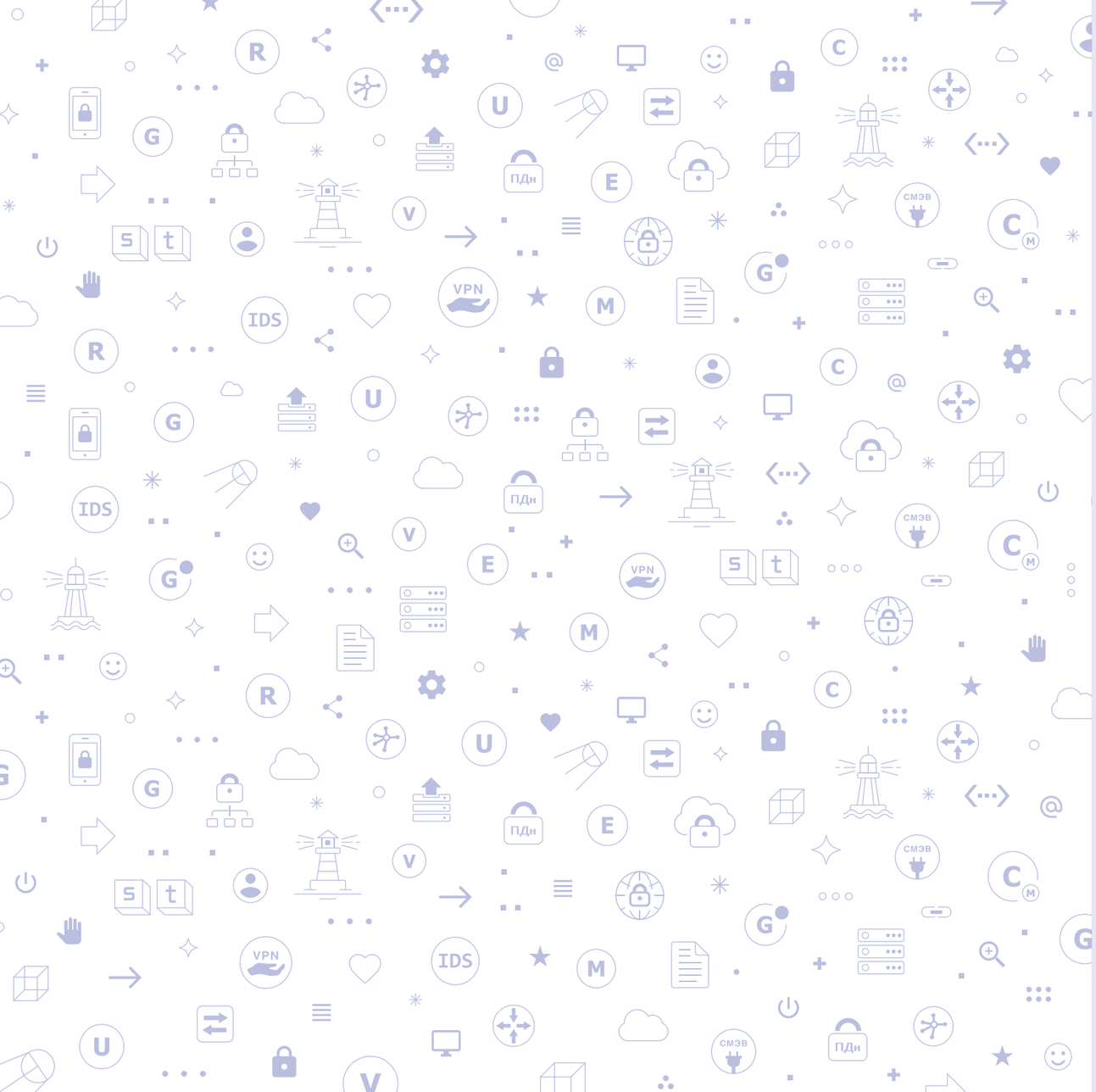
с•терра®

Ваш ориентир в мире безопасности

КАТАЛОГ ПРОДУКТОВ И РЕШЕНИЙ

СЕРТИФИЦИРОВАННЫЕ СРЕДСТВА
СЕТЕВОЙ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ



О КОМПАНИИ

Компания «С-Терра СиЭсПи» основана в 2003 году и является ведущим российским разработчиком и производителем сертифицированных средств защиты информации на основе технологии IPsec VPN.

Основные принципы работы компании:

- использование актуальных российских криптоалгоритмов ГОСТ;
- соответствие международным техническим стандартам, в том числе IKE/IPsec;
- сертификация продуктов в ФСБ России, ФСТЭК России, Минцифры России;
- обеспечение обширной сетевой функциональности продуктов;
- прозрачная ценовая политика;
- предоставление комплексной и всесторонней поддержки заказчиков.

Партнерская сеть компании «С-Терра СиЭсПи» насчитывает более 400 компаний, включая всех крупнейших российских системных интеграторов. Имеется представительство в Республике Беларусь.

Простоту интеграции продуктов С-Терра в любую сетевую инфраструктуру обеспечивают:

- выверенный многолетней мировой практикой архитектурный дизайн;
- широкий спектр типовых решений и уникальных сценариев применения;
- полная и доступная документация на продукты;
- оперативная многоуровневая техническая поддержка.

Решения С-Терра широко применяются:

- в госструктурах различных уровней, от местных администраций до федеральных органов власти;
- в государственных информационных системах (СМЭВ, ИС ЕПТ, ГосСОПКА и др.);
- в кредитно-финансовых организациях, в том числе в крупнейших банках и страховых компаниях;
- в коммерческих компаниях, в том числе малого и среднего бизнеса;
- на производственных предприятиях, включая масштабные нефтегазовые холдинги и предприятия федерального уровня.

Продуктовая линейка компании «С-Терра СиЭсПи» позволяет защитить информационную систему любого масштаба: от небольшой локальной сети до инфраструктуры федерального уровня. При этом, топология сети также может быть любой: точка-точка, звезда, иерархическая, полносвязная или частично-связная.

