



РЕШЕНИЯ для ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ

Топливо-энергетическая отрасль государства является стратегически важной частью экономики. Последствия от действий злоумышленников в этой отрасли могут быть настолько глобальными, что стоимость их устранения может легко превысить совокупную стоимость отдельных энергетических компаний.

Поэтому отраслевые стандарты безопасности выдвигают весьма серьезные требования к ИБ. Учитывая специфику ТЭК, а именно – географическую распределенность объектов, одним из важнейших аспектов является обеспечение конфиденциальности и целостности информации при передаче по недоверенным каналам связи (например, по сети Интернет). Если в информационной системе обрабатывается информация, подлежащая обязательной защите в соответствии с российским законодательством (например, персональные данные – ПДн), то необходимо использовать сертифицированные средства защиты, прошедшие процедуру оценки регуляторами – ФСБ России и ФСТЭК России.

Российская компания «С-Терра СиЭсПи» предлагает высокопроизводительные, надежные и оптимальные по стоимости решения для защиты сетевого взаимодействия компаний ТЭК и т.п.

Преимущества решений С-Терра

1. **Легкая интеграция** в существующую сетевую инфраструктуру, благодаря использованию единых компонентов:

- система централизованного управления и мониторинга оборудования С-Терра КП;
- любой удостоверяющий центр, выпускающий ГОСТ-сертификаты (например, Microsoft CA с Крипто-Про CSP);
- Cisco-like интерфейс управления.

Таким образом, нет необходимости обучать или нанимать новых специалистов для поддержания работоспособности безопасности сетевой инфраструктуры.

2. **Использование мировых стандартов IKE/IPsec (RFC2401-2412)** обеспечивает отсутствие ошибок, связанных с дизайном протокола защиты. Архитектура IPsec проверена многократным техническим анализом и тестированием специалистами многих стран, и внедряется по всему миру, в том числе и в России.

3. **Отсутствие зависимости от поставщика оборудования.** Технология IPsec является унифицированным мировым стандартом. Поэтому, если в Вашей организации уже используется иностранное оборудование для защиты сетей, Вы сможете плавно и без лишних усилий перейти на соответствующие отечественным стандартам продукты С-Терра.

Более того, можно использовать уже имеющиеся в организации аппаратные платформы, установив на них ПО С-Терра VPN.

4. **Легитимность.** Продукты компании «С-Терра СиЭсПи» сертифицированы ФСБ России до классов КСЗ и МЭ4 включительно, а также ФСТЭК России по уровням МЭ 3, НСД 3, ОУД 4+, НДВ 3, АС 1В, ГИС до 1кл. вкл., ПДн 1-4 ур. Указанные уровни сертификации обеспечивают выполнение требований Российского законодательства по защите персональных данных: Федеральный закон №152 «О персональных данных» и Федеральный закон №149 «Об информации, информационных технологиях и о защите информации».

5. **Высокая экономическая эффективность продуктов.** Оптимальный функциональный состав решений С-Терра, а также использование международных технологических стандартов позволяет не только оптимизировать Ваши первоначальные затраты на приобретение, но и снизить стоимость обслуживания (ТСО). Стоимость лицензий зафиксирована в рублях и не зависит от курса доллара.

6. **Качественная, оперативная служба технической поддержки.** Выбрав решения С-Терра для решения задач информационной безопасности (ИБ), Вы не останетесь с ними «один на один»: наши специалисты всегда готовы Вас проконсультировать. Время реакции нашей службы технической поддержки - от 2 часов. В техническую поддержку может обратиться как конечный пользователь, так и партнер. Возможен выезд специалиста к Вам в офис. На все аппаратные платформы С-Терра предоставляется гарантия производителя не менее 3-х лет. Некоторые платформы поставляются на условиях безусловной оперативной замены в случае выявления неисправности (в течение срока гарантии).

Решения С-Терра для различных задач ТЭК

Таблица 1. Сводная таблица решений С-Терра для ТЭК

Решения С-Терра	Продукты С-Терра	Описание
Задача:	<u>Защита взаимодействия между офисами</u>	
<u>Защита корпоративной сети</u>	• С-Терра Шлюз • С-Терра Виртуальный Шлюз • Модуль Cisco CSCO-STVM	Защита любого сетевого трафика при передаче по недоверенным каналам связи. Широкая линейка продуктов в различных форм-факторах, масштабирование производительности.
Задача:	<u>Удаленный доступ сотрудников, работающих вне офиса</u>	
<u>Защита удаленного доступа</u>	• С-Терра Клиент • С-Терра Клиент-М	Удаленный доступ сотрудников через интернет с помощью программного клиента для различных ОС.
Задача:	<u>Защита взаимодействия компонентов АСУ ТП</u>	
Защита АСУ ТП	• С-Терра Шлюз	Компактный С-Терра Шлюз на защищенной аппаратной платформе.
Задача:	<u>Защита взаимодействия с ЦОД или между ЦОД</u>	
<u>Защита канала 10Gb</u>	• С-Терра Шлюз • С-Терра Шлюз 10G	Защита канала 10G с помощью одной пары шлюзов. Использование кластера мощных шлюзов.

