

Криптошлюзы: комплексная защита сетевого периметра

Полный цикл услуг по построению защищенных каналов связи — от проектирования до внедрения и сопровождения.

Обеспечиваем не только формальное соответствие требованиям ФСТЭК, ФСБ и ЦБ РФ, но и реальное повышение безопасности бизнес-процессов за счет современных криптографических технологий.





Кто мы такие? О компании РДТЕХ

Наша миссия — обеспечение комплексной защищенности бизнеса клиентов в цифровой среде. Мы сочетаем глубокие экспертные знания в области законодательства и compliance в части ИБ с сильными проектными компетенциями.

Мы снижаем риски, обеспечивая соответствие требованиям регуляторов (152-ФЗ, ФСТЭК, ФСБ, ЦБ РФ) и строим эффективные процессы безопасности.

Наши ключевые компетенции в области ИБ



Архитектура, методология и стратегия внедрения криптошлюзов



Управление проектами и рисками



Нормативное соответствие (Compliance)



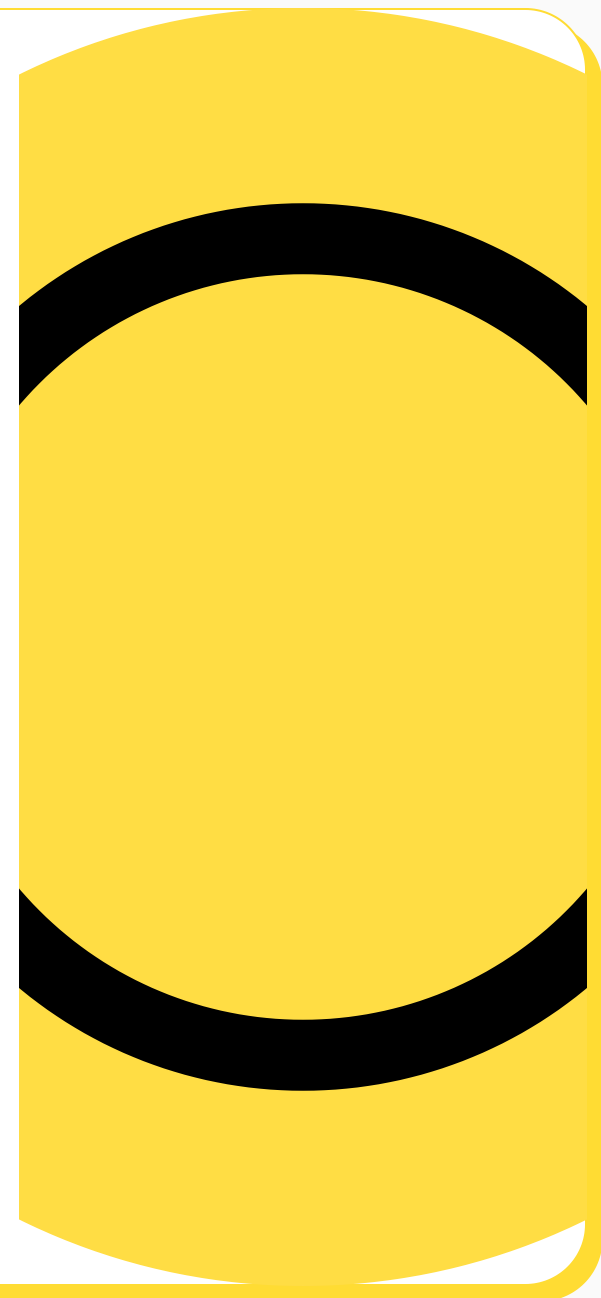
Обследование существующих решений



Сетевая безопасность



Инжиниринг и внедрение СЗИ



Функционал криптошлюзов

1

Безопасность трафика

- Организация защищенного туннеля
- Шифрование ГОСТ
- Расшифровка трафика
- Формирование и проверка подписи для пересылаемых данных
- Межсетевой экран

2

Доступ и управление

- Маршрутизация и NAT
- Контроль доступа
- Портал управления
- Централизованное управление и логирование

3

Для сложных инфраструктур

- Высокая отказоустойчивость и кластеризация
- Стабильная производительность решений

Государственное регулирование в части криптошлюзов

Для Критической ИИ (КИИ)

- **Документ:** Приказ ФСТЭК № 235, 239
- **Суть:** соответствие требованиям регулятора

Для ИСПДн (защита периметра)

- **Документ:** Приказ ФСТЭК № 17, 21, 152-ФЗ от 27.07.2006
- **Суть:** создание защищенных каналов связи для передачи и хранения данных

Для ИСПДн (шифрование)

- **Документ:** Приказ ФСБ № 378 от 10.07.2014
- **Суть:** Специальные требования для криптошлюзов

Для банковской сферы

- **Документ:** ГОСТ Р 57580.1-2017
- **Суть:** Базовая мера защиты для финансовых организаций

Для Критической ИИ (КИИ)

- **Документ:** Приказ ФСБ России о ГОССОПКА
- **Суть:** подключение к системе обнаружения, предупреждения и ликвидации последствий компьютерных атак

Для банковской сферы

- **Документ:** Положения Банка России: 382-П, 762-П
- **Суть:** Базовая мера защиты для финансовых организаций

Для ИСПДн (аттестат)

- **Тип:** Аттестат соответствия.
- **Куда:** Подается в Роскомнадзор (РКН)

Для ИСПДн (декларация)

- **Тип:** Декларация соответствия.
- **Куда:** Подается в Роскомнадзор (РКН)