Основой защиты передаваемых данных служит технология IPsec VPN, надежность и безопасность которой подтверждена многолетним мировым опытом. Построение защищенных соединений, межсетевое экранирование, поддержка современных сетевых протоколов, соответствие требованиям регуляторов ИБ позволяет органично интегрировать решения и продукты С-Терра в существующую корпоративную сеть.

Полный комплект средств сетевой защиты С-Терра обеспечивает защиту:

- пользовательских устройств
- серверов
- сетевой инфраструктуры
- специализированных устройств (банкоматы, IP-видеокамеры, системы управления, устройства контроля и т. д.).

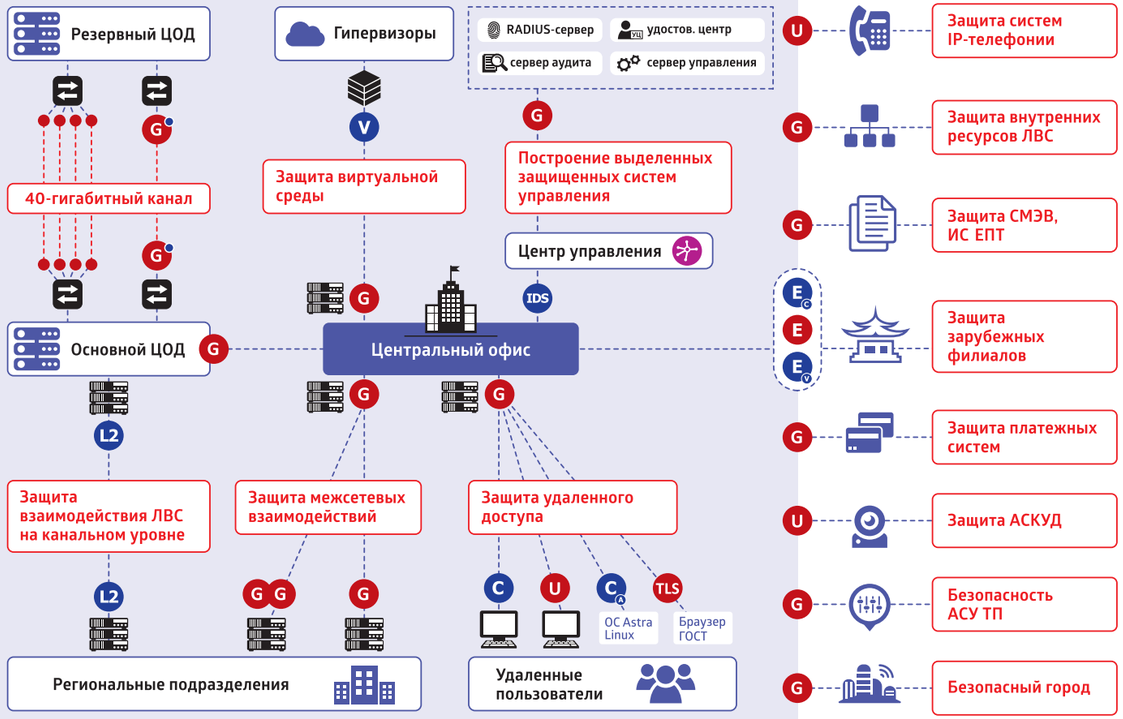
ПРЕИМУЩЕСТВА:

- стандартный протокол IPsec
- сертификация ФСБ России и ФСТЭК России
- продукты в Реестре российского ПО и в реестре Минпромторга
- cisco-like интерфейс
- широкий спектр сетевых функций
- бесплатная техподдержка в первый год

Продукты С-Терра включены в «Единый реестр российских программ для ЭВМ и баз данных» и могут использоваться как в государственных учреждениях, так и в коммерческих организациях в соответствии с отраслевыми стандартами и требованиями по защите информации, в том числе для следующих целей:

- защита конфиденциальной информации;
- защита подключения информационных систем государственных органов к Интернет;
- защита персональных данных;
- защита объектов критической информационной инфраструктуры;
- защита систем управления технологическими процессами (АСУ ТП);
- защита крупных территориально-распределенных сетей;
- защита IP-телефонии, видеонаблюдения, видеоконференцсвязи, СКУД;
- защита подключения к СМЭВ, ИС ЕПТ, ГосСОПКА и др.

Схема решений С-Терра



продукты в реестре Российского ПО

С-Терра Клиент, С-Терра Клиент А

Программный комплекс для защиты и фильтрации трафика с контролем состояния сессий для пользовательских устройств с ОС Windows и ОС Astra Linux.

ПРЕИМУЩЕСТВА

- Межсетевой экран
- Удалённое централизованное управление с С-Терра КП
- Инкапсуляция IPsec трафика в HTTP (IPsec-over-HTTP)
- Авторизация через RADIUS (xAuth), в т.ч. с одноразовыми паролями
- Режим пользовательского токена (*хранение на токене закрытого ключа и конфигурации клиента*)
- Работа через прокси

ХАРАКТЕРИСТИКИ

- IKE / IPsec с криптоалгоритмами ГОСТ согласно RFC и ТК26
- Stateless фильтрация IP-трафика
- Statefull фильтрация трафика для TCP и FTP
- Поддержка split tunneling
- Маркировка трафика
- Получение адреса из предопределенного пула
- IKECFG-интерфейс (*в том числе DNS*)
- Работа через NAT
- Событийное протоколирование Syslog
- Мониторинг по SNMP
- Поддержка токенов

Экспортное исполнение С-Терра Клиент Е.
Сертификация ФСБ России – СКЗИ КС1, КС2.

