s•terra

РЕШЕНИЯ для ГОСУДАРСТВЕННОГО СЕКТОРА

Информационная безопасность в государственных организациях жёстко регламентирована нормативно-правовыми актами. Техническими регуляторами в отношении средств защиты информационной безопасности выступают ФСБ России и ФСТЭК России. Средства защиты, прошедшие процедуру подтверждения требованиям технических регламентов, получают сертификат соответствия и могут использоваться в государственных информационных системах.

Российская компания «С-Терра СиЭсПи» предлагает высокопроизводительные, надежные и оптимальные по стоимости решения для защиты сетевого взаимодействия в системе органов законодательной, исполнительной, судебной власти и местного управления на базе собственных продуктов С-Терра VPN – сертифицированных программных и программно-аппаратных комплексов (криптошлюзов).

Преимущества решений С-Терра

1. **Соответствие Российскому законодательству**. Продукты компании «С-Терра СиЭсПи» сертифицированы ФСБ России до классов КС3 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, в том числе:

- Федеральный закон №149 «Об информации, информационных технологиях и о защите информации»,
- Федеральный закон №152 «О персональных данных»,
- Приказ ФСТЭК России №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в **государственных информационных системах**».

Продукты С-Терра включены в единый реестр отечественного программного обеспечения Минкомсвязи России и позволяют выполнить требования Постановления Правительства РФ №1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей **осуществления закупок для обеспечения государственных и муниципальных нужд**».

Продукты С-Терра рекомендованы к использованию для подключения к системе межведомственного электронного взаимодействия (СМЭВ).

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

3. **Отсутствие зависимости от поставщика оборудования.** Технология IPsec является унифицированным мировым технологическим стандартом. В любой организации уже используются вычислительные системы в архитектуре Intel (x86/x86-64 совместимые) и ARM универсального назначения. Поэтому, установив на них ПО С-Терра VPN, вы защитите свою сеть в соответствии с российским законодательством.

4. **Высокая экономическая эффективность продуктов**. Оптимальный функциональный состав решений С-Терра, а также использование международных технологических стандартов позволяют не только оптимизировать Ваши первоначальные затраты на приобретение, но и снизить стоимость дальнейшего владения. Цены на право пользования продуктами С-Терра фиксированы в рублях и не зависят от курса валют.

5. **Качественная, оперативная служба технической поддержки.** Выбрав решения С-Терра для обеспечения 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. Возможен выезд специалиста к Вам в офис. На все аппаратные платформы, входящие в состав криптошлюзов, предоставляется гарантия производителя не менее 3-х лет. Некоторые платформы поставляются на условиях безусловной оперативной замены в случае неисправности (в течение срока гарантии).

Решения С-Терра для задач отрасли

Решения С-Терра	Продукты С-Терра	Описание
Задача:	***Защита взаимодействия между отделениями одной организации***	
Защита корпоративной сети	• С-Терра Шлюз • С-Терра Виртуальный Шлюз • Криптомаршрутизатор ESR-ST	Защита любого сетевого трафика при передаче по открытым каналам связи. Широкая линейка продуктов в различных форм-факторах, UTM-устройства. Масштабирование производительности.
Задача:	***Удаленный доступ сотрудников, работающих вне организации***	
Защита удаленного доступа	• С-Терра Клиент • С-Терра Клиент-М	Удаленный доступ сотрудников через интернет с помощью программного клиента для различных ОС.
Задача:	***Подключение к СМЭВ***	
Подключение к СМЭВ	• С-Терра Шлюз	Рекомендовано Минкомсвязи России к использованию.
Задача:	***Защита взаимодействия с ЦОД или между ЦОД***	
Защита канала 10Гб	• С-Терра Шлюз • С-Терра Шлюз 10G	Защита канала 10G с помощью одной пары шлюзов. Использование кластера мощных шлюзов.

Решения С-Терра	Продукты С-Терра	Описание
Задача:	***Защита взаимодействия с зарубежными филиалами***	
Защита трансграничного взаимодействия	• С-Терра Шлюз Е • С-Терра Клиент-Е	Экспортное исполнение для работы за пределами РФ. Упрощенное оформление разрешения на вывоз.

