Сертифицированная в ФСБ России криптография в решениях Cisco

Проблема

Решения Cisco признаны лучшими в сегменте VPN-решений во многих странах и считаются стандартом де-факто в среде специалистов по всему миру. Однако российские нормативно-правовые акты в ряде случаев устанавливают для заказчиков дополнительные требования, в частности, об использовании национальных алгоритмов и обязательной сертификации продуктов. Это связано как с действующим законодательством о порядке ввоза на таможенную территорию Таможенного союза и вывоза с таможенной территории Таможенного союза шифровальных (криптографических) средств, так и с требованиями законодательства по защите отдельных видов информации ограниченного доступа с помощью сертифицированных средств криптографической защиты.

Почему недостаточно использовать сертифицированное криптоядро?

В России распространена практика встраивания сертифицированного криптоядра (криптобиблиотеки, криптопровайдера) в различные прикладные системы, средства защиты и сетевое оборудование. Однако согласно позиции ФСБ России этот подход применим исключительно в области прикладных систем. VPN-продукты, стойкость которых должна оцениваться по совокупности характеристик криптоалгоритмов и криптографического протокола в целом, подлежат сертификации как средства криптографической защиты информации (СКЗИ) в целом. В одном из своих писем ФСБ России разъясняет этот момент:

«Так называемая «оценка корректности встраивания СКЗИ» в соответствии с ПКЗ 2005 является оценкой отсутствия негативного влияния разработанного ПО на работу СКЗИ. Но такой оценки применительно к VPN-продуктам недостаточно, т.к. необходима еще проверка правильности работы соответствующих криптографических протоколов, надежности их реализации, корректности настроек и т.д. Все эти аспекты применяются в рамках сертификационных исследований VPN-продуктов». Иными словами, VPN-решение должно быть сертифицировано полностью, а не просто использовать сертифицированное криптоядро. О необходимости сертификации часто говорится и в документации на встраиваемую сертифицированную криптобиблиотеку. Например, согласно формуляру на «КриптоПро CSP 3.0» при его встраивании в системы, используемые для защиты конфиденциальной информации, подлежащей защите в соответствии с законодательством Российской Федерации, необходима обязательная сертификация осуществленной интеграции по техническому заданию, согласованному с ФСБ России.

Для решения названной проблемы компания Cisco прикладывает серьезные усилия. В частности, совместно с российским разработчиком средств защиты – компанией С-Терра СиЭсПи (www.s-terra.com) было разработано два решения, позволяющие использовать самые современные технологии Cisco и сертифицированные по требованиям ФСБ России VPN-решения С-Терра СиЭсПи.

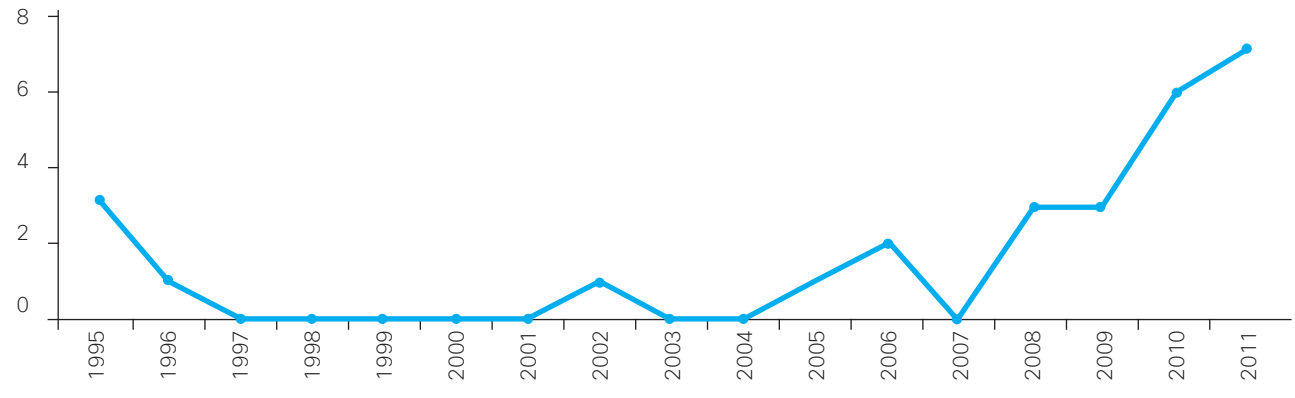

Рисунок 1. Рост числа нормативных актов с требованием использования сертифицированных средств защиты информации

Модуль сетевой модернизированный NME-RVPN (MCM)

Исторически первым было разработан модуль NME-RVPN в исполнении MCM. Он предназначен для установки в маршрутизаторы Cisco ISR первого и второго поколений (Cisco ISR серий 2800/3800 и Cisco ISR серий 2900/3900). Компании Cisco и С-Терра СиЭсПи предложили российским потребителям уникальное устройство, позволяющее обеспечить как эффективную обработку различных видов трафика (данных, голоса, видео), так и их защиту в соответствии с требованиями регулирующих органов (рис. 2).

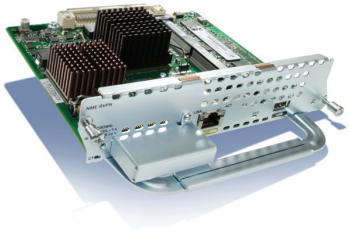

Рисунок 2.
Модуль сетевой модернизированный NME-RVPN (MCM)

При этом маршрутизаторы Cisco ISR G2 с модулем NME-RVPN обладают унифицированным управлением, используя графический интерфейс и интерфейс командной строки (CLI) Cisco для формирования правил маршрутизации и защиты сетевых взаимодействий. Подобная глубокая интеграция позволяет существенно уменьшить сложность ИТ-инфраструктуры, не предъявлять дополнительных требований к квалификации персонала и, как результат, снизить затраты на развертывание