы	РФ	Импорт
Сетевое оборудование	РФ	Импорт
Виртуализация	РФ	Импорт
Операционная система	РФ	Импорт
Платформенное ПО	РФ	Импорт
Система управления инфраструктурой / облачная платформа	РФ	Импорт
Системы хранения данных	РФ	Импорт и РФ
Приложения	РФ	Импорт и РФ
СКУД	РФ	Импорт и РФ
Инженерная инфраструктура ЦОД	Импорт и РФ*	Импорт и РФ
Оборудование СЗИ	РФ	Импорт и РФ
Средства СКЗИ	РФ	Импорт и РФ

*к инженерной инфраструктуре ЦОД не применяются требования к импортозамещению

Зоны ответственности

Клиент

Выбор категории ОКИИ

Своевременное предоставление сведений:

- о результатах присвоения объекту КИИ одной из категорий значимости
- об отсутствии необходимости присвоения ему одной из таких категорий

Исполнитель

Предоставление инфраструктуры для размещения объектов КИИ

Обеспечение мониторинга событий ИБ, своевременное реагирование на инциденты

Взаимодействие с НКЦКИ[1] по передаче инцидентов информационной безопасности, событий и проведение расследований, связанных с ними

Подключение к ГосСОПКА[2] (обмен информацией об инцидентах)

Контроль настроек ПО СЗИ, соответствие актуальным требованиям нормативной документации, регулярное проведение аудита настроек и версионности ПО и средств защиты информации

1. Национальный координационный центр по компьютерным инцидентам.

2. ГосСОПКА — государственная система предупреждения, обнаружения и ликвидации последствий компьютерных атак на критическую информационную инфраструктуру (КИИ) Российской Федерации.

Ценность для заказчика

Соблюдение законов и требований регуляторов к объектам КИИ

Сервисная модель получения инфраструктуры для КИИ. Отсутствуют единовременные затраты

Готовность к полному импортозамещению [1]

Готовность к ужесточению требований регулятора

Повышение безопасности размещенных информационных систем

Существенное сокращение рисков предписаний и санкций со стороны регуляторов

1. В рамках Указа Президента РФ № 250 с 1 января 2025 г. запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними.

Облако КИИ — беспрецедентный уровень сервиса

Предоставление услуги

24x7x365

Выделенная команда службы эксплуатации специалистов, размещенных непосредственно на площадке ЦОД