Защита взаимодействия между отделениями одной организации

Защита взаимодействий в территориально-распределенной сети организации – типовая задача для решения с помощью продуктов С-Терра, многократно проверенная нашими заказчиками.

В каждом отделении устанавливается криптошлюз, реализующий IPsec VPN с ГОСТ-алгоритмами и межсетевое экранирование. Благодаря широкой линейке продуктов С-Терра, можно подобрать подходящее устройство для решения любой задачи, с требуемой скоростью передачи данных.

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

Удаленный доступ сотрудников

Для реализации своих полномочий мобильным сотрудникам необходим доступ со своих пользовательских устройств через сеть Интернет к общим ресурсам организации.

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

a) С-Терра Клиент – для ОС Windows;
b) С-Терра Клиент-М – для ОС Android.

В точке подключения сотрудников к сети организации (например, в головном отделении) устанавливается С-Терра Шлюз.

Подключение к СМЭВ

Шлюзы безопасности С-Терра внесены в перечень рекомендованного криптографического оборудования для защиты подключения к СМЭВ, что закреплено в документе, размещенном на технологическом портале СМЭВ (Регламент 3.4[1] Приложение 3 «Требования к сети передачи данных участников информационного обмена»).

[1] Регламент обеспечения предоставления государственных услуг и исполнения государственных функций в электронном виде. Версия 3.4

Для организации подключения пользователей в федеральном центре обработки данных СМЭВ – на площадке ПАО «Ростелеком» – установлены криптошлюзы компании «С-Терра СиЭсПи».

Для организации защищенного подключения используются С-Терра Шлюз, сертифицированные ФСБ России как СКЗИ по классу КС3.

Защита взаимодействия с ЦОД

Для создания полномасштабной единой сетевой инфраструктуры, интегрированной с системами обеспечения безопасности, и устойчивости функционирования необходима централизация ИТ ресурсов. При этом появляется задача защиты высокоскоростных каналов связи между организациями и центром обработки данных (ЦОД), а также между основным и резервным ЦОДами.

Распространенные заблуждения о том, что оптические каналы связи не требуют защиты, а также об отсутствии отечественных средств криптографической защиты для скоростей 10Гб/с, 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 отечественных криптошлюзов сегодня значительно возросла – С-Терра Шлюз 10G шифрует до **10Гб/с смешанного** трафика по ГОСТ28147-89.

Данный продукт является уникальной разработкой компании «С-Терра СиЭсПи» и базируется на высокопроизводительной аппаратной платформе и ПО С-Терра Шлюз, специально оптимизированном для решения именно такой задачи.

Как результат, всего **одна пара** устройств С-Терра Шлюз 10G обеспечивает защиту канала связи 10Гб/с шифрованного IMIX трафика.

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

Защита взаимодействия с зарубежными филиалами

Сотрудникам государственных органов, имеющих зарубежные представительства и ведомства, тоже необходим защищенный доступ к ресурсам центрального офиса и/или ЦОДа, расположенным в Российской Федерации. Большинство отечественных средств криптографической защиты могут использоваться только на территории РФ, для вывоза за рубеж требуется специальное разрешение и множество согласований.

Для решения этой задачи компания «С-Терра СиЭсПи» разработала экспортный вариант своих самых популярных продуктов – С-Терра Шлюз Е и С-Терра Клиент Е, предназначенные для использования как в России, так и за её пределами. При необходимости применения данного продукта за пределами РФ, применяется упрощенная процедура вывоза средств криптографической защиты за рубеж.

Наши клиенты

Среди пользователей решений С-Терра: крупнейшие банки, финансовые учреждения, Совет Федерации, МИД, Федеральная налоговая служба, Росимущество, Рособрнадзор, Министерство транспорта, Росавтодор (ФДА), Министерство образования и науки, Конституционный Суд Российской Федерации, МВД, МЧС, Федеральная служба по контролю за оборотом наркотиков, Почта России, Региональные органы власти (более 25 субъектов).

Приобретение решений

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

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