TI Облако

Информационная безопасность из облака: преимущества и кейсы

Алексей Кубарев,
директор по информационной безопасности

Холдинг Т1

1992
Год основания

25 000+
Сотрудников

Крупнейшая
ИТ компания *

800+
проектов для государства и ключевых отраслей

222,9 млрд ₽
Оборот за 2023

Ключевые отрасли

- Государственный сектор
- Финансовый сектор
- Промышленность
- Коммуникации и медиа
- Топливно-энергетический комплекс
- Транспорт и логистика
- Ритейл и услуги

* По версии аналитических агентств CNews Analytics и RAEX

О компании

T1 Облако

4 дата-центра Tier-III

8+ лет на рынке облачных услуг

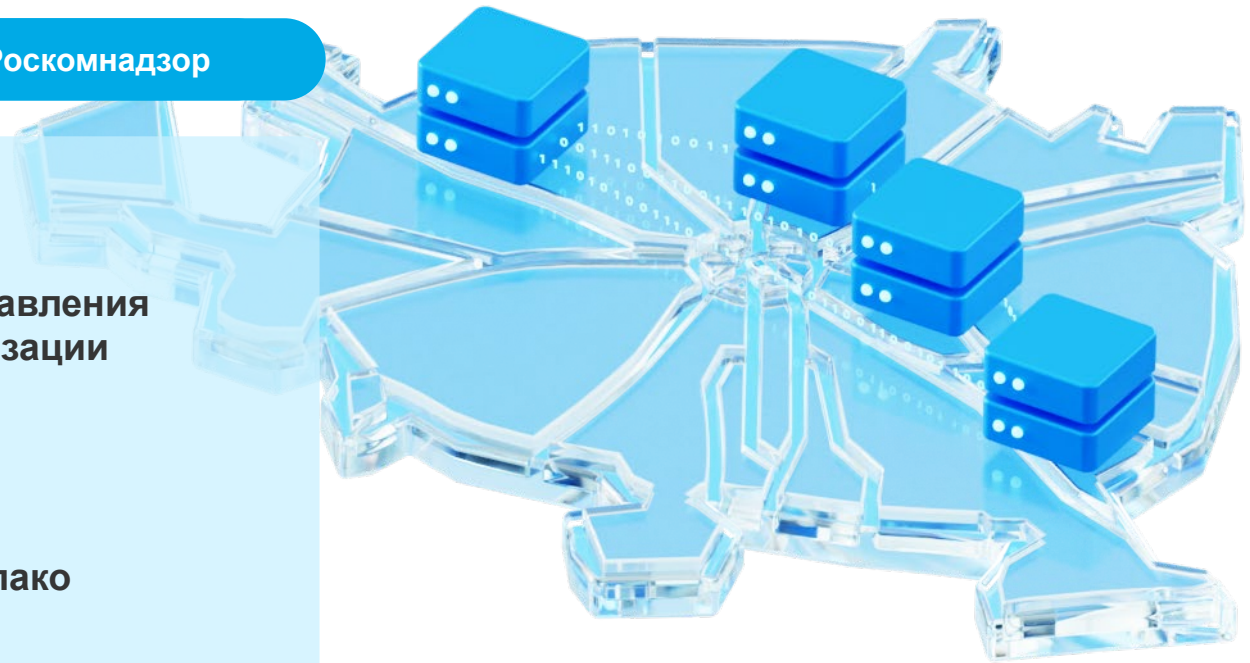
ТОП 5 облачных провайдеров Cnews Enterprise 2023

30+ облачных сервисов

ТОП 3 облачных провайдеров SLA IaaS***

IaaS провайдер 2023 года**

Лицензии: **ФСТЭК** • **ФСБ** • **Роскомнадзор**



Облачная платформа Т1 Облако* в Едином реестре российского ПО

Единый интерфейс управления платформами виртуализации OpenStack/VMware

Выбор модели внедрения
Публичные, частные, гибридные облака

Геораспределённое облако
Сетевая связность «из коробки»

*Свидетельство о регистрации ЕРРП № 11873 от 22.10.2021

8** По версии Cnews Awards 2023

8*** Ежегодный рейтинг SLA IaaS провайдеров

Модели реализации

TI Облако

Публичное облако

- Быстрый старт
- Доступ к ресурсам за несколько часов
- Доступные инструменты автоматизированной миграции в облако
- Компетентная техническая поддержка

Частное облако

- Индивидуальный подход
- Проведение аудита
- Разработка архитектуры
- Закупка оборудования
- Настройка, запуск и миграция облака
- Выделенная команда технической поддержки

Гибридное облако

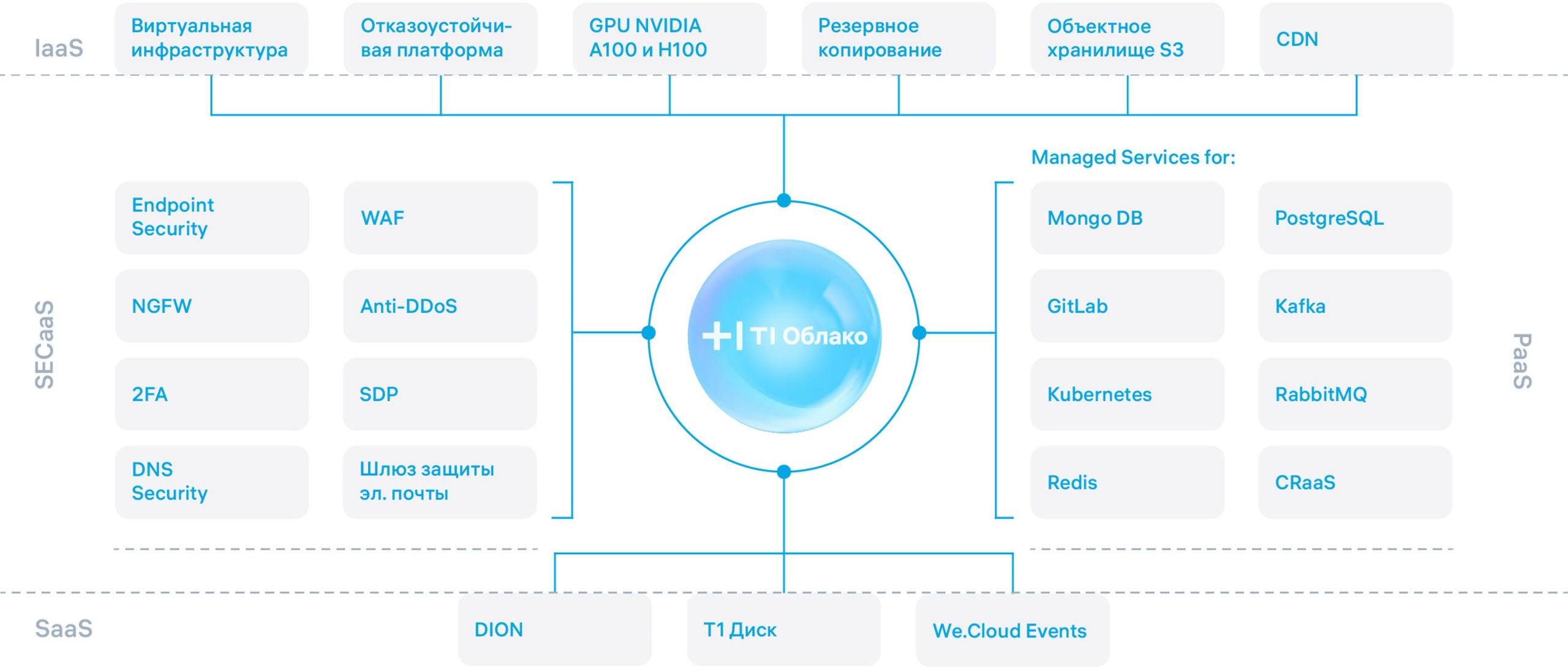
- Индивидуальный подход
- Проведение аудита ИТ-инфраструктуры
- Проработка облачной архитектуры
- Запуск и настройка
- Обучение сотрудников
- Компетентная техническая поддержка

Отчуждаемое облако

- Построение облака на ресурсах клиента
- Индивидуальный конструктор доступных сервисов
- Отечественная платформа виртуализации
- Настройка, запуск и миграция в облако
- Обучение сотрудников работе и самостоятельной поддержке облака
- Соблюдение повышенных требований ИБ

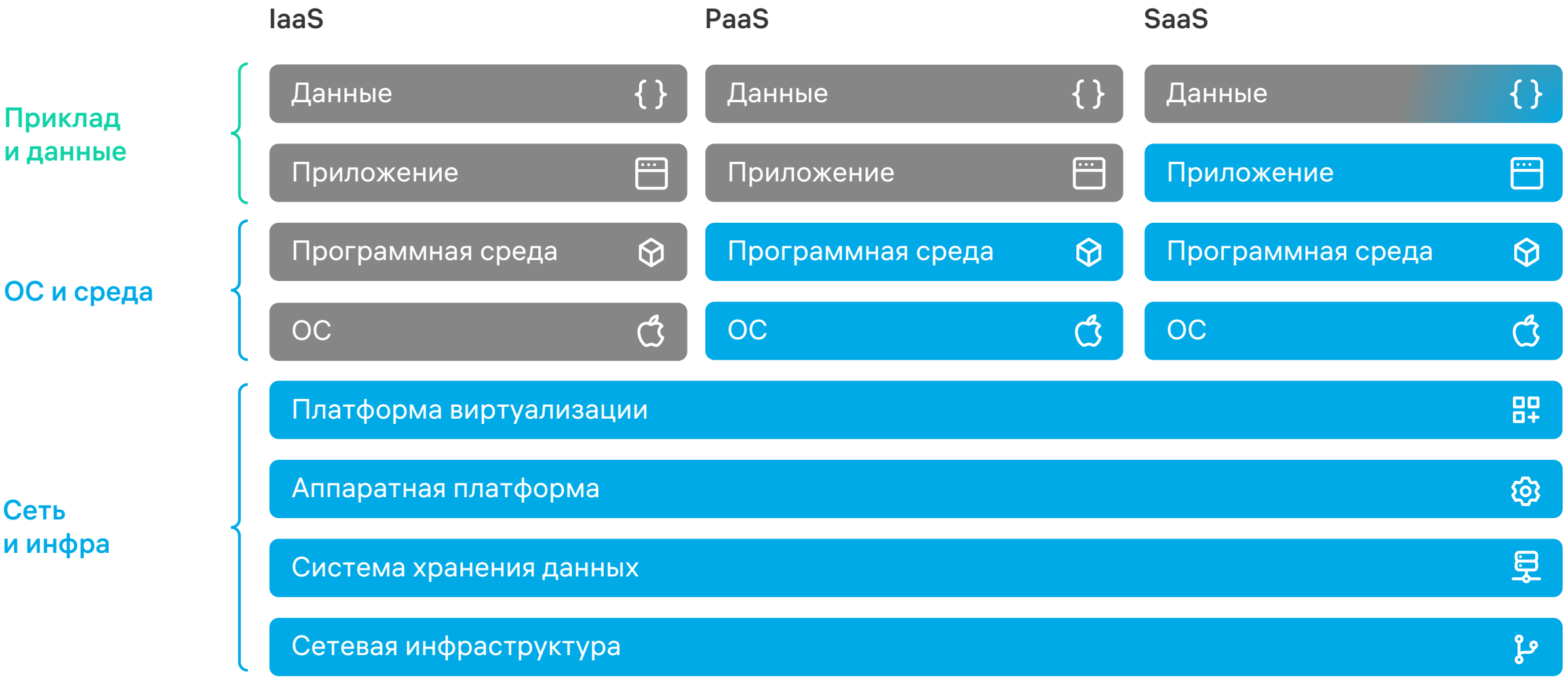
Ключевые сервисы

T1 Облако



Модели предоставления облачных услуг и ЗО

TI Облако



ИБ на разных уровнях инфраструктуры

TI Облако

Уровень приложения и данных

- ✓ Идентификация и аутентификация
- ✓ Регистрация событий безопасности
- ✓ Управление учетными записями и безопасностью

Уровень ОС и среды

- ✓ Идентификация и аутентификация
- ✓ Управление учетными записями
- ✓ и доступом
- ✓ Ограничение программной среды
- ✓ Ограничение аппаратной среды
- ✓ Регистрация событий безопасности
- ✓ Антивирусная защита
- ✓ Обнаружение и предотвращение сетевых компьютерных атак
- ✓ Межсетевое экранирование
- ✓ Резервное копирование и восстановление

Уровень сети и инфраструктуры

- ✓ Идентификация и аутентификация
- ✓ Управление учетными записями и доступом
- ✓ Защита информации при её передаче по каналам связи
- ✓ Ограничение программной среды
- ✓ Ограничение аппаратной среды
- ✓ Анализ защищенности
- ✓ Управление уязвимостями
- ✓ Регистрация событий безопасности
- ✓ Мониторинг информационной безопасности
- ✓ Антивирусная защита
- ✓ Обнаружение и предотвращение сетевых компьютерных атак
- ✓ Межсетевое экранирование
- ✓ Управление доступом к интернет-ресурсам
- ✓ Защита от DOS-атак
- ✓ Физическая защита
- ✓ Резервное копирование и восстановление
- ✓ Защита веб-приложений
- ✓ Защита от спама

Почему безопасность облака — это важно

TI Облако

Минимизация утечек

Минимизация простоев

Спокойствие за ИТ-системы

Упрощение аттестации

Что входит в состав облачных услуг?

TI Облако

Физическая защита оборудования (СКУД, видео и т. д.)

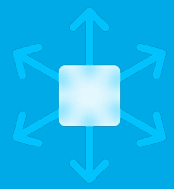
Георезервирование

Резервирование каналов связи

Повышенный SLA

Круглосуточный мониторинг

Меры защиты на уровнях в рамках ЗО



Повышенные компетенции в применяемых ИТ

Регуляторные ограничения отсутствуют

TI Облако

Информационн
персональных

Автоматизиро
финансовых ор

омационной

ства

Законопроект

№ 404786-8

О внесении изменений в отдельные законодательные акты Российской Федерации
(в части совершенствования правовых основ для аутсорсинга информационных технологий и использования облачных услуг финансовыми организациями)

НА РАССМОТРЕНИИ

Паспортные данные

Субъект права законодательной инициативы	**Депутаты Государственной Думы А.Г.Аксаков, А.Н.Свистунов, О.В.Савченко, О.Д.Димов, А.В.Терентьев, В.С.Макаров, И.Н.Бабич; Сенаторы Российской Федерации Н.А.Журавлев, М.М.Ульбашев, С.Н.Рябухин, А.Д.Артамонов, Д.И.Оюн, Т.А.Сахарова**
Форма законопроекта	**Федеральный закон**
Ответственный комитет	**Комитет Государственной Думы по финансовому рынку**
Комитеты-соисполнители	**Комитет Государственной Думы по информационной политике, информационным технологиям и связи**
Отрасль законодательства	**080.000.000 Финансы**
Тематический блок законопроектов	**Бюджетное, налоговое, финансовое законодательство**
Профильный комитет	**Комитет Государственной Думы по финансовому рынку**
Пакет документов при внесении	PDF

СТАДИИ РАССМОТРЕНИЯ

Защищённое публичное Т1 Облако

Т1 Облако

TIER III, георезерв (4 ЦОД)

Импортонезависимость

ИСПДн УЗ-1 (152-ФЗ)

ГОСТ 57580-1 УЗИ-1

PCI DSS 4.0

КИИ К3-1 (187-ФЗ), включено в реестр ЗО КИИ

ГОСТ 27017

ГОСТ 27018

Аттестация Т1 Облако на соответствие 187-ФЗ

Т1 Облако

Соответствие инфраструктуры публичного сегмента Т1 Облако законодательству Российской Федерации о безопасности критической информационной инфраструктуры по первой категории значимости

Аттестат подтверждает соответствие следующим НПА

- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
- Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127
- Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239
- Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом ФСТЭК России от 21 декабря 2017 г. № 235

Обеспечивает возможность размещения в облаке

- Информационные системы
- Автоматизированные системы управления
- Информационно-телекоммуникационные сети ЮЛ и ИП

Деятельность в сферах

- Финансовый сектор
- Энергетика
- Наука
- Связь
- Промышленность
- Транспорт
- Здравоохранение
- Гос. регистрация прав на недвижимое имущество

Надежный провайдер

TI Облако

Являемся субъектом КИИ и выполняем 187-ФЗ

Соответствуем ISO 27001 (СМК в области ИБ)

Имеем лицензию ФСТЭК России по ТЗКИ

Имеем лицензию ФСБ России по криптозащите несекретной информации

Имеем лицензии Роскомнадзора в сфере связи

Входим в реестр Роскомнадзора хостинг-провайдеров

Входим в реестр Роскомнадзора операторов персональных данных

Поставили свои информационные ресурсы под мониторинг ИБ ГосСОПКА

Сервисы информационной безопасности

TI Облако

Secure Development Platform

Платформа защищённой облачной разработки для Secure SDLC

Защита от DDoS-атак

Решение для защиты инфраструктуры и онлайн-ресурсов от всех видов DDoS-атак

Web App Firewall

Защита от атак на уязвимости в веб-приложениях

2-Factor Authentication

Двухфакторная аутентификация

Резервированный доступ

Резервированный доступ в Интернет обеспечивает отказоустойчивость соединения

Шлюз защиты эл. почты

Защита от атак при помощи электронного почтового обмена

Endpoint Security

Комплексная защита виртуальных машин

vNGFW

Сервис сетевой безопасности

Услуги по ИБ

TI Облако

Обследование

+ Определение состава ИС
+ Классификация ИС
+ Формирование ТЗ

Разработка СИБ

+ Моделирование угроз и нарушителя
+ Проектирование СИБ
+ Выбор оптимальных СЗИ

Внедрение

+ Закупка СЗИ
+ Монтаж и коммутация, установка СЗИ
+ Разработка ОРД

Аттестация

+ Анализ и устранение уязвимостей
+ Тестирование на проникновение
+ Подготовка подтверждающих документов

Сопровождение

+ Мониторинг ИБ
+ Управление СЗИ
+ Реагирование на инциденты ИБ

Аудит

+ Анализ уязвимостей
+ Пентест
+ Проверка осведомленности

ИБ на разных уровнях инфраструктуры (IaaS)

T1 Облако

Реализуется Т1 Облако на уровне инфры

Уровень сети и инфраструктуры

1. Идентификация и аутентификация (в том числе многофакторная) (ИАФ)
2. Управление учетными записями и доступом (УЗД)
3. Защита информации при её передаче по каналам связи (ЗКС)
4. Ограничение программной среды (ОПС)
5. Ограничение аппаратной среды (управление подключениями аппаратных средств) (ОАС)
6. Анализ защищенности (АНЗ)
7. Управление уязвимостями (УПУ)
8. Регистрация событий безопасности (РСБ)
9. Мониторинг информационной безопасности (МИБ)
10. Антивирусная защита (узлов, почты и сетевого потока) (АВЗ)
11. Обнаружение и предотвращение сетевых компьютерных атак (СОВ)
12. Межсетевое экранирование (МЕЭ)
13. Управление доступом к интернет-ресурсам (УДИ)
14. Защита от DOS-атак (ЗУО)
15. Физическая защита (ФЗЩ)
16. Резервное копирование и восстановление (РКВ)
17. Защита веб-приложений (ЗВП)
18. Защита от спама (ЗОС)

Реализуется Т1 Облако как сервис

Уровень ОС и среды

1. Идентификация и аутентификация (в том числе многофакторная) (ИАФ)
2. Управление учетными записями и доступом (УЗД)
3. Ограничение программной среды (ОПС)
4. Ограничение аппаратной среды (управление подключениями аппаратных средств) (ОАС)
5. Регистрация событий безопасности (РСБ)
6. Антивирусная защита (узлов) (АВЗ)
7. Обнаружение и предотвращение сетевых компьютерных атак (СОВ)
8. Межсетевое экранирование (МЕЭ)
9. Резервное копирование и восстановление (РКВ)

В зоне ответственности клиента

Уровень приложения и данных

1. Идентификация и аутентификация (в том числе многофакторная) (ИАФ)
2. Управление учетными записями и доступом (УЗД)
3. Регистрация событий безопасности (РСБ)

Микрокредитная организация без ИБ

TI Облако

Вводные:

Микрокредитная организация приняла решение разместить свою инфраструктуру в облаке

При этом требовалось выполнить требования по ИБ: законодательство о ПДн + законодательство о безопасности КИИ + ГОСТ 57580-1.