Уровень доступности

> 99,982 %*

Не более 6 технологических окон за квартал

Максимальная длительность технологического окна — не более 3 часов

* При использовании основной и резервной площадок

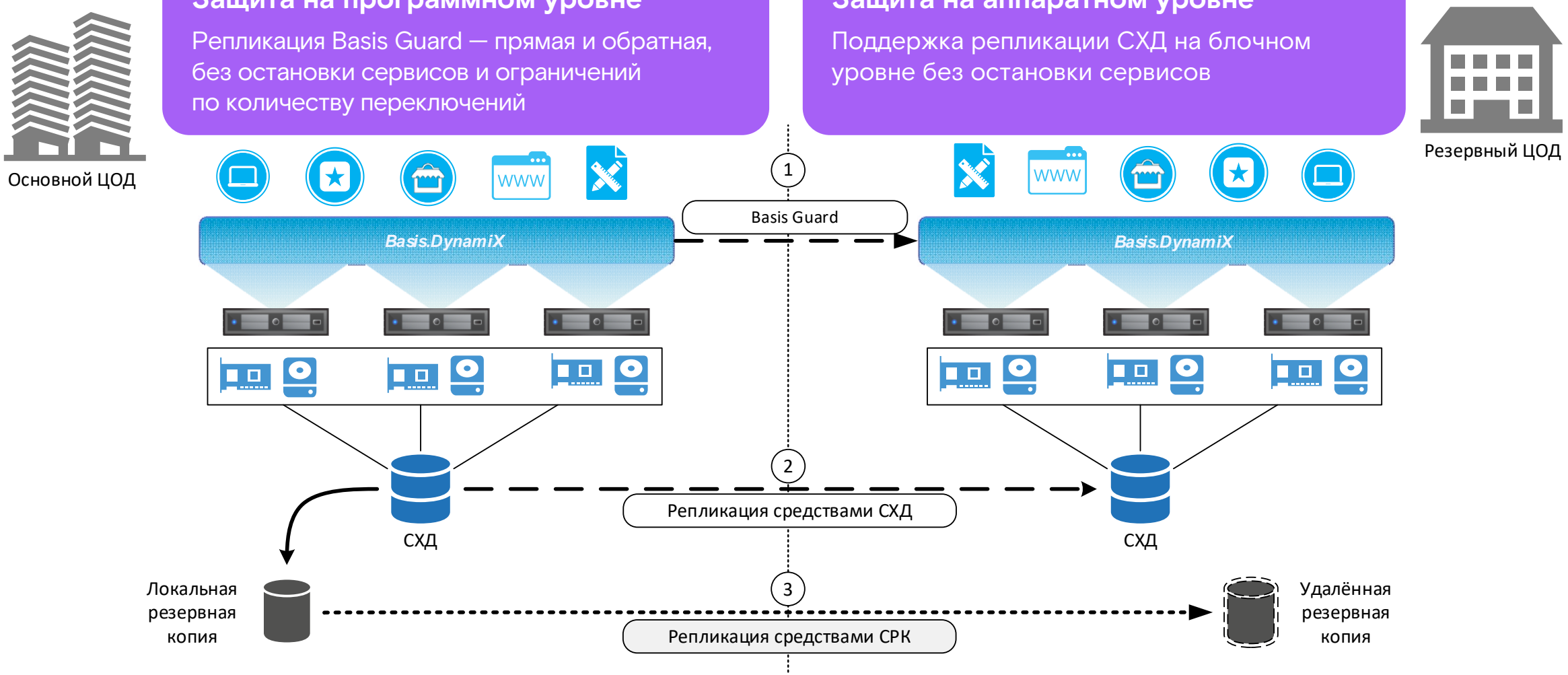
Отечественные решения катастрофоустойчивости

Защита на программном уровне

Репликация Basis Guard — прямая и обратная, без остановки сервисов и ограничений по количеству переключений

