s•terra

ЗАЩИТА УДАЛЕННОГО ДОСТУПА. ДОВЕРЕННЫЙ СЕАНС СВЯЗИ

Задача

Одним из инструментов развития современного бизнеса является повсеместное использование информационных технологий. Сотрудникам компаний необходим доступ к корпоративной информации из любой точки мира, поэтому от информационных систем требуется гибкость и способность быстро подстраиваться под новые условия. Перед службами безопасности компаний стоит непростая задача: предоставить пользователям удобное решение, обеспечивающее удаленный доступ к сервисам компании, сохранив высокий уровень защищенности, включая:

- организацию индивидуального защищенного удаленного доступа к виртуальным рабочим столам, сервисам или приложениям;
- контроль доступа пользователей к сервисам и ресурсам компании;
- защиту устройств удаленных пользователей, работающих вне контролируемой зоны.

При выборе инструментов для решения поставленной задачи следует учитывать возможные риски информационной безопасности (ИБ), которые могут привести к нарушению конфиденциальности, целостности и доступности информации. Этими рисками являются:

- Невыполнение пользователем предписанного ему регламента безопасности вне контролируемой зоны;
- Компрометация операционной системы (ОС) сотрудника компании, т.е. содержание в ней вредоносного кода, вируса, программных закладок, программного обеспечения типа spyware, malware и т.д.;
- Незамкнутость вычислительной и сетевой среды пользователя, т.е. возможность установки неконтролируемых соединений с рабочего места сотрудника.

Без контроля за конечными устройствами мобильных пользователей и применения специальных средств защиты администратору ИБ трудно минимизировать все риски.

Кроме этого, если в информационной системе компании обрабатывается информация, подлежащая обязательной защите согласно российскому законодательству (например, персональные данные), то необходимо использовать сертифицированные средства защиты.

Существует несколько вариантов решения этой задачи, удовлетворяющих всем требованиям и обеспечивающих защищенный доступ к корпоративной информации и сервисам компании, сохраняя при этом высокий уровень защищенности самой информационной системы:

1. **Решение по защите устройств конечных пользователей с помощью программного клиента (ПК).** В этом варианте на каждое конечное устройство пользователя, работающего вне контролируемой зоны, устанавливается программный VPN-клиент, обеспечивающий криптографическую защиту передаваемого трафика и пакетную фильтрацию. Перед тем, как пользователю предоставляется доступ к сервисам компании, он проходит процедуру аутентификации путем ввода пароля и цифрового сертификата открытого ключа, закрытый ключ которого может храниться на токене. Уровень защищенности конечного устройства (актуальность антивирусных баз данных, обновление ОС и т.п.) контролируется дополнительным средством защиты (возможно, не одним). На рынке ИБ существуют программные продукты, удовлетворяющие данным требованиям и сертифицированные регуляторами. Однако у системных администраторов компании не всегда

имеется возможность установить требуемое ПО на рабочую станцию удаленного пользователя (например, его домашний ПК). Совместная работа VPN-клиента и средства контроля также возможна далеко не во всех случаях.

2. **Решение по защите устройств конечных пользователей с помощью специального загрузочного носителя.** Каждому пользователю предоставляется защищенный загрузочный USB-носитель. С него загружается замкнутая программная среда, изолированная от ОС рабочего места. Ни пользователь, ни нарушитель не могут модифицировать или добавлять файлы в изолированную среду, поэтому нет необходимости в индивидуальных средствах защиты (антивирусе и т.п.). Аутентификация пользователя происходит посредством ввода PIN-кода и цифрового сертификата открытого ключа, закрытый ключ которого храниться на носителе. Для шифрования трафика от пользовательского устройства до информационной системы компании используются отечественные криптоалгоритмы ГОСТ. Никакие данные пользователя от предыдущих сеансов не сохраняются на устройстве.

VPN-продукты С-Терра уже более 10 лет успешно используются для реализации первого решения.

В связи с возросшими потребностями пользователей в эффективном и комплексном решении, компания «С-Терра СиЭсПи» подготовила вариант исполнения второго решения.

Решение по защите устройств на базе С-Терра «Пост»

Предлагаемое решение не требует дополнительных средств защиты для контроля пользовательских устройств и соответствует требованиям российского законодательства в области информационной безопасности. Оно позволяет сотрудникам получить защищенный доступ к информационной системе компании из любой точки мира.