При этом в данной организации отсутствует необходимый штат специалистов по ИБ.

Результат:

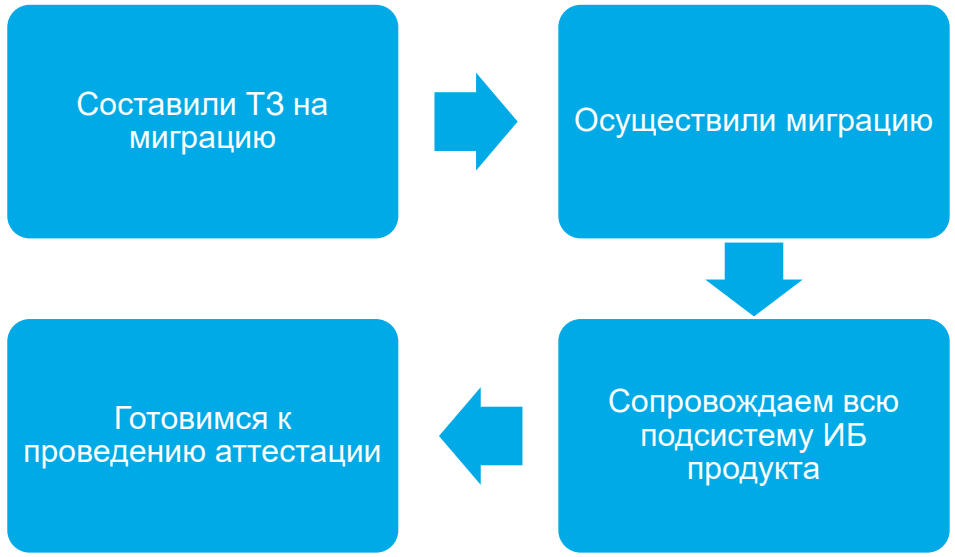
У вас так хорошо получается...

Вводные:
Основной цифровой продукт Клиента размещен в частном облаке, подсистема ИБ под нашим управлением.
Требуется оптимизировать затраты на инфраструктуру.

Задачи:

- Осуществить миграцию продукта из частного в публичное облако
- Оптимизировать систему ИБ продукта
- Минимизировать количество возможных точек отказа
- Соблюсти требования по информационной безопасности – ГОСТ 57580-1 и законодательство о ПДн.

T1 Облако



~ 60% - оптимизация затрат после миграции

- ✓ Заказчик планирует передачу Т1 Облако **сопровождение всех** подсистем ИБ, в т. ч. бэкофисных и размещенных локально;
- ✓ Заказчик планирует передачу Т1 Облако приведение в соответствие ГОСТ 57580-1 **всей ИБ** в т. ч. бэкофисных и размещенных локально.

Защищенный сайт для международного инвестиционного форума

TI Облако

Цель:

Обеспечение безотказного функционирования сайта международного форума

Задачи:

За 2 месяца обеспечить:

- Гибкую и отказоустойчивую инфраструктуру с гарантированно высоким уровнем доступности и безопасности
- Надежное размещение и бесперебойную работу портала в условиях пикового траффика
- Высокую пропускную способность сайта до 35 000 RPS
- Информационную безопасность интернет-портала: защиту от DDoS-атак и других вредоносных активностей до, в течение всей трансляции и 2 месяца после

Результат:

- ✓ **< 2** месяцев на подготовку инфраструктуры
- ✓ Обеспечена **непрерывная** доступность сайта
- ✓ Более **50 000** запросов в секунду пропускная способность при пиковых нагрузках.
- ✓ Организация усиленных мер безопасности обеспечила **безупречное качество онлайн-трансляции** в режиме реального времени без сбоев и задержек.
- ✓ Устойчивое функционирование под мощной **DDoS-атакой**

TI Облако

Спасибо за внимание!