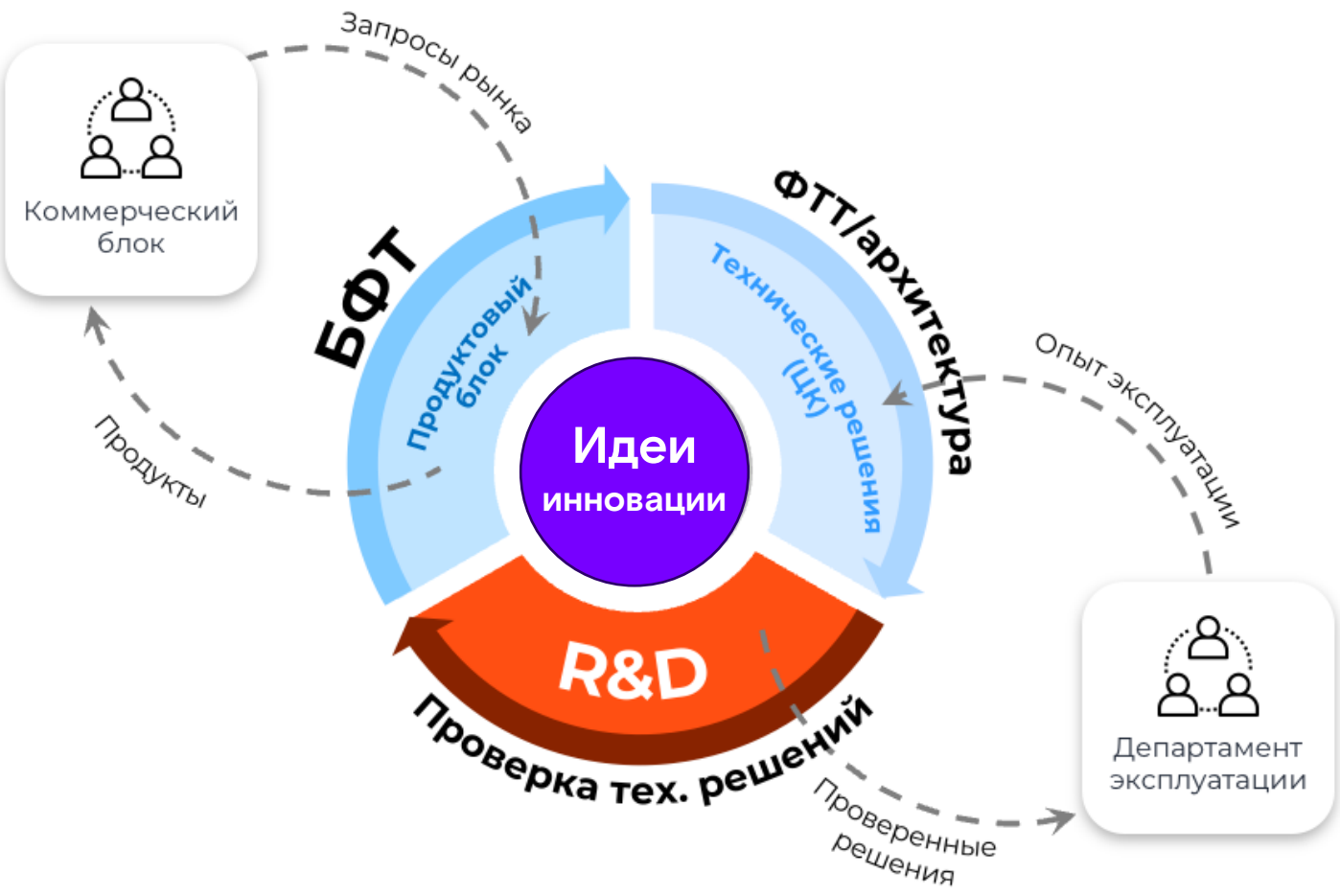
Защита на аппаратном уровне

Поддержка репликации СХД на блочном уровне без остановки сервисов



Бесшовная миграция ИС с инфраструктуры заказчика (Bare Metal, VMware, KVM, XEN, Hyper-V) в Облако КИИ (Базис.DynamiX)

Тестирование новых версий и решений



Работаем на опережение
Всегда в поиске новых решений

Являемся крупнейшей в РФ фабрикой по тестированию отечественных решений

- Созданы выделенные стенды, построенные на импортонезависимом оборудовании
- Проведено более **50** комплексных исследований в 2023 году
- Разработаны регламенты и ПМИ для проверки оборудования и ПО перед переводом в промышленную эксплуатацию
- Выстроен непрерывный процесс повышения надежности технических решений