Продукт	Операционные системы	Сертификация ФСБ России	Сертификация ФСТЭК России
С-Терра Клиент	Windows 8, 8.1, 10, 11 Server 2012 / 2016 / 2019 / 2022	СКЗИ КС1, КС2	МЭ В4, 4 уровень доверия
С-Терра Клиент А	Astra Linux Common Edition релиз «Орёл» Astra Linux Special Edition релиз «Смоленск»	СКЗИ КС1, КС2, КС3	

продукт в реестре Российского ПО

продукт в реестре Минпромторга

С-Терра Юнит

Компактный VPN-шлюз для защиты и фильтрации трафика отдельных устройств.

ПРЕИМУЩЕСТВА

- Самый миниатюрный VPN-шлюз на российском рынке
- Межсетевой экран
- Удаленное централизованное управление с С-Терра КП
- Упрощенное развертывание и обновление ПО
- Защита беспроводных каналов связи
- Защита трафика устройств, на которые установка VPN-клиента невозможна

ПРИМЕНЕНИЕ

- мобильные устройства на любой ОС
- АСУТП
- системы контроля
- банкоматы
- IP-камеры, ВКС
- интерфейсы управления (ILO, CIMC, IPMI)
- беспроводные каналы связи

ХАРАКТЕРИСТИКИ

- Габариты: 80 x 45 x 22 мм
- IKE / IPsec с криптоалгоритмами ГОСТ согласно RFC и ТК26
- Stateless фильтрация IP-трафика
- Statefull фильтрация трафика для TCP и FTP
- Приоритизация и маркировка трафика (QoS)
- Температурный диапазон работы: от -5 до +40°C
- Питание – USB 5V
- Гарантия на АП – 1 год

Макс. произв-ть шифрования	Сертификация ФСБ России	Сертификация ФСТЭК России
10 Мбит/с	СКЗИ КС1, КС2, КС3	МЭ А4, 4 ур. доверия

продукт в реестре Российского ПО

С-Терра Шлюз

Программно-аппаратный комплекс для обеспечения сетевой безопасности корпоративной сети любой топологии, с любым количеством туннелей.

ПРЕИМУЩЕСТВА

- Межсетевой экран
- Удаленное централизованное управление и обновление с С-Терра КП
- Интеграция с RADIUS сервером
- Использование Zabbix-агента «из коробки»
- Поддержка технологий NetFlow, IPFIX
- IPsec-over-HTTP
- Интеграция с С-Терра СОВ и С-Терра TLS Шлюз

Сертификация ФСБ России	Сертификация ФСТЭК России
СКЗИ КС1, КС2, КС3	МЭ А4 / Б4, 4 ур. доверия

ХАРАКТЕРИСТИКИ

- Туннелирование трафика – маскировка топологии защищаемого сегмента сети
- Stateless фильтрация IP-трафика
- Stateful-фильтрация трафика для TCP и FTP
- IKE / IPsec с криптоалгоритмами ГОСТ согласно RFC и ТК26
- Поддержка split tunneling
- Приоритизация и маркировка трафика (QoS)
- Событийное протоколирование Syslog
- Мониторинг по SNMP
- Отказоустойчивость: горячее резервирование по VRRP, балансировка нагрузки с RRI и т.д.
- Резервирование провайдеров
- Поддержка технологии-аналога DMVPN
- Динамическая маршрутизация RIP, OSPF, BGP
- L2 VPN (*возможность построения полносвязной оптимальной топологии*)
- Гарантия на АП – 3 года

Экспортное исполнение С-Терра Шлюз Е.
Сертификация ФСБ России – СКЗИ КС1, КС2, КС3.

	С-Терра Шлюз	Целевое назначение	Макс. производ-ть шифрования, Мбит/с	Кол-во туннелей
	100	Малые офисы, банкоматы, подключение к гос. системам	150	10 / 200
	1000	Небольшие офисы	405	50 / 500
	2000		1060	500
	3000	Средние офисы	1510	1000
	7000 Std	Крупные офисы, ЦОД	2590	не ограничено
	7000 HE		5710	
	8000		9290	
	ПРОМЫШЛЕННОЕ ИСПОЛНЕНИЕ			
	100	Эксплуатация в сложных условиях окружающей среды	74	10

продукт в реестре Российского ПО

продукт в реестре Минпромторга

С-Терра Шлюз в реестре российской радиоэлектронной продукции

Модель С-Терра Шлюз	Целевое назначение	Макс. производ-ть шифрования, Мбит/с	Кол-во туннелей
100	Малые офисы, банкоматы, подключение к гос. системам	170	10 / 200
1000	Небольшие офисы	340	50 / 500
3000 Std	Средние офисы	1200	1000
3000 HE		2300	не ограничено
7000 HE	Крупные офисы, ЦОД	2900	не ограничено
8000		8800	

С-Терра Шлюз 100 на аппаратной платформе собственной разработки — АП «**СТК-100**»

продукт в реестре Российского ПО

С-Терра Шлюз DP

10G / 25G / 40G / 100G

Специализированный VPN-шлюз для защиты высокопроизводительных каналов связи, в том числе магистральных, между ЦОД, доступ к СХД, к ЦОД.

ПРЕИМУЩЕСТВА

- Рекордная производительность за счет специального механизма приема и отправки пакетов сетевой подсистемой
- Работа на любых каналах связи
- Выделенные интерфейсы для:
  - управления: С-Терра КП, протокол SSH
  - мониторинга: С-Терра КП, SNMP, Zabbix
  - динамической маршрутизации
- Интеграция Zabbix-агента
- Встроенная возможность шифрования на квантовых ключах

ХАРАКТЕРИСТИКИ

- Шифрование трафика на уровне L2 с возможностью работы по L3-каналам связи (*L2-over-L3*)
- Фрагментация трафика средствами VPN-шлюза
- IKE / IPsec с криптоалгоритмами ГОСТ согласно RFC и ТК26
- Событийное протоколирование Syslog
- Мониторинг по SNMP
- Топологии:
  - «точка-точка»
  - «звезда» с ограничением по количеству партнеров/«лучей»
- Для модели 40G: агрегирование до трёх С-Терра Шлюз 10G
- Гарантия на АП – 3 года

Сертификация ФСБ России	Сертификация ФСТЭК России
СКЗИ КС1, КС2, КС3	МЭ А4 / Б4, 4 ур. доверия

Модель	Макс. производительность шифрования	Формфактор
10G	20 Гбит/с	1U
25G	30 Гбит/с	1U
40G	50 Гбит/с	2U
100G	100 Гбит/с	2U

продукт в реестре Российского ПО

C-Терра Виртуальный Шлюз

Программный комплекс, представляющий собой VPN-шлюз в виде виртуальной машины, предназначенный как для защиты доступа к элементам виртуальной среды, так и для защиты взаимодействия между территориально-распределёнными компонентами сети.