Защита взаимодействия между офисами

Защита взаимодействий территориально-распределенных подразделений и офисов – типовая задача для продуктов С-Терра, многократно проверенная нашими заказчиками.

В каждом таком подразделении компании или её дочерней структуры устанавливается криптошлюз, реализующий IPsec VPN ГОСТ и межсетевое экранирование. Благодаря широкой линейке продуктов С-Терра, можно подобрать подходящее устройство для решения любой задачи, с любой требуемой скоростью передачи данных. В том числе, имеется возможность встраивания в маршрутизаторы Cisco.

Для повышения отказоустойчивости канала связи с критически важными объектами в продуктах С-Терра поддерживается кластеризация.

Удаленный доступ сотрудников

Темпы развития современного бизнеса требуют оперативной реакции на запросы. Для этого сотрудникам необходим доступ к корпоративным ресурсам, где бы они ни находились – дома, в командировке или в отпуске. При этом, они осуществляют доступ к корпоративным ресурсам через Интернет, который является недоверенной сетью.

Для того, чтобы снизить риски и обеспечить конфиденциальность и целостность передаваемых данных, непосредственно на устройство пользователя устанавливается VPN-клиент С-Терра:

- а) [С-Терра Клиент](#) – для ОС Windows;
- б) [С-Терра Клиент-М](#) – для ОС Android.

В точке подключения клиентов к корпоративной сети (например, в головном офисе) устанавливается [С-Терра Шлюз](#).

Защита взаимодействия компонентов АСУ ТП

В контексте сетевой защиты автоматизированных системы управления на первом месте находится целостность данных (передаваемых команд) и аутентификация абонентов. При этом важна надежность средств защиты и прозрачность для прикладных систем. Прозрачность подразумевает задержку, которая не влияет на функционирование системы, и отсутствие необходимости модификации сети.

Для обеспечения аутентификации, целостности и конфиденциальности передаваемых данных на объекты устанавливается [С-Терра Шлюз](#) в компактном исполнении. Он позволяет защитить взаимодействия компонентов АСУ ТП, информационно-измерительные системы учёта, систем контроля доступа и т.п.

Защита взаимодействия ЦОД

Одним из современных трендов в бизнесе является централизация ИТ-ресурсов. При этом, появляется задача защиты высокоскоростных каналов связи между офисом и центром обработки данных (ЦОД), а также между основным и резервным ЦОДами.

Распространенные заблуждения о том, что оптические каналы связи не требуют защиты, и что отсутствуют отечественные средства криптографической защиты для обеспечения скорости шифрования 10Гб/с и выше, очень легко опровергнуть.

Во-первых, устройства съема информации с оптических каналов значительно снизились в цене и могут быть свободно приобретены за 100-300\$, что существенно расширяет возможности злоумышленников и свидетельствует о том, что оптические каналы связи нужно защищать точно так же, как и любые другие.

Во-вторых, производительность устройства С-Терра Шлюз 10G на смешанном трафике достигает 10Гб/с, при этом в продуктах С-Терра для шифрования используется ГОСТ28147-89. Данный продукт является уникальной разработкой компанией «С-Терра СиЭсПи» и базируется на высокопроизводительной аппаратной платформе и ПО С-Терра Шлюз, специально оптимизированном для решения именно такой задачи.

Как результат, решение С-Терра защиту взаимодействия с ЦОД, используя всего **одну пару** устройств С-Терра Шлюз 10G, обеспечивает защиту канала связи с пропускной способностью 10Гб/с с IMIX трафиком.

Для обеспечения защиты более высокоскоростных каналов предусмотрено масштабирование решения до скорости 40G.

Наши клиенты

Пользователями решений С-Терра являются крупнейшие компании отрасли в частности СО ЕЭС, Газпромнефть, а также многие другие.

Приобретение решений

По всем вопросам, касающимся конфигурации системы ИБ и подбора продуктов для решения Ваших задач информационной безопасности обращайтесь к нашим менеджерам:

- по телефону +7 499 940-90-61
- или по почте sales@s-terra.ru