Готов ответить на ваши вопросы

Забродин Алексей

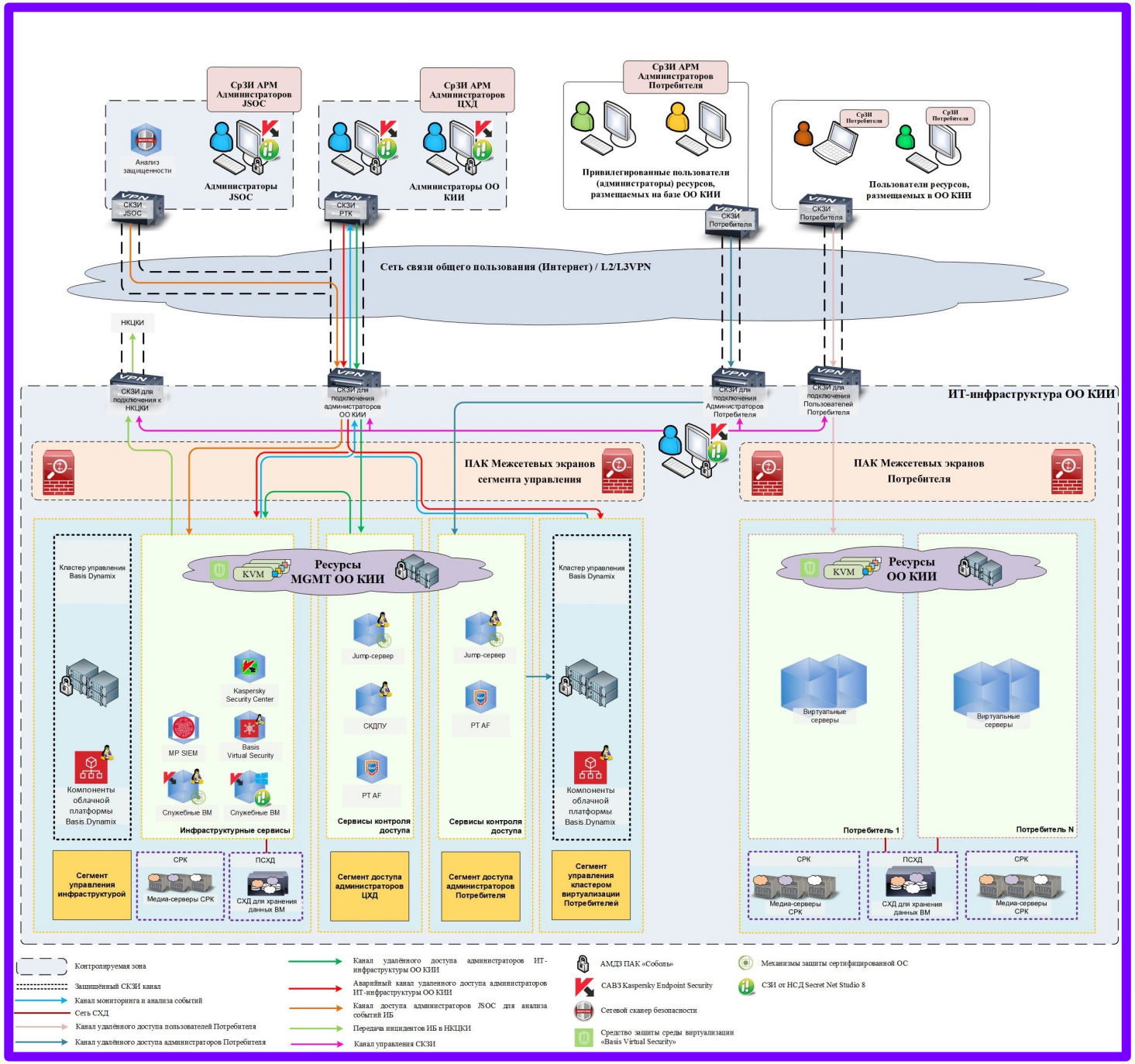
Технический директор

+7 (985) 774-65-45

Приложения

Ростелеком
ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ

Функциональная схема облака КИИ



Важные изменения

В 2023 году вышел законопроект №390902-8 «О внесении изменения в статью 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» об уточнении перечня субъектов КИИ, включающий еще две отрасли:

14.11.2023 вышло Постановление Правительства РФ №1912 «О порядке перехода субъектов критической информационной инфраструктуры РФ на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах КИИ РФ»:

- Переход к использованию доверенных ПАК на объектах КИИ до 1 января 2030 года
- С 1 сентября 2024 года не допускается использование ПАК, не являющихся доверенными, за исключением случаев отсутствия произведенных в РФ аналогов

Также утверждено Постановление Правительства РФ от 20.12.2022 № 2360 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127», определившее создание перечней типовых отраслевых объектов КИИ и обязанность мониторинга предоставления актуальных и достоверных сведений и проверок в отношении субъектов КИИ, подведомственных государственным органам и российским юридическим лицам

Основные отличия облачных платформ «Ростелеком-ЦОД»