Основным компонентом решения является продукт С-Терра «Пост», представляющий собой специальный загрузочный носитель (СЗН) «СПДС-USB-01» с размещенной на нем доверенной замкнутой программной средой. Благодаря использованию такого съемного носителя, обеспечивается безопасный доступ удаленных пользователей к различным корпоративным информационным ресурсам с устройства, расположенного вне контролируемой зоны компании.

Точка подключения удаленного рабочего места к корпоративным сервисам компании защищается криптографическим шлюзом безопасности С-Терра Шлюз. Структурная схема решения представлена на рисунке 1.

Для организации защищенного удаленного доступа пользователю выдается СЗН, на котором находится:

- Модуль доверенной загрузки среды функционирования;
- Целостный эталон среды функционирования (СФ), включающей эталонную операционную систему и комплект средств криптографической защиты информации (СКЗИ);
- Пользовательское программное обеспечение (ППО) для решения бизнес-задач компании пользователя.

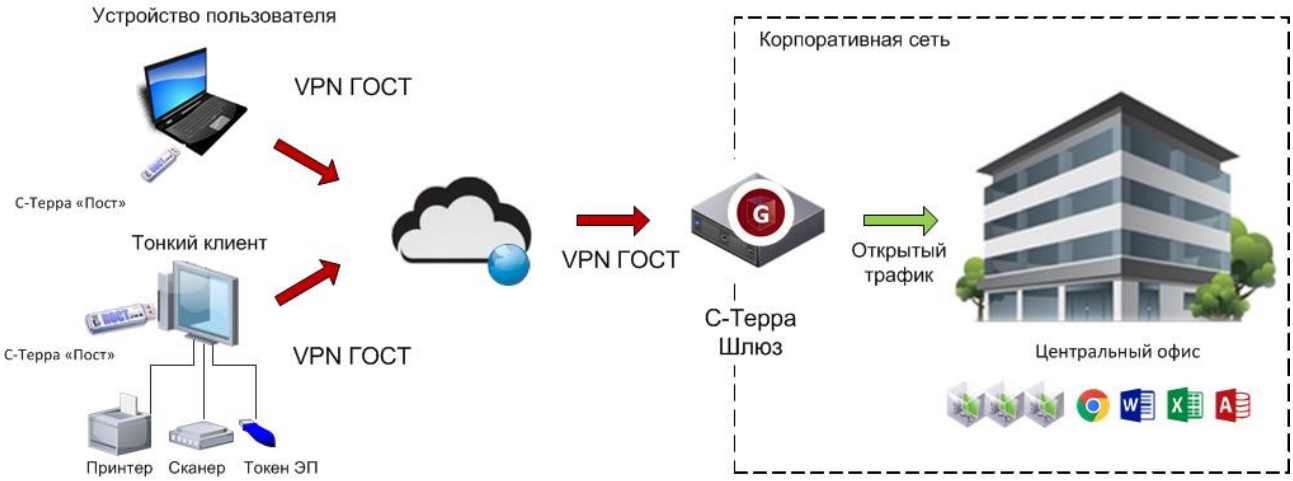

Рисунок 1. Схема решения для организации защищенного удаленного доступа сотрудников на базе С-Терра «Пост»

Запись посторонних данных на СЗН исключена, как и доступ к операционной системе или посторонним приложениям. Пользователь получает доступ строго к прикладному программному обеспечению, функциональность которого выбирается, исходя из задач сотрудника. Пользователю будет разрешен доступ только к конкретной удаленной рабочей машине или организовано подключение к инфраструктуре VDI компании. При этом к компьютеру, выступающему в качестве рабочего места сотрудника, не предъявляются требования по защищенности. Т.е. он может быть заражен вирусами или вредоносным ПО, но эталон среды функционирования, размещенный на СЗН, не будет взаимодействовать со скомпрометированным жестким диском, а файлы системы на нем не будут подвержены изменениям, т.к. целостность среды функционирования контролируется. Никакие данные пользователя на СЗН не хранятся и в СФ не вносятся.

Рисунок 2. Архитектура С-Терра «Пост»

Перед первым использованием С-Терра «Пост» на ПК сотрудника производится настройка BIOS, позволяющая производить загрузку рабочего места с USB-накопителя.

После подключения СЗН и загрузки происходит аутентификация – необходимо ввести PIN-код, при этом количество попыток ввода ограничено. По результатам аутентификации загружаются эталонный образец среды функционирования и пользовательское программное обеспечение. Тип встроенного ППО выбирается, исходя из потребностей заказчика, на стадии подготовки бизнес-требований к решению.

Между рабочим местом пользователя и точкой доступа в корпоративную сеть устанавливается защищенное VPN-соединение на основе набора протоколов IKE/IPsec с применением отечественных криптоалгоритмов. Открытый трафик при этом исключается политикой безопасности VPN-продукта, чем достигается полная изоляция сетевой среды, в которой реализуется доверенный сеанс. Встроенный межсетевой экран С-Терра Шлюз с функциями пакетной фильтрации трафика блокирует все незащищенные соединения.

Преимущества решения на базе С-Терра «Пост»

В сравнении с традиционными технологиями защиты удаленных и мобильных клиентов, решение на основе продуктов компании «С-Терра СиЭсПи» имеет целый ряд преимуществ:

- **Используется целостная замкнутая программная среда на защищенном USB-носителе, обеспечивающая доверенный сеанс связи, блокирующая модификацию системных файлов и приложений конечными пользователями или вредоносным ПО.** Заказчик может отказаться от применения средств индивидуальной антивирусной защиты от опасного ПО или программных "закладок". Это позволяет не только сэкономить на антивирусном ПО на рабочих местах сотрудников (достаточно его наличия только на серверной части), но и существенно облегчить процесс эксплуатации мобильных устройств, поскольку нет необходимости контролировать их конфигурацию и обновлять на них антивирусные базы.

- **Строгая двухфакторная аутентификация пользователя VPN при доступе к информационным ресурсам в рамках доверенного сеанса.** Сотрудник компании производит процедуру аутентификации перед загрузкой СФ при помощи PIN-кода (число попыток ввода пароля ограничено), доступ в корпоративную сеть осуществляется на основе цифрового сертификата, открытого ключа ГОСТ Р 34.10 и ГОСТ 34.11, закрытый ключ которого храниться на защищенном USB-носителе. При необходимости эти методы могут быть усилены дополнительными средствами аутентификации в составе прикладного ПО.

- **Сеанс связи полностью изолирован от посторонних воздействий и защищен стойкими ГОСТ криптоалгоритмами.** Защита передаваемого трафика до корпоративной сети осуществляется на основе криптоалгоритма ГОСТ 28147, обеспечивающего конфиденциальность и целостность передаваемых данных и самого соединения. Контроль состояния сессии производится за счет встроенных функций межсетевого экранирования, блокирующих злоумышленникам доступ извне к приложениям, размещенным на СЗН.

- **Гибкий выбор пользовательского программного обеспечения.** Наличие разнообразного ППО позволяет реализовать различные сценарии применения С-Терра «Пост», адаптированные под конкретные бизнес-задачи заказчика, начиная от организации защищённого уделенного доступа сотрудника к виртуальной инфраструктуре компании, и до защиты данных, передаваемых с тахографов водителей.

Решение позволяет выполнить требования российского законодательства, так как входящие в его состав продукты обладают сертификатами соответствия:

- ФСБ России (СКЗИ КС2, МЭ 4 класса защищенности)
- ФСТЭК России (МЭ 3 класса защищенности, СЗИ с оценочным уровнем доверия 4+ (усиленный) по «Общим критериям» ГОСТ Р ИСО/МЭК 15408, по 3 уровню контроля на отсутствие недекларированных возможностей)

и могут использоваться в автоматизированных системах класса защищенности до 1В включительно, а также в государственных информационных системах до 1 класса защищенности включительно, в том числе, обеспечивающих 1, 2, 3 и 4 уровни защищенности персональных данных.

Характеристики С-Терра «Пост»

С-Терра «Пост» обеспечивает защищенный доступ к удаленным ресурсам в соответствии с требованиями законодательства, без ущерба для удобства работы пользователей. Отсутствие необходимости использования дополнительных средств защиты позволяет Заказчику уменьшить расходы и ощутимо облегчить процесс эксплуатации системы безопасности.

Таблица 1. Характеристики С-Терра «Пост»

Описание	Спецификация
Операционная система	Debian 6
Протоколы IKE/IPsec	Стандарты RFC 2401 - 2412
Алгоритм шифрования	ГОСТ 28147-89
Алгоритмы электронной подписи	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012
Алгоритмы вычисления хэш-сумм	ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012
Криптография	«КРИПТО-ПРО» и собственная криптография «С-Терра СиЭсПи»
Событийное протоколирование	Syslog
Сбор статистики	Централизовано через систему управления и мониторинга С-Терра КП
Формат сертификатов публичных ключей	X.509 v.3 (ГОСТ)
Способы получения сертификатов	Протоколы IKE, LDAP v.3 Импорт из файла (bin и base64, PKCS#7 bin и base64, PKCS#12 bin и base64)
Способ получения ключевой пары	Генерация внешним PKI сервисом с доставкой или централизованно через С-Терра КП

Описание	Спецификация
Примеры поддерживаемого пользовательского программного обеспечения	Терминальные клиенты (Tsclient, Rdesktop) Клиенты VDI систем (VMware View Client, Citrix Receiver) Web-браузеры (Firefox, Chrome)

Настройка и управление С-Терра «Пост»

Первичная настройка С-Терра «Пост» и его дальнейшее сопровождение производится при помощи централизованной системы управления С-Терра КП, устанавливаемой на отдельный сервер в защищенной сети.

Использование единой точки управления позволяет администратору ИБ повысить общий уровень безопасности ИС компании, получить удобное средство настройки, управления и мониторинга всеми удаленными VPN-устройствами независимо от их географического положения, отвечает всем требованиям технологичности и снижает общую стоимость владения системой защиты компании (ТСО).

Сервер управления С-Терра КП выполняет следующие функции:

- Учет СЗН по серийным номерам.
- Первичная настройка С-Терра «Пост», а также его последующее обновление.
- Создание запросов к Удостоверяющему центру (УЦ) на формирование ключевых пар и сертификатов. Запись ключевых документов в С-Терра «Пост».
- Формирование и обновление политик безопасности VPN-клиентов. Запись политик в С-Терра «Пост».
- Настройка в составе VPN-клиентов подсистем сигнализации (SNMP) и событийного протоколирования (Syslog).

Защита серверной части осуществляется шлюзом безопасности С-Терра Шлюз, который может быть выполнен как в виде виртуальной машины С-Терра Виртуальный Шлюз, работающей под управлением гипервизора (VMware ESX, Citrix XenServer, Parallels, KVM), так и в традиционном варианте на аппаратной платформе.

Варианты использования С-Терра «Пост»

В основном, продукт С-Терра «Пост» применяется для осуществления защищенного доступа в следующих случаях:

- терминальный доступ к рабочему столу (по протоколам RDP, Citrix ICA, VNC и другим протоколам);
- доступ сотрудников к корпоративным веб-ресурсам (например, почта, портал, CRM и т.д.);
- доступ сотрудников к VDI-инфраструктуре VMware, Citrix и т.д.;

- доступ системных администраторов к ресурсам компании.

Кроме того, С-Терра «Пост» может использоваться и в более узкоспециализированных ситуациях:

- **Защита терминального доступа к инфраструктуре VDI с помощью комплекта доверенного сеанса (КДС).** Сотрудник компании получает КДС, состоящий из тонкого клиента и С-Терра «Пост». Тонкий клиент оснащен специализированным замком для BIOS, благодаря которому загрузка возможна исключительно с СЗН. В качестве клиентской части VDI может выступать Citrix Receiver, VMware View или RDP клиент. Доступ к системе VDI реализуется при помощи использования персонального токена, необходимого для усиления уровня защиты и контроля доступа пользователей.

- **Активация тахографов со встроенным СКЗИ.** Требования к тахографам и транспортным средствам, на которые они обязательны к установке, предписаны приказом Минтранса России от 13 февраля 2013 г. № 36. Перед началом работы тахографа со встроенным блоком СКЗИ необходимо провести его активацию. В пунктах активации, так называемых мастерских, для защищенного доступа используется КДС, в центрах технического обслуживания – С-Терра Шлюз. Решение обеспечивает защиту первичной инициализации смарт-карт для блоков СКЗИ тахографов.

- **Защита медицинских информационных систем (МИС).** Использование С-Терра «Пост» в различных МИС позволяет организовать сменную работу сотрудников на одном рабочем месте. Причем их данные будут полностью изолированы друг от друга – каждый работает с собственным СЗН. Данные между рабочим местом медицинского работника и сервером передаются по защищенному каналу. Возможна поддержка электронной подписи с помощью индивидуальных токенов.

Конкретный вариант использования практически полностью зависит от типа ППО, которое подбирается, исходя из бизнес-задач. В состав ППО входят:

- ПО, обеспечивающее функциональность, необходимую для работы пользователя. Например, в качестве RDP-клиента выступает ПО rdesktop, а для подключения к инфраструктуре Citrix – Citrix receiver for Linux. Поддержка «пробрасываемой» периферии может реализовываться клиентским ПО, либо отдельной утилитой.
- Набор драйверов для поддержки периферии (в том числе сетевых адаптеров, модемов, принтеров, сканеров и т.д.).
- Средства диагностики.

В связи с многообразием вариантов ППО, на основе продукта С-Терра «Пост» можно реализовать различные сценарии защиты сети или ее компонентов, как традиционные, для защиты удалённого доступа пользователей, так и специфические, реализующие узконаправленные потребности заказчика.

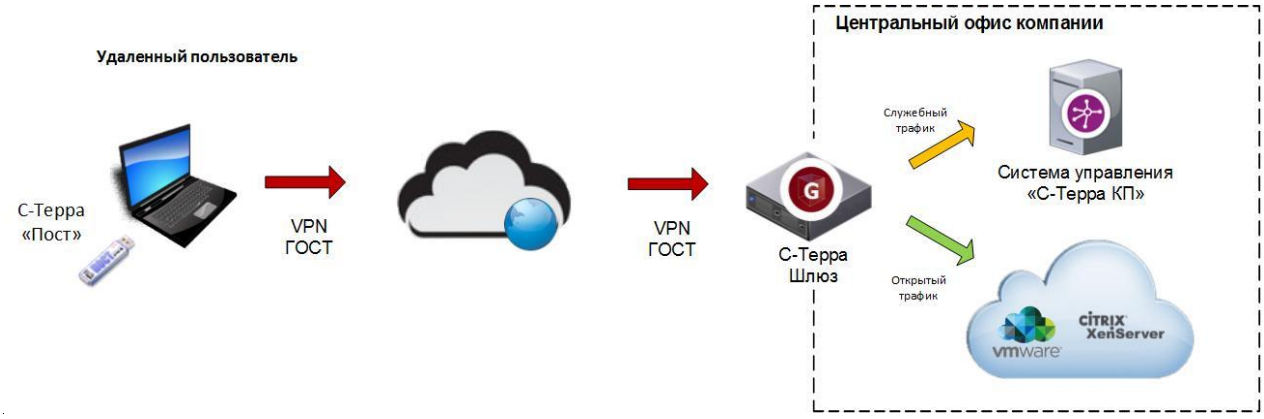

Рисунок 3. Типовая схема работы решения

Поддержка внедрений

Ввиду того, что технологии построения доверенного сеанса сегодня являются узкоспециализированными, компания «С-Терра СиЭсПи» реализует индивидуальные проекты с адаптацией решения под конкретные задачи заказчика.

Проекты организуются в следующем порядке:

1. Демонстрация заказчику возможностей решения С-Терра «Пост».
2. Согласование с заказчиком бизнес-требований для адаптации решения под его задачи, включая поддержку определенного парка оборудования, периферийных устройств и т.д.
3. Подготовка модификации решения в соответствии с согласованными бизнес-требованиями.
4. Внедрение, ввод в эксплуатацию.

На этапе согласования бизнес-требований конкретизируются параметры, имеющие определяющее значение для применения продукта С-Терра «Пост», а именно:

- аппаратные средства, которые будут использоваться в решении (терминалы, ноутбуки и т.д.);
- тип ППО для реализации требований заказчика;
- периферийные устройства (принтеры, сканеры);
- способы аутентификации пользователей;
- интеграция с системами управления, контроля доступа, мониторинга и аудита, и УЦ.

Рекомендации по выбору продуктов

Для выбора конкретных продуктов, кроме требуемого класса защиты, необходимо учитывать тип передаваемого трафика, ППО, количество пользователей, требования к резервированию и отказоустойчивости. Рекомендации по выбору оборудования представлены в таблице 2.

Таблица2. Расчет примерного состава решения по защите доступа на базе С-Терра «Пост». СКЗИ класса КС1 на стороне периметра.

КС1	До 10 устройств	До 100 устройств	До 500 устройств
Управление	1хС-Терра КП (лицензия на 10 устройств)	1хС-Терра КП (лицензия на 100 устройств)	1х С-Терра КП (лицензия на 500 и более устройств)
Серверная часть	1хС-Терра Виртуальный Шлюз (лицензия на 1 ядро) или 1хС-Терра Шлюз 100 или 1хМСМ-950	1хС-Терра Виртуальный Шлюз (лицензия на 4 ядра) или 1хС-Терра Шлюз 3000LE или 1хМСМ-950	2хС-Терра Виртуальный Шлюз (лицензия на 4 ядра) или 2хС-Терра Шлюз 3000 или 1хС-Терра Шлюз 7000
Клиентская часть	10хС-Терра «Пост»	100хС-Терра «Пост»	500хС-Терра «Пост»

Таблица 3 - Расчет примерного состава решения по защите доступа на базе С-Терра «Пост». СКЗИ класса КС2 на стороне периметра.

КС2	До 10 устройств	До 100 устройств	До 500 устройств
Управление	1хС-Терра КП (лицензия на 10 устройств)	1хС-Терра КП (лицензия на 100 устройств)	1х С-Терра КП (лицензия на 500 и более устройств)
Серверная часть	1хС-Терра Шлюз 100 или 1хМСМ-950	1хС-Терра Шлюз 3000LE или 1хМСМ-950	2хС-Терра Шлюз 3000 или 1хС-Терра Шлюз 7000
Клиентская часть	10хС-Терра «Пост»	100хС-Терра «Пост»	500хС-Терра «Пост»

Приведенные в таблицах 2 и 3 данные носят ориентировочный характер, поскольку трафик целевых приложений может отличаться в различных прикладных задачах. Кроме того, при оценке производительности шлюза безопасности следует учитывать статистику сеансов доступа. Данные в таблицах приведены для одновременной работы пользователей. Если сеансы пользователей статистически распределены во времени, требуемая мощность шлюза серверной части может быть снижена. Решение на базе С-Терра «Пост» может быть масштабировано на несколько сотен тысяч пользователей.

Техническая поддержка

Для С-Терра «Пост» компания «С-Терра СиЭсПи» разработала двухуровневую систему технической поддержки.

Обращения пользователей рассматривает корпоративная служба поддержки организации, эксплуатирующей решение (1-ая линия).

Обращения корпоративных заказчиков обрабатываются службой технической поддержки компании «С-Терра СиЭсПи» (2-ая линия).

Оплата сервиса технической поддержки строится на следующих принципах:

- Стоимость первого года технического обслуживания входит в цену решения.
- Стоимость продления сервиса годового технического сопровождения составляет примерно 10% от стоимости решения. Продление осуществляется для всего парка устройств на основании данных об активных лицензиях.

Возможны индивидуальные условия поддержки, выходящие за рамки стандартного сервиса.

О компании «С-Терра СиЭсПи»

ООО «С-Терра СиЭсПи» основано в 2003 году и является ведущим российским разработчиком и производителем средств сетевой информационной безопасности на основе технологии IPsec VPN.

Компания «С-Терра СиЭсПи» предлагает органично входящие в сетевую инфраструктуру решения, которые используют набор протоколов IPsec и российские сертифицированные криптографические алгоритмы ГОСТ. Решения характеризуются отличной масштабируемостью, надежностью и рекордной производительностью, что обеспечивает высокую экономическую эффективность.

Продукты и решения С-Терра обеспечивают защиту каналов связи любой производительности (как на сетевом, так и на канальном уровне), безопасный удаленный доступ, в том числе с мобильных платформ, а также предоставляет эффективное управление VPN-инфраструктурой С-Терра.

Продукты С-Терра сертифицированы ФСТЭК России и ФСБ России, в том числе как средства криптографической защиты информации (СКЗИ) по классу КС1, КС2, КС3, а также как межсетевой экран.

Компания является первым российским технологическим партнером Cisco (Cisco Solution Technology Integrator), Серебряным партнером Samsung и Авторизованным партнером Huawei.

Партнерская сеть компании "С-Терра СиЭсПи" состоит из более чем 300 компаний, включая всех крупнейших российских системных интеграторов. Имеется представительство компании в Республике Беларусь.