ПРЕИМУЩЕСТВА

- Интеграция непосредственно в виртуальную инфраструктуру
- Быстрая доставка, установка, настройка
- Масштабируемость лицензионно (*для 1, 4, 12 ядер*)
- IKE / IPsec с криптоалгоритмами ГОСТ согласно RFC и ТК26
- Эффективное использование ресурсов
- Оперативная адаптация к меняющимся требованиям
- Независимость от аппаратной платформы
- Наличие экспортного исполнения

Сертификация ФСБ России	Сертификация ФСТЭК России
СКЗИ КС1	МЭ Б4, 4 ур. доверия

ХАРАКТЕРИСТИКИ

- Полная функциональность C-Терра Шлюз

ГИПЕРВИЗОРЫ

- VMware
- Hyper-V
- KVM
- Promox VE

Кол-во ядер	Макс. производительность шифрования
1	340 Мбит/с
4	1350 Мбит/с
12*	3050 Мбит/с

* *только при использовании passthrough или SR-IOV для сетевых адаптеров.*

Экспортное исполнение C-Терра Виртуальный Шлюз E.
Сертификация ФСБ России – СКЗИ КС1.

C-Терра TLS Шлюз

Программный комплекс для защиты доступа к веб-порталам, корпоративным приложениям и другим ресурсам, расположенным в защищённой сети, с помощью протокола TLS.

ПРЕИМУЩЕСТВА

- Актуальные криптоалгоритмы ГОСТ: Магма и Кузнечик
- Широкий модельный ряд АП
- Защита трафика с устройств на любой ОС при использовании браузера с ГОСТ-шифрованием
- Межсетевой экран и IPsec VPN (*при совместном использовании с C-Терра Шлюз*)

Исполнения:

- виртуальное
- на аппаратной платформе
- на одной аппаратной платформе с C-Терра Шлюз

Сертификация ФСБ России	СКЗИ КС1, КС2

ХАРАКТЕРИСТИКИ

- Работа с браузерами: Яндекс.Браузер, Chromium-Gost
- Одно- и двусторонняя аутентификация
- Широкий перечень средств для получения статистики и мониторинга
- Локальное и удаленное управление: Web API, SSH, web-интерфейс
- Отказоустойчивый кластер VRRP
- Режим перешифрования с международных на ГОСТ-криптоалгоритмы
- Гранулированный доступ
- Гарантия на АП – 3 года

ПРОИЗВОДИТЕЛЬНОСТЬ:

- От 100 до 14000 Мбит/с в зависимости от модели и количества подключений
- Количество подключений лицензируется

C-Терра TLS Клиент с двусторонней аутентификацией — в процессе разработки.

продукт в реестре Российского ПО

С-Терра СОВ

Программный комплекс для выявления компьютерных атак на основе анализа сетевого трафика.

ПРЕИМУЩЕСТВА

- Наглядный графический интерфейс
- Удобная система управления и мониторинга
- Ролевая модель администрирования и управления доступом
- Гибкий настраиваемый поиск инцидентов
- Работа с большим количеством сенсоров (больше 100)

Выбор исполнения:

- виртуальная
- на аппаратной платформе
- на одной платформе с С-Терра Шлюз

Базы решающих правил:

- поддержка нескольких источников БРП
- С-Терра БРП в реестре баз данных

Доверенный канал управления защищен С-Терра Шлюз.

Сертификация ФСТЭК России	СОВ ур. сети 4 кл. защиты, 4 ур. доверия

ХАРАКТЕРИСТИКИ

- Базы данных сигнатур
  - on-line и off-line режимы обновления
  - централизованное автоматическое обновление
  - возможно здание правил вручную
- Анализ данных сигнатурным и эвристическим методами
- Анализ служебной информации сетевых протоколов
- Регистрация атак
  - графический интерфейс
  - система распределённого хранения данных
- Работа с инцидентами
  - выборочный контроль отдельных объектов сети
  - поиск, сортировка, упорядочивание данных в журнале инцидентов
  - вкл./откл. отдельных правил и групп правил
- Оповещение
  - консоль администратора
  - графический интерфейс
  - e-mail
  - интеграция с ГосСОПКА

Гарантия на АП – 3 года.

продукт в реестре Российского ПО

С-Терра КП

Централизованная система управления VPN-продуктами С-Терра. В состав входят: **Сервер управления**, устанавливаемый на выделенный компьютер и предназначенный для управления VPN-устройствами, и **Клиент управления**, установленный на управляемое VPN-устройство.