	Облако КИИ	Облака на рынке
Обнаружение и предотвращение компьютерных атак	✓	✓
Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	✓	✓
Антивирусная защита	✓	✓
Защита периметра информационной системы (ИС) при взаимодействии с другими ИС и телекоммуникационными сетями	✓	✗
Исключение возможности отрицания пользователем факта отправки или получения информации	✓	✗
Контроль использования интерфейсов ввода и вывода информации на машинные носители информации	✓	✗
Поиск и получение обновлений программного обеспечения от доверенного источника	✓	✗
Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций (георезервирование ИС)	✓	✗
Центр мониторинга ИБ, подключение к ГосСОПКА	✓	✗
Обучение персонала правилам безопасности и информирование об угрозах ИБ	✓	✗
Планирование и отработка действий в нештатных ситуациях	✓	✗

Зоны ответственности

Клиент

Административная ответственность

Статья 19.7.15 КоАП РФ. Непредставление сведений, предусмотренных законодательством в области обеспечения безопасности КИИ РФ.

Административный штраф для должностных лиц в от 10 до 100 тыс. руб., для юридических лиц — от 50 до 500 тыс. руб.

Уголовная ответственность

Уголовная ответственность делится между клиентом и «Ростелеком-ЦОД» по результатам расследования, которое проводят уполномоченные органы власти

Исполнитель

Административная ответственность

Статья 13.12.1 КоАП РФ. Нарушение требований в области обеспечения безопасности КИИ РФ.

Административный штраф для должностных лиц от 10 до 50 тыс. руб., для юридических лиц — от 50 до 500 тыс. руб.

Уголовная ответственность

Статья 274.1 УК РФ. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ РФ, или ИС, ИТС, АСУ, сетей электросвязи, относящихся к КИИ РФ, либо правил доступа к указанным информации, ИС, ИТС, АСУ, сетям электросвязи, если оно повлекло причинение вреда КИИ РФ.

Принудительные работы на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового, либо лишение свободы на срок до 6 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового.

До 2023 года преобладали зарубежные решения

Средства ИБ:

FORTINET

ARBOR NETWORKS

CHECK POINT

ViPNet

Приложения: SAP, IBM, ORACLE, Microsoft, 1С

Система управления инфраструктурой / облачная платформа: Microsoft, vmware

Платформенное ПО: IBM, ORACLE, Microsoft

Операционная система: Microsoft

Виртуализация: Microsoft, vmware

Серверы: cisco, IBM

Системы хранения данных: NetApp

Сетевое оборудование: cisco, hp

Оборудование ИБ: FORTINET, ARBOR NETWORKS

Каналы и сеть: cisco, IBM

СКУД:

HID

Lenel United Technologies

Инженерная инфраструктура ЦОД: Schneider Electric

Зарубежное решение

Частично импортозамещено

Облако КИИ

Средства ИБ:

UserGate

Kaspersky OS

Код безопасности

Соболь

infotecs

Приложения: CommuniGate Pro Unified Communications Platform; МойОфис; Р7-ОФИС; TrueConf

Система управления инфраструктурой/ облачная платформа: BASIS

Платформенное ПО: SmartControl; RuBackup; КИБЕР Бэкап

Операционная система: Astra Linux; alt linux

Виртуализация: BASIS

Серверы: YADRO; AQUARIUS; kraftway Российские технологии

Системы хранения данных: YADRO

Сетевое оборудование: BH TECH

Оборудование ИБ: UserGate

Каналы и сеть: BH TECH

СКУД: BOLID Системы безопасности; SIGUR

Инженерная инфраструктура ЦОД: DKC; DEKraft; C3Solutions; ИМБИТ

История появления КИИ

1 января 2018 вступил в силу Федеральный закон «О безопасности критической информационной инфраструктуры РФ» от 26.07.2017 (№187-ФЗ)

Отрасли:

- Банковская сфера и другие сферы финансового рынка
- Топливно-энергетический комплекс
- Атомная промышленность
- Военно-промышленный комплекс
- Ракетно-космическая промышленность
- Горнодобывающая промышленность
- Металлургическая промышленность
- Химическая промышленность
- Наука, транспорт, связь, здравоохранение
- ЮЛ и ИП, которые обеспечивают взаимодействие объектов КИИ

