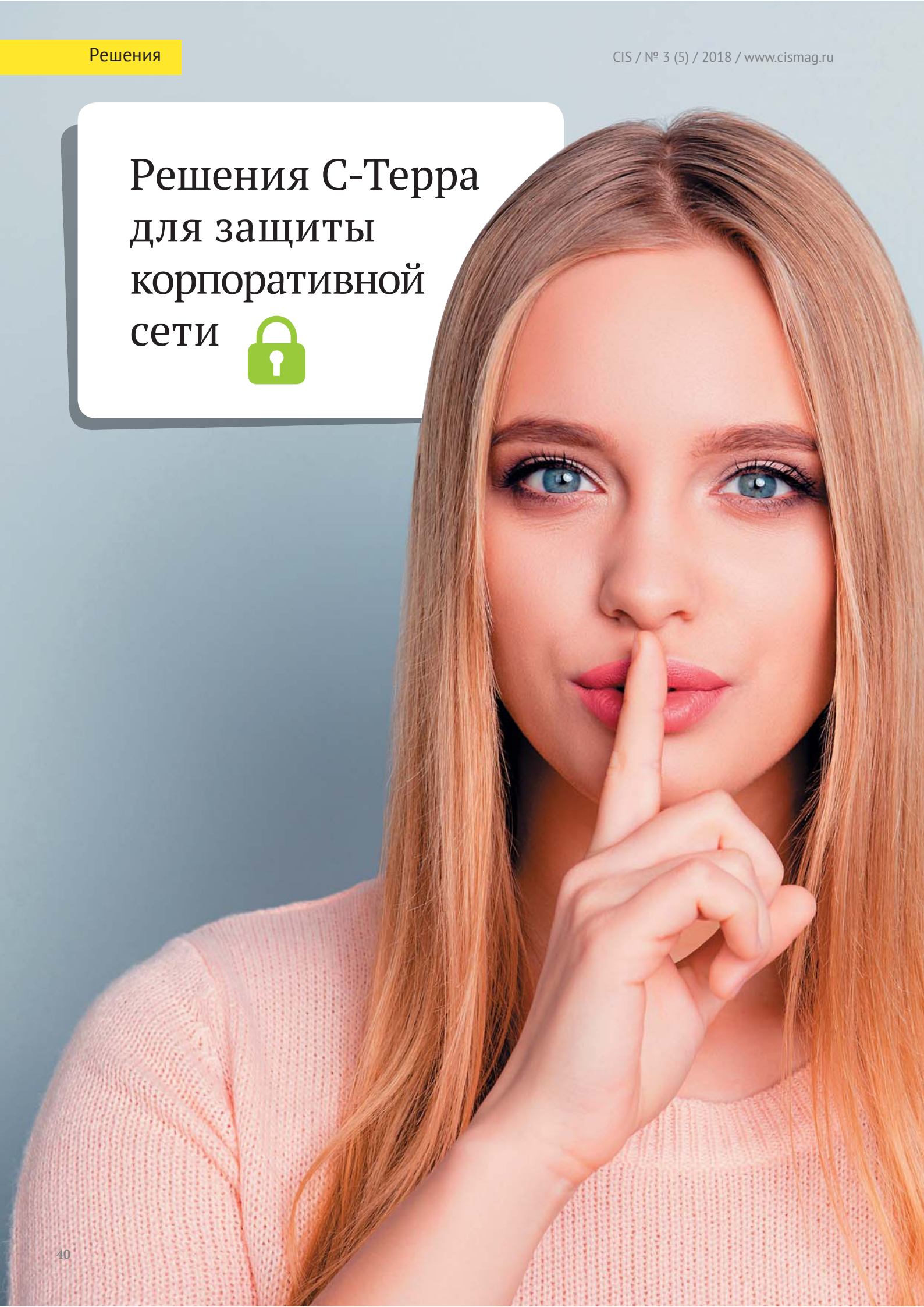
Решения С-Терра для защиты корпоративной сети



Любая организация заботится о сохранении своей информации, т. к. её разглашение может нанести ущерб как самой организации, так и другим лицам. Такую информацию называют конфиденциальной.

С этимологической точки зрения слово «конфиденциальный» происходит от латинского confidentia – доверие. В современном русском языке это слово означает «доверительный, не подлежащий огласке, секретный».

С развитием информационных технологий задача обеспечения информационной безопасности и, в частности, конфиденциальности приобретает всё большую значимость. Она крайне важна для любой организации, а для некоторых областей регламентируется на государственном уровне. 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. В связи с этим российский рынок средств информационной безопасности является достаточно специфичным. Проведение сертификации под силу не каждой компании – необходимо быть лицензиатом ФСБ России и ФСТЭК России.

Компания «С-Терра СиЭсПи» основана в 2003 году и является ведущим российским разработчиком и производителем средств сетевой информационной безопасности, специализирующимся на разработке и производстве средств криптографической защиты информации (СКЗИ) на основе российских криптоалгоритмов ГОСТ и стандартов IKE/IPsec (RFC2401-2412). Архитектура IPsec проверена многократным технический анализом и тестированием специалистов многих стран и внедряется по всему миру, в том числе и в России. Все продукты сертифицированы ФСБ России как средства криптографической защиты информации (СКЗИ) по классам КС1, КС2, КС3, а также во ФСТЭК России. Продуктовая линейка компании активно расширяется и позволяет решить множество задач, при этом соблюдая требования законодательства.

Продукты С-Терра используются в государственных и банковских организациях, в федеральных и региональных органах законодательной и исполнительной власти, в силовых структурах, крупных промышленных корпорациях, небольших коммерческих организациях.

Использование оборудования С-Терра позволяет решить целый ряд задач:

- защита филиальной сети различного масштаба и топологии;
- защищённый доступ удалённых сотрудников;
- защита высокопроизводительных каналов связи между ЦОД;
- защита доступа к виртуальной инфраструктуре;
- подключение к СМЭВ;

и прочих.

Защита территориально распределённых сегментов

Современный бизнес не ведётся в пределах офисных стен: компоненты инфраструктуры большинства компаний географически распределены. При этом им необходимо единое информационное пространство для создания которого используются, в том числе, недоверенные каналы связи. Для обеспечения конфиденциальности и целостности информации, передаваемой по таким каналам, необходимы VPN-продукты.

Компания «С-Терра СиЭсПи» предлагает широкую линейку шлюзов безопасности «С-Терра Шлюз», которые обеспечивают защиту трафика при его передаче, а также межсетевое экранирование. В центральной точке шлюзы могут работать в отказоустойчивой конфигурации для обеспечения беспрерывного сервиса.

Линейка шлюзов безопасности масштабируется от миниатюрных устройств, размером чуть больше спичечного коробка, до полноценных серверов, предназначенных для защиты десятков гигабит трафика. Это позволяет найти оптимальное по производительности решение для любой задачи, будь то защита взаимодействия офисов, IP-телефонии, видеоконференцсвязи и т.д.

Защита удалённого доступа

Множество организаций требуют от сотрудников постоянно находиться на связи и быть готовыми отреагировать в сжатые сроки на любые виды запросов. Компании привлекают сотрудников из других городов, регионов, даже стран. Удалённо работающие сотрудники – это тоже сегмент корпоративной сети, и ему нужна защита.

Для решения этой задачи на удалённое рабочее место устанавливается программное обеспечение – «С-Терра Клиент» (для всех современных ОС Windows) или «С-Терра Клиент-М» (для ОС Android). Продукты обеспечивают защиту трафика как внутри сети, так при передаче по внешним каналам связи. Поддерживается режим изоляции

от внешних сетей с помощью туннелирования всего трафика в корпоративную сеть с выходом в интернет через отдельный прокси-сервер. Также могут быть использованы дополнительные факторы аутентификации, например, токены и аутентификация на RADIUS-сервере.

Защита высокопроизводительных каналов между ЦОД

ЦОД стали чрезвычайно привлекательной мишенью для злоумышленников. Особенно перспективной точкой взлома выглядят магистральные волоконно-оптические каналы связи, соединяющие различные ЦОД, ведь через них передаётся колоссальное количество данных. При этом устройства съёма данных с волоконно-оптических каналов без разрыва волокна стоят всего лишь несколько сотен долларов. С их помощью злоумышленники могут в режиме реального времени получать доступ к передаваемым данным, а также собирать информацию для будущих атак.

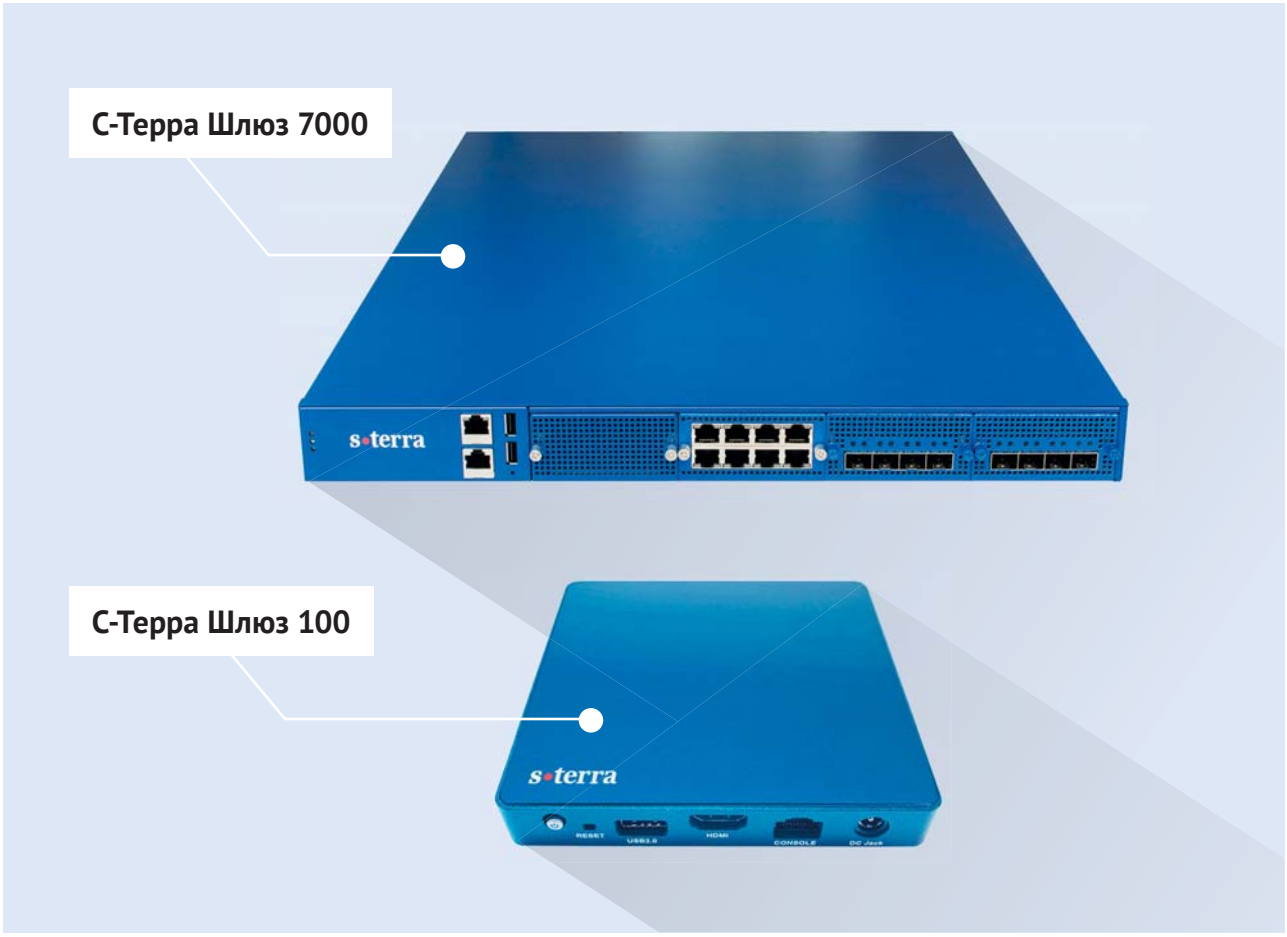
Становится очевидно, что каналы, соединяющие ЦОД между собой, необходимо защищать как от пассивного вмешательства (т.е. прослушивания данных), так и от активных действий злоумышленников (т.е. попыток изменить передаваемую информацию или не допустить её передачи). Когда ЦОД географически удалены друг от друга, физическая защита становится очень дорогой, а зачастую совсем невозможной. В такой ситуации приходится использовать недоверенные каналы связи и необходимо применять криптографическую защиту передаваемых данных.

Компания «С-Терра» предлагает комплексное решение на базе сертифицированных VPN-устройств «С-Терра Шлюз 10G» и коммутаторов, обеспечивающих балансировку трафика. Решение позволяет организовать высокопроизводительный защищённый канал между центрами обработки данных на скоростях от 10 Гбит/с и выше.

Минимальный комплект состоит из четырёх шлюзов безопасности и набора документации. Для его применения требуется наличие двух коммутаторов, соответствующих определённым требованиям: поддержка протокола LACP или PAgP, наличие необходимого количества интерфейсов 10 Гбит/с. Шлюзы используются для построения защищённого туннеля связи на канальном уровне. Такой туннель позволяет обеспечить конфиденциальность и целостность передаваемых данных даже в том случае, если промежуточное оборудование на канале было взломано злоумышленником. Коммутаторы выступают в роли балансировщиков трафика, обеспечивая масштабируемость и отказоустойчивость решения. Для балансировки трафика коммутаторы используют агрегированный канал (LACP или PAgP). Главные преимущества решения – отказоустойчивость и масштабируемость.

Защита доступа к виртуальной инфраструктуре

Использование дополнительных аппаратных VPN-шлюзов для защиты доступа к виртуальной среде не всегда целесообразно. Непосредственное встраивание в виртуальную среду позволяет в полной мере использовать основные преимущества технологии виртуализации: экономичность, масштабируемость, отказоустойчивость, а также позволяет



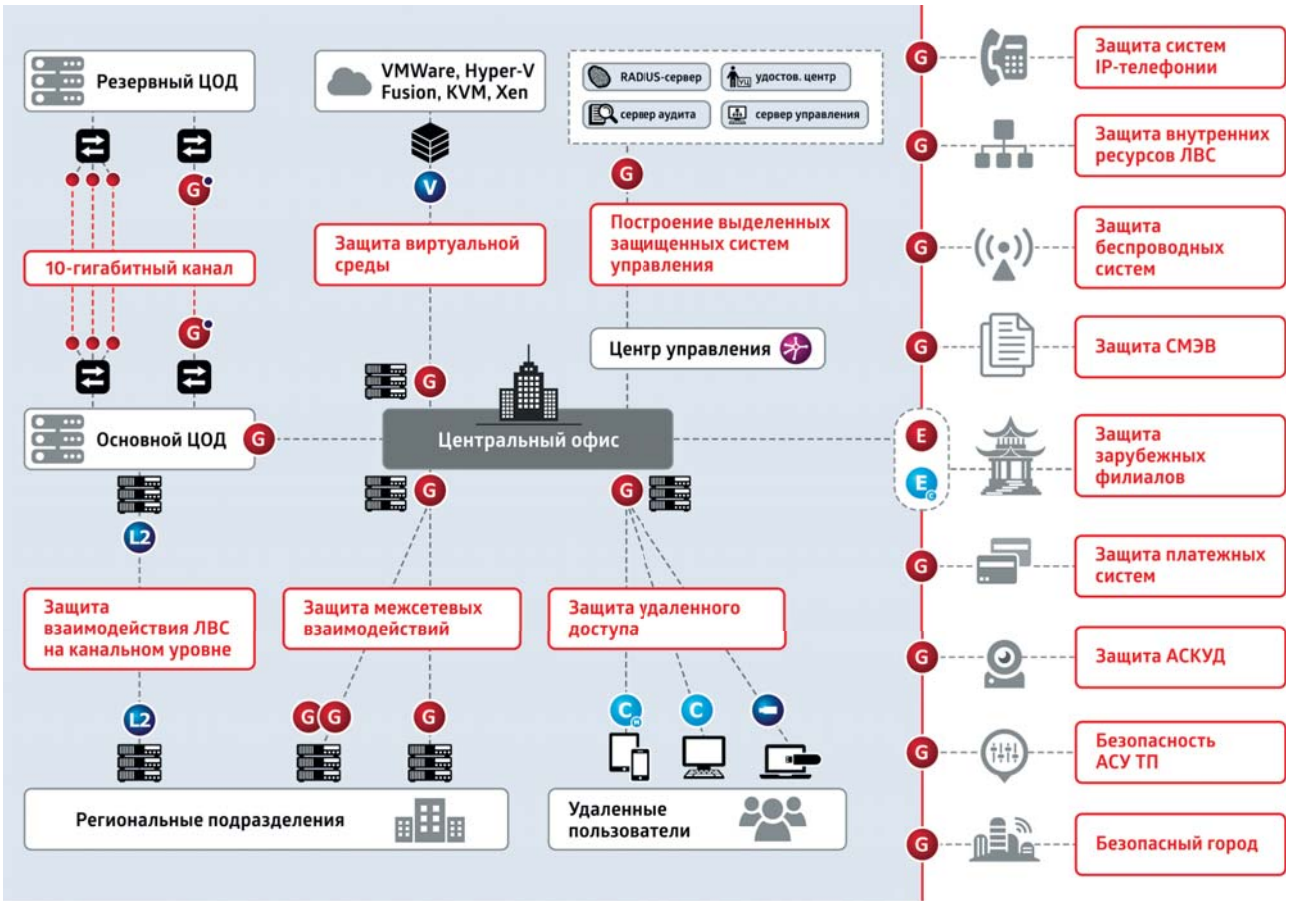


Схема решений.

избежать неудобств, возникающих при эксплуатации программно-аппаратных комплексов. Средства защиты, выполненные в виде виртуальных программных комплексов, имеют аналогичную функциональность, не уступающую традиционным программно-аппаратным решениям, при этом повышая удобство пользования сетевыми сервисами и упрощая администрирование средств защиты информации.

В линейке «С-Терра» этот подход реализован в продукте «С-Терра Виртуальный Шлюз». Это виртуальная машина для гипервизоров VMware ESXi, Citrix XenServer, MS Hyper-V, KVM, HW Fusion с функциональностью полноценного аппаратного криптошлюза «С-Терра». Виртуальный шлюз сертифицирован ФСБ России по классу КС1, а также во ФСТЭК России. Производительность зависит от частоты процессора аппаратной платформы и лицензии, которая ограничивает количество ядер, используемых для шифрования. К заказу доступны лицензии на 1, 4 и 12 ядер. Гибкий лицензионный механизм позволяет подобрать оптимальный вариант шлюза под любую задачу, а при необходимости – повысить производительность. На данный момент это уникальный для российского рынка продукт.

Подключение к СМЭВ

Приказом Минкомсвязи России от 23.06.2015 № 210 установлены Технические требования к взаимодействию информационных систем в СМЭВ, которые, в частности, предусматривают использование для обеспечения сетевой защиты данных набора протоколов IPsec, а также защиту всех каналов связи, выходящих за пределы контролируемых зон участников взаимодействия, с помощью сертифицированных средств криптографической защиты информации (СКЗИ) класса не ниже КС3.

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

При подключении к системе заказчик самостоятельно приобретает «С-Терра Шлюз» необходимой производительности для своей площадки, далее передаёт его для управления и поддержки операторам системы – сотрудникам ПАО «Ростелеком».

Резюме

«С-Терра СиЭсПи» является одним из лидеров рынка отечественных VPN-продуктов. Компания предлагает решения, соответствующие всем современным техническим требованиям в области информационной безопасности и позволяющие обеспечить выполнение требований регуляторов в сфере информационно безопасности. Именно такой подход обеспечивает надёжную защиту любой информационной системы.

Веселов Александр,
руководитель отдела технического консалтинга ООО «С-Терра СиЭсПи»

s·terra®
ВАШ ОРИЕНТИР В МИРЕ БЕЗОПАСНОСТИ

***«С-Терра СиЭсПи»** – российский разработчик и производитель средств сетевой информационной безопасности.*

www.s-terra.ru