ПРЕИМУЩЕСТВА

- Повышение безопасности системы
- Снижение стоимости владения системой
- Удобство работы
- Графический интерфейс управления
- Защита от неудачного обновления
- Унифицированная консоль управления без зависимости от ОС

ОС, поддерживаемые Сервером управления	Windows Server 2012 / 2016 / 2019 / 2022
Сертификация	В качестве системы управления в составе линейки продуктов С-Терра

ХАРАКТЕРИСТИКИ

- Гибкое управление правами администратора
- Обновление настроек С-Терра Клиент на компьютерах пользователей, не имеющих прав администратора
- Инициализация, восстановление и обновление С-Терра Шлюз с флеш-носителя
- Автоматизация процесса подготовки дистрибутивов для инициализации управляемых VPN-устройств

На управляемых VPN-устройствах

- Изменение параметров, в т.ч.:
  - локальная политика безопасности
  - настройки VPN и МЭ
  - сертификаты, списки отозванных сертификатов
- Формирование ключевой пары (*обновление сертификата*)

Для управляемых VPN-устройств

- Контроль активности
- Контроль срока действия сертификатов
- Задание настроек с помощью интерактивных мастеров
- Конвертация политик безопасности с ранних версий на современную

Об управляемых VPN-устройствах

- Сбор и анализ статистической информации
- Архивирование и восстановление данных на сервере управления

Защита корпоративной сети

Продукты С-Терра позволяют решить любые задачи по защите взаимодействия сегментов корпоративной сети, выстраивая через недоверенную сеть защищенный IPsec-туннель. В результате все передаваемые данные оказываются под надежной защитой: злоумышленник не может ни прочитать, ни изменить защищенные сообщения.

Защита данных, передаваемых между сегментами сети, и межсетевое экранирование осуществляются VPN-устройствами С-Терра Шлюз, линейка которых масштабируется от небольших экономичных устройств (*С-Терра Шлюз 100*), до мощных серверов, предназначенных для защиты до 10 Гбит трафика (*С-Терра Шлюз 8000*). В центральном офисе шлюзы могут работать в отказоустойчивой конфигурации для обеспечения беспрерывного сервиса. Помимо стандартных аппаратных платформ, шлюз может работать в виде виртуальной машины (*С-Терра Виртуальный Шлюз*).

Передача multicast и broadcast пакетов, трафика с VLAN-тегами и другого трафика, который не проходит через IPsec в обычном режиме, реализуется с помощью программного продукта С-Терра L2.

Магистральные каналы или другие сети связи, по которым передаются десятки гигабайт трафика, защищают высокопроизводительные шлюзы линейки С-Терра Шлюз DP.

Управление и настройку VPN-продуктов С-Терра выполняет централизованная система управления С-Терра КП.

ПРЕИМУЩЕСТВА:

- Стандартные протоколы IPsec
- Актуальные криптоалгоритмы ГОСТ
- Интеграция в существующую инфраструктуру (*в том числе виртуальную*)
- Сертификация ФСБ России и ФСТЭК России
- Продукты включены в Реестр Российского ПО и в реестр Минпромторга
- Первый год технической поддержки – бесплатно

Безопасный удаленный доступ к ресурсам корпоративной сети с устройств, работающих на ОС Windows, обеспечивает программный комплекс С-Терра Клиент, а на ОС Astra Linux – С-Терра Клиент А.

Удаленный доступ с пользовательских устройств можно защищать с помощью миниатюрного шлюза С-Терра Юнит, который не зависит от установленной на рабочем месте операционной системы.

Защита персональных данных

Продукты С-Терра, сертифицированные ФСБ России и ФСТЭК России, позволяют обеспечить защиту персональных данных (ПДн) в информационной системе (ИСПДн) любого уровня защищенности, во исполнение ФЗ №152 от 27.07.2006 «О персональных данных».

Применение продуктов С-Терра для защиты ПДн разного уровня защищенности

Криптографическая защита удаленного доступа к ресурсам

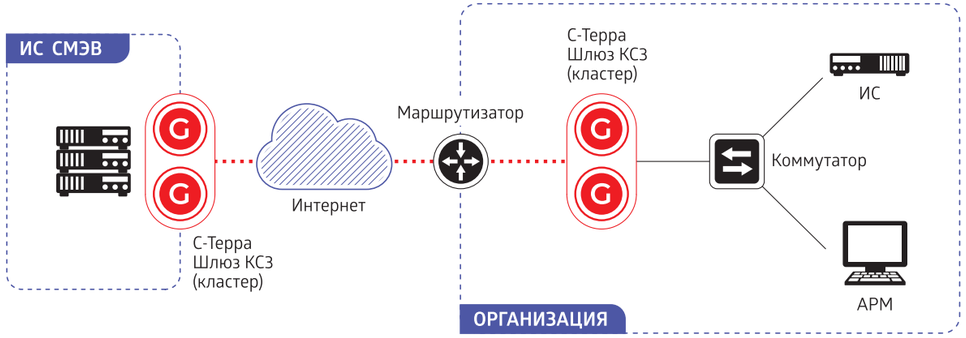
	УЗ-1	УЗ-2	УЗ-3	УЗ-4
С-Терра Шлюз, С-Терра TLS Шлюз С-Терра Виртуальный Шлюз С-Терра Клиент С-Терра Клиент А С-Терра Шлюз DP С-Терра Юнит	–	+	+	+

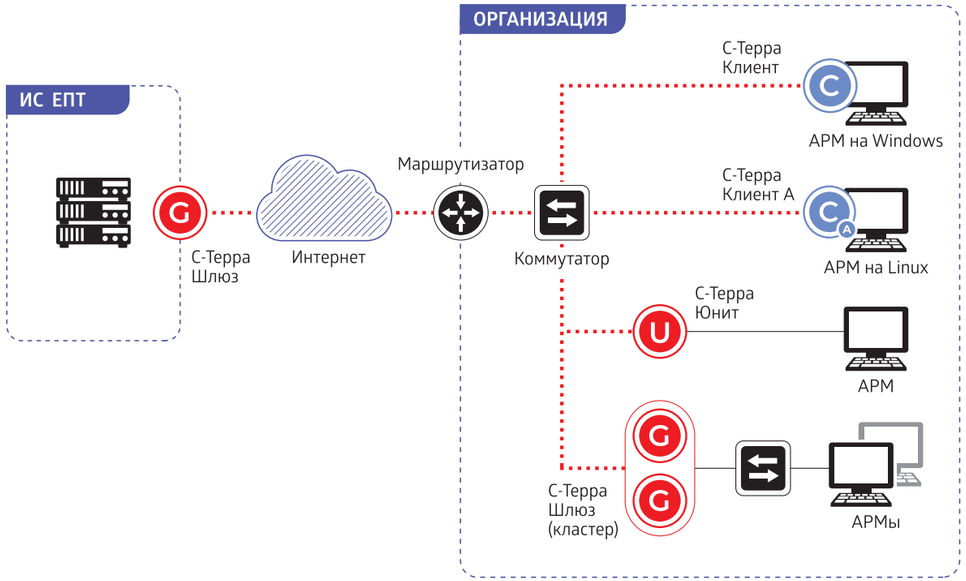
Межсетевое экранирование при доступе к ресурсам ИСПДн

	УЗ-1	УЗ-2	УЗ-3	УЗ-4
С-Терра Шлюз С-Терра Виртуальный Шлюз С-Терра Клиент С-Терра Клиент А С-Терра Шлюз DP С-Терра Юнит	+	+	+	+

Защита от вторжений при доступе к ресурсам ИСПДн

	УЗ-1	УЗ-2	УЗ-3	УЗ-4
С-Терра СОВ	+	+	+	+





Защита подключений к государственным информационным системам

ГосСОПКА

Шлюзы безопасности С-Терра Шлюз, сертифицированные в качестве СКЗИ по классу КС3, входят в перечень оборудования, рекомендованного для организации защищенного взаимодействия с ГосСОПКА. Подключение осуществляется путем построения защищенного канала с технической инфраструктурой Национального координационного центра по компьютерным инцидентам (НКЦКИ).

СМЭВ*

Шлюзы безопасности С-Терра Шлюз, сертифицированные в качестве СКЗИ по классу КС3, рекомендованы для защиты подключения к СМЭВ. Для организации подключения пользователей шлюзы безопасности С-Терра установлены в федеральном центре обработки данных СМЭВ – на площадке ПАО «Ростелеком».

ИС ЕПТ**

Функции ИС ЕПТ:

- аттестация сотрудников,
- исключение фальсификации тестирования,
- подача заявления об аттестации.

Для подключения к защищенной сети передачи данных ИС ЕПТ рекомендованы следующие VPN продукты С-Терра: С-Терра Клиент, С-Терра Клиент А, С-Терра Юнит, С-Терра Шлюз.

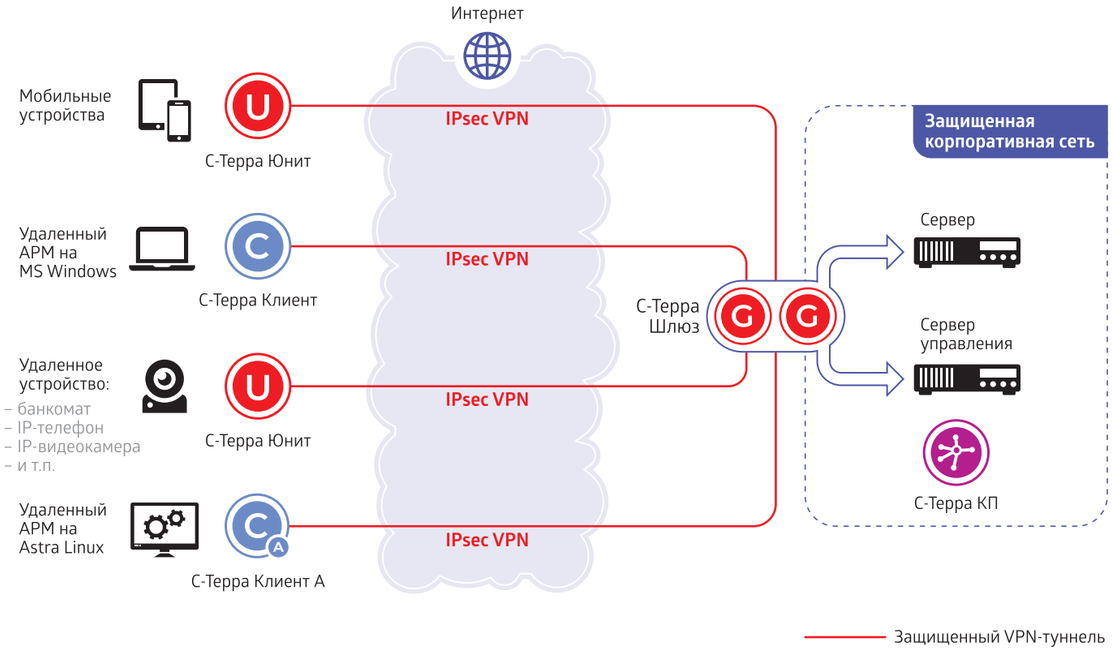
ВЫБОР МОДИФИКАЦИИ ОБОРУДОВАНИЯ ЗАВИСИТ ОТ:

- требуемой пропускной способности защищенного канала,
- количества подключаемых автоматизированных рабочих мест (АРМ),
- необходимости обеспечения резервирования.

* *Система Межведомственного Электронного Взаимодействия.*

** *Информационная Система «Единый портал тестирования в области промышленной безопасности, безопасности гидротехнических сооружений, безопасности в сфере электроэнергетики».*

Защита удаленного доступа



Защита удаленного доступа

Продукты С-Терра защищают доступ сотрудников к корпоративной информации и к сервисам корпоративной сети из любой точки мира. Их применение позволяет выполнить требования Российского законодательства и регуляторов отрасли.

Защита каналов связи между удаленным пользовательским устройством под управлением ОС Windows и корпоративной сетью, защищенной решением С-Терра, осуществляется программным VPN-клиентом С-Терра Клиент. Он запускается до входа пользователя в систему, может работать через различные прокси и поддерживает интеграцию с RADIUS и xAuth.

Для защиты трафика устройств с ОС Astre Linux применяется С-Терра Клиент А.

Если у провайдеров разрешен только HTTP (*например, в публичных местах*), то для построения защищенных соединений применяется инкапсуляция IPsec трафика в протокол HTTP.

Если на пользовательском устройстве используется операционная система, для которой не предусмотрен программный клиент, то применяется миниатюрный VPN-шлюз С-Терра Юнит. Его габариты, немногим превосходящие спичечный коробок, позволяют использовать его для защиты данных, передаваемых в корпоративную сеть с банкоматов, камер видеонаблюдения, систем АСУ ТП, измерительных и контрольных устройств и датчиков, а также с мобильных устройств на любой операционной системе.

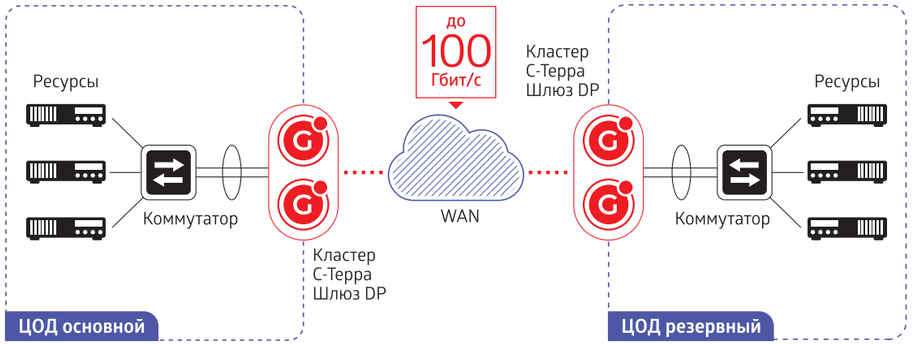
В качестве точки подключения удаленных пользователей к корпоративной сети используются шлюзы безопасности С-Терра Шлюз, С-Терра Виртуальный Шлюз. Для организации удаленного доступа к Web-ресурсам можно использовать С-Терра TLS Шлюз и С-Терра TLS Клиент.

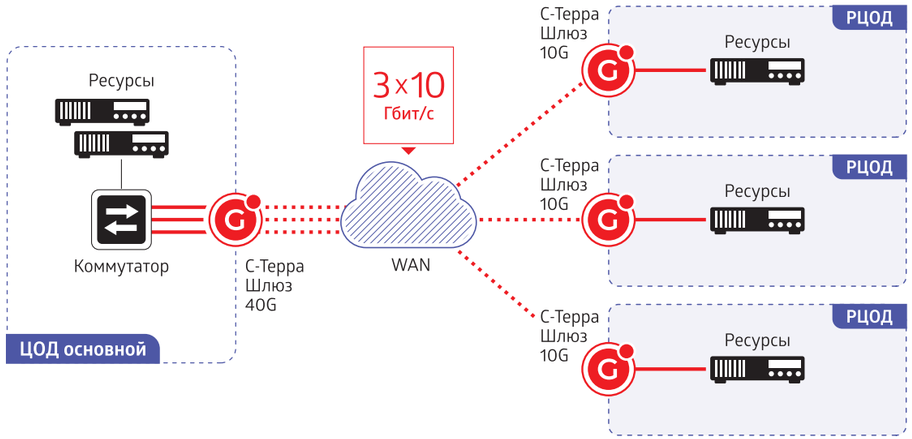
Своевременное обновление цифровых сертификатов на удаленных пользовательских устройствах выполняет централизованная система управления С-Терра КП.

ПРИМЕНЕНИЕ:

- Защита доступа с мобильных устройств
- Индивидуальный защищенный доступ к виртуальным рабочим столам (VDI)
- Контроль доступа пользователей в корпоративную сеть
- Защита доступа с устройств вне контролируемой зоны
- Защита АСУ ТП
- Защита трафика банкоматов
- Защита беспроводных каналов связи
- Защита IP-телефонии, ВКС, трафика IP-видеокамер

Защита высокопроизводительных каналов связи





Защита высокопроизводительных каналов связи

Продукты С-Терра обеспечивают надежную защиту каналов связи с производительностью до 100 Гбит/с, выполняя при этом требования регуляторов ИБ, а также обеспечивая отказоустойчивость и высокое качество сервиса.

Безопасное взаимодействие между двумя ЦОД обеспечивают высокопроизводительные VPN-шлюзы С-Терра Шлюз DP в сочетании с устройствами для балансировки трафика. В зависимости от пропускной способности канала связи выбирается модификация VPN-шлюза: С-Терра Шлюз 10G, 25G, 40G или 100G.

Отказоустойчивость обеспечивается созданием кластера с резервным шлюзом безопасности.

Решение масштабируется по производительности путем добавления дополнительных шлюзов безопасности в кластер. Балансировка реализуется коммутаторами с использованием протоколов LACP (*до 8 шлюзов безопасности*) или PAgP (*до 16 шлюзов безопасности*).

Непрерывность пользовательских сервисов сохраняется при проведении разного рода работ на шлюзах безопасности.

ПРИМЕНЕНИЕ:

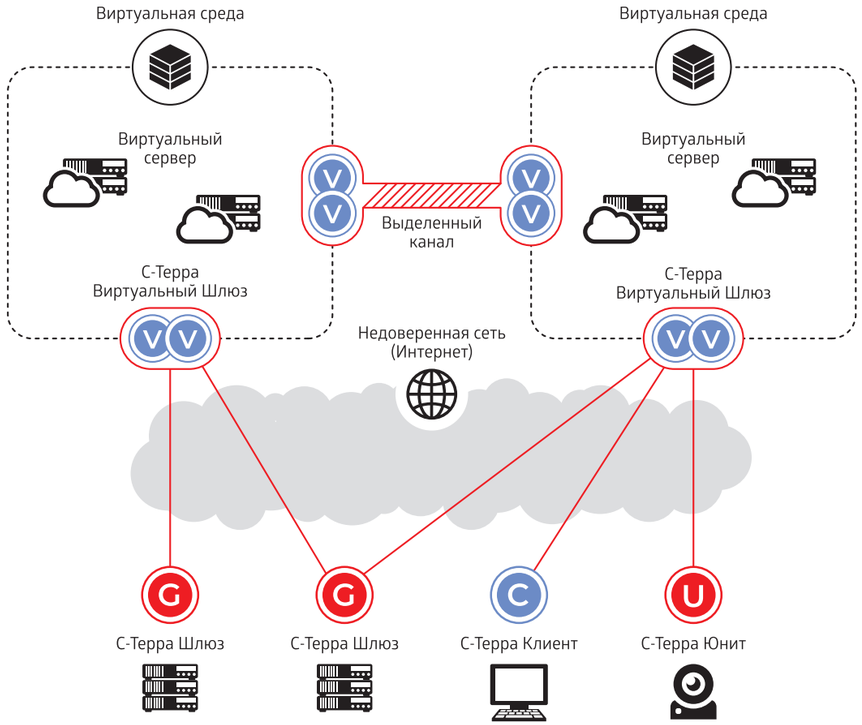
- Взаимодействие между ЦОД
- Доступ к системам хранения данных (СХД), iSCSI-трафик
- Миграция ЦОД без остановки сервисов
- Передача данных по магистральным каналам связи
- Миграция виртуальных машин без простоев

Обеспечить защиту взаимодействия между центральным ЦОД и тремя резервными ЦОДами возможно с применением топологии «трёхлучевая звезда».

Криптошлюз С-Терра Шлюз 40G способен терминировать на себе до трёх каналов связи производительностью 10 Гбит/с, защищаемых с помощью С-Терра Шлюз 10G, объединяя в единый broadcast домен четыре территориально распределенных сети с помощью IPsec туннелей.

Применение С-Терра Шлюз DP позволяет реализовать решение с шифрованием трафика с применением квантового распределения ключей.

Защита виртуальной среды



Защита виртуальной среды

Продукты С-Терра обеспечивают надежную защиту в виртуальной среде, позволяя в полной мере использовать основные преимущества виртуализации: экономичность, масштабируемость, отказоустойчивость, в то же время соблюдая требования российского законодательства и регуляторов ИБ.

Защитить виртуальную инфраструктуру организации для обеспечения безопасного доступа к ней можно, использовав программно-аппаратный комплекс С-Терра Шлюз, но удобнее и эффективнее в этом случае установить специализированный программный комплекс С-Терра Виртуальный Шлюз, который интегрируется непосредственно в инфраструктуру популярных систем виртуализации (*VMware ESX, KVM, Hyper-V и др.*).

Доступ к виртуальной инфраструктуре, «периметр» которой защищен средствами безопасности С-Терра Виртуальный Шлюз, осуществляется с использованием любого из VPN-продуктов С-Терра, в том числе: С-Терра Шлюз, С-Терра Клиент, С-Терра Клиент А, С-Терра Юнит.

Защита каналов связи между различными физическими серверами, составляющими виртуальную среду, может обеспечиваться также как программно-аппаратными С-Терра Шлюз, так и программными С-Терра Виртуальный Шлюз. Это решение применяется, например, в случае географически распределенной виртуальной среды, или если каналы связи и промежуточное оборудование не являются доверенными (*например, при аренде нескольких серверов в ЦОДе стороннего провайдера*).

ПРИМЕНЕНИЕ:

- Безопасный доступ к виртуальной среде
- Защита виртуальной инфраструктуры одновременно с физическими компонентами системы
- Недорогое сертифицированное решение для малого бизнеса

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

- **СТАНДАРТНАЯ**
  Дистанционно по телефону, e-mail, в личном кабинете на сайте
- **РАСШИРЕННАЯ**
  Стандартная + ускоренная обработка заявок
- **ПРЕМИАЛЬНАЯ**
  Стандартная + приоритетная обработка заявок + персональный инженер + возможен выезд инженера на площадку заказчика

ОБУЧЕНИЕ

Обучающие курсы предназначены для технических специалистов и инженеров в области информационной безопасности и безопасности сетей. Требования к начальной подготовке слушателей: техническая подготовка на уровне Cisco CCNA.

Авторизованные курсы в Учебных центрах

Преподаватели, обученные в компании «С-Терра СиЭсПи», на лекционных и практических занятиях познакомят слушателей с продуктами и решениями С-Терра, особенностями их применения, а также с правовыми основами в области защиты информации.

АНО ДПО ЦПК «АИС» – «Защита сетевой инфраструктуры на основе продуктов С-Терра» (**2 дня**).

АНО ДПО ЦПК «АИС» – «Построение защищенных виртуальных сетей на основе IPsec с использованием алгоритмов шифрования ГОСТ на базе шлюзов безопасности С-Терра» (**5 дней**).

По итогам обучения выдаются Сертификаты установленного образца.

Собственный обучающий семинар

«Защита сетевой инфраструктуры на основе продуктов С-Терра»

Длительность – **2 дня**.

От практикующих инженеров компании слушатель узнает самую актуальную информацию о продуктах С-Терра, а также получит практические навыки реализации решений С-Терра.

В ходе семинара предоставляется возможность задать интересующие вопросы специалистам-разработчикам компании-производителя оборудования.

По итогам обучения выдается Сертификат компании «С-Терра СиЭсПи».

КОНТАКТНАЯ ИНФОРМАЦИЯ

ПРИОБРЕТЕНИЕ ПРОДУКЦИИ

Телефон: +7 (499) 940 9060
E-mail: sales@s-terra.ru

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Телефон: +7 (499) 940 9071
E-mail: support@s-terra.ru

ТЕХНИЧЕСКИЙ КОНСАЛТИНГ

Телефон: +7 (499) 940 9001
E-mail: presale@s-terra.ru

МАРКЕТИНГ, PR

Телефон: +7 (499) 940 9061
E-mail: pr@s-terra.ru

WWW.S-TERRA.RU

124460 г. Москва, г. Зеленоград,
ОЭЗ Технополис Москва,
ул. Конструктора Лукина, д. 14, стр. 12.

Подписано в печать 22.01.2024