Особенности облака КИИ

Аттестат соответствия требованиям к ОКИИ до II категории значимости

позволяет размещать в облаке информационные системы, которые относятся к значимым ОКИИ, с соблюдением всех требований регуляторов

Применение российских программных и аппаратных решений

позволяет выполнить предписания нормативных документов в части импортозамещения

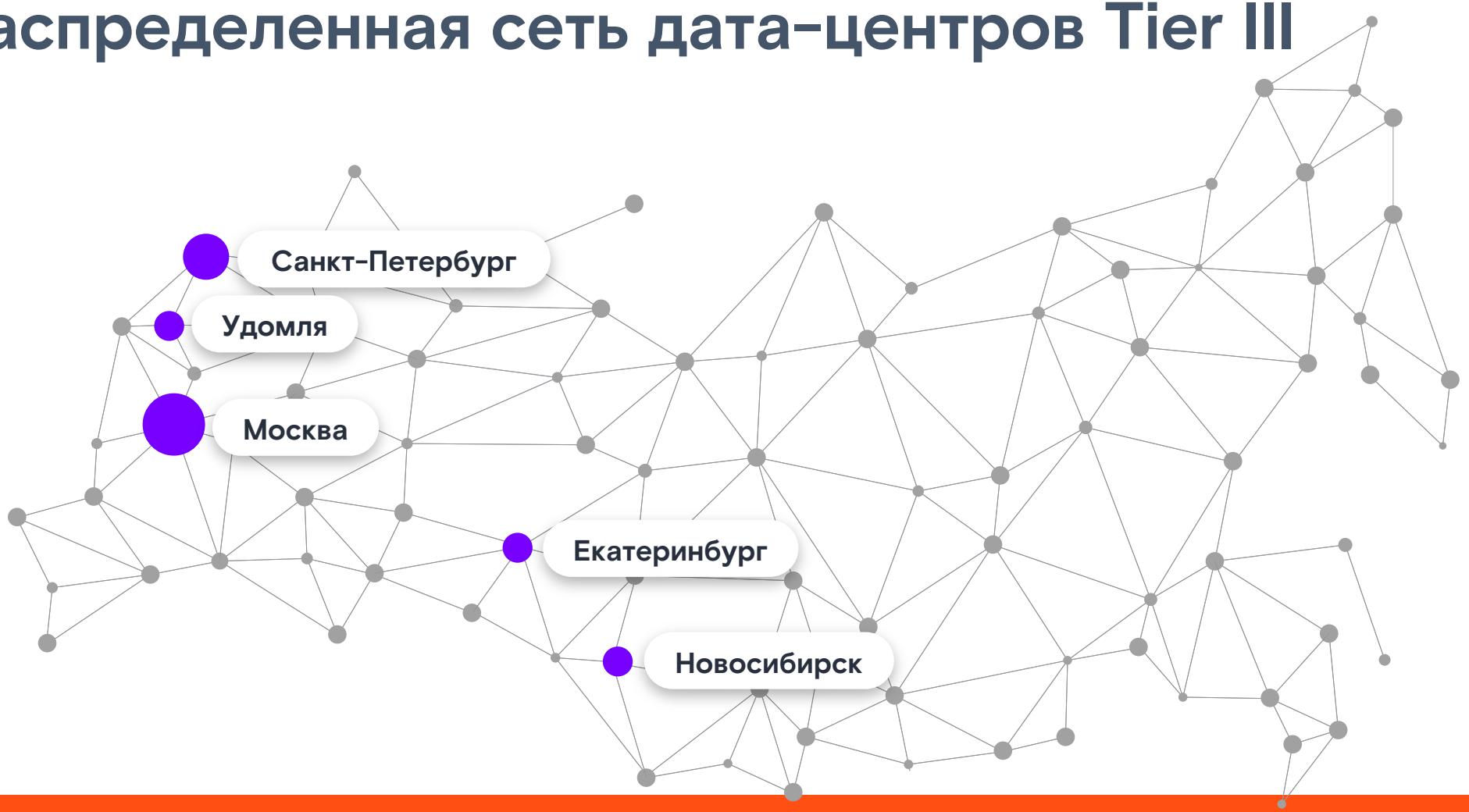
Дополнительные процедуры и меры защиты ОКИИ

- Управление обновлениями программного обеспечения
- Планирование мероприятий по обеспечению безопасности
- Планирование и отработка действий в нештатных ситуациях
- Аудит событий информационной безопасности
- Реагирование на ИТ-инциденты

Почему мы?