Российские решения в проектах. S-terra

Модельный ряд ГОСТ криптошлюзов S-terra

- Модели и характеристики:
 - Шлюз 100 → до 10 туннелей, до 180Мбит/с
 - Шлюз 1000 → До 500 туннелей, 339Мбит/с
 - Шлюз 3000HE → До 1000 туннелей, до 2900 Мбит/с
 - •Шлюз 7000HE → Не ограничено туннелей, до 5 900 Мбит/с
 - Шлюз 8000HE → Не ограничено туннелей, до 7 700Мбит/с

📄 <https://www.s-terra.ru/products/catalog/s-terra-shlyuz-5-0/?tab=1>

Аппаратные криптошлюзы



Российские решения в проектах. S-terra DP

Аппаратные криптошлюзы

Модельный ряд ГОСТ криптошлюзов S-terra DP

- Модели и характеристики:
 - Шлюз 10G → Не ограниченно туннелей, до 16 730 Мбит/с
 - Шлюз 24G → Не ограниченно туннелей, до 26 000 Мбит/с
 - Шлюз 40G → Не ограниченно туннелей, до 47 980 Мбит/с
 - Шлюз 100G → Не ограниченно туннелей, до 105 047 Мбит/с

📄 <https://www.s-terra.ru/products/catalog/s-terra-shlyuz-dp-4-3/?tab=1>



Российские решения в проектах. S-terra виртуальный криптошлюз

Производительность криптошлюза:

- Характеристики:
 - Виртуальный Шлюз (1 ядро) → До 50 туннелей, до 280 Мбит/с
 - Виртуальный Шлюз (4 ядра) → До 200 туннелей, до 1015 Мбит/с
 - Виртуальный Шлюз (12 ядер) → До 1000 туннелей, до 2050 Мбит/с

📄 <https://www.s-terra.ru/products/catalog/s-terra-shlyuz-dp-4-3/?tab=1>

Российские решения в проектах. Код Безопасности (с МСЭ)

Классификация ГОСТ криптошлюзов по производительности

- Модели и производительность:
 - Континент 4 IPC-R50 → До 50 подключений, до 350 Мбит/с
 - Континент 4 IPC-R800 → До 800 подключений, До 5 Гбит/с
 - Континент 4 IPC-R5000 → До 3500 подключений, до 15,5 Гбит/с
 - Континент 3.9 IPC-3000FC-40G → До 40 Гбит/с

 <https://www.securitycode.ru/products/kontinent-4/>

Аппаратные криптошлюзы



Российские решения в проектах. VIPNet Coordinator HW 4 (с МСЭ)

Классификация ГОСТ криптошлюзов VIPNet по производительности

- Категории и производительность:
 - HW10 → До 500 подключений, до 35 Мбит/с
 - HW100C → До 1000 подключений, до 400 Мбит/с
 - HW1000D → До 10000 подключений, до 2500 Мбит/с
 - HW2000 → До 15000 подключений, до 6600Мбит/с
 - HW5000 → До 15000 подключений, до 10000Мбит/с

 <https://infotecs.ru/products/vipnet-coordinator-hw-4/>

Аппаратные криптошлюзы



Экспертиза нашей команды

Архитектор ИБ

- Разработка стратегии, модели угроз и нарушителя, соответствие ГОСТ, ФСТЭК, ФСБ. Управление комплексными программами ИБ.

Менеджер проектов

- Управление сроками, бюджетом (CAPEX/OPEX), рисками. Опыт внедрения единичных решений и крупных инфраструктур.

Методолог по СЗИ

- Разработка политик и регламентов. Аудит на соответствие ФСБ 378, Приказам ФСТЭК №17, 21, 235, 239, требованиям ЦБ РФ.

Специалист по сетевой безопасности

- Проектирование и аудит защищенных сетей (FW, FAW, сегментация, криптошлюзы), расследование инцидентов.

Инженер-проектировщик

- Проведение аудитов, разработка ТЗ, ТП, РД по ГОСТ. Внедрение и администрирование криптошлюзов NGFW.

Опыт: Кейс — Производственный сектор

Клиент: Крупная производственная компания

Проект: Модернизация криптографической
защиты каналов связи (КЗКС)

- Модернизация КЗКС корпоративной сети передачи данных (КСПД)
- Модернизация КЗКС основного центра обработки данных (ОЦОД)
- Расширение КЗКС на резервный центр обработки данных (РЦОД)

Результат: Создана единая защищенная среда передачи данных между всеми площадками компании, обеспечено соответствие требованиям ФСБ и ФСТЭК.



Опыт: Кейс — Финансовый сектор

Клиент: Финансовая компания

Проекты:

1. Обследование существующей инфраструктуры МСЭ и криптотунелей КСПД организованных на импортных решениях, разработка дорожно карты по импортозамещению.
2. Внедрение криптошлюзов с МСЭ для СПД: внедрение криптошлюзов с МСЭ отечественного вендора для защиты сети от внешних угроз, обеспечение сегментации СПД по доменам безопасности.

Результат: Комплексное приведение ИБ-инфраструктуры СПД в соответствие с требованиями ФСТЭК 17, 21.

Почему выбирают РДТЕХ?

Глубокие экспертные знания

В области нормативных требований

Проверенный опыт

Реализации проектов под ключ

Сильная команда

С покрытием всех ключевых требований в части криптошлюзов и МСЭ

Понимание бизнес-процессов

В различных отраслях (Финтех, ТЭК, Промышленность)

Технологический нейтралитет

Подбираем решения, исходя из задач
Заказчика





Next Steps / Контакты

Обсудим ваши задачи и построим дорожную карту внедрения решений ИБ, соответствующих вашей ИТ-стратегии и требованиям регуляторов.

Контактное лицо: Дорошенко Алексей Алексеевич

Должность: Директор проектного офиса



Alexey.Doroshenko@rdtex.ru