Ростелеком
ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ

Геораспределенная сеть дата-центров Tier III



22
дата-центр

20,5k
стоек

170 МВт
мощность

PCI DSS
на все дата-центры

Наши возможности

Мы создали и развиваем

- Крупнейшее публичное облако в РФ
- Инфраструктуру для электронного правительства РФ и «Гособлака»

Обслуживаем

150 000
виртуальных машин
в публичном облаке

2 900
корпоративных
и государственных заказчиков

85 000
рабочих мест
наших заказчиков

Сервис-провайдер ИТ полного цикла

От стандартных облачных сервисов до создания вертикально интегрированных специализированных решений под потребности заказчика

Решаем задачи любого уровня сложности в любом регионе

Доводим идеи до готового сервиса или экосистемы

Разрабатываем индивидуальные решения в кратчайшие сроки

Работаем с казначейским сопровождением в масштабных проектах

Облака

За 10 лет мы создали частные, общественные и публичные облака совокупной вычислительной мощностью

>540 000
виртуальных ядер

3 ПБ
оперативной памяти

109 ПБ
хранения

Наши клиенты

Государство

Генеральная прокуратура

Роспотребнадзор

МИД РФ

Минцифры РФ

Министерство просвещения

РосКапСтрой

ФГИС Моя Школа

Почта России

На базе облачной инфраструктуры «Ростелеком-ЦОД» была организована прямая линия с Президентом РФ.

Мы обеспечиваем цифровыми площадками крупные государственные проекты, такие как ЕГИСЗ, Система 112, Безопасный город, Росреестр и другие.

Корпоративные клиенты

Крупные промышленные корпорации

Транснефть

LUKOIL

Роснефть

Трансконтейнер

Россети

ВСК Страховой дом

Интер РАО

Хайлэнд Голд

Danone

Локо Тех

Финансовые институты

ВТБ

РСХБ

Home Credit Bank

Отличительные меры защиты в Облаке КИИ

Меры, реализуемые в Облаке КИИ (приказ ФСТЭК № 239),
в отличие от ГИС (приказ ФСТЭК № 17) и ИСПДн (152-ФЗ, приказ ФСТЭК № 21)

Контроль процессов ИБ

- Регламентация всех процессов ИБ
- Контроль данных, вводимых в информационную / автоматизированную систему
- Контроль настроек ПО СЗИ по актуальным требованиям нормативной документации
- Мониторинг событий ИБ, своевременное реагирование на инциденты

Предотвращение угроз ИБ

- Идентификация пользователей и инициируемых процессов
- Эшелонированная защита информационной / автоматизированной системы
- Обнаружение и предотвращение компьютерных атак
- Хранение и защита информации о компьютерных инцидентах
- Создание запасных мест хранения и обработки информации

Контроль инструментов ИБ

- Регулярный аудит настроек и версионности ПО
- Поиск и получение обновлений ПО от доверенного источника
- Контроль целостности обновлений ПО
- Тестирование обновлений ПО
- Установка обновлений ПО

Комплексные продукты для облака КИИ

Все продукты проходят всестороннее тестирование по строгим ПМИ

Продукты для Облака КИИ отрабатываются сначала в публичном облаке

Готовность к полному импортозамещению [1]

Готовность к ужесточению требований регулятора

Повышение безопасности размещенных информационных систем

Существенное сокращение рисков предписаний и санкций со стороны регуляторов

1. В рамках Указа Президента РФ № 250 с 1 января 2025 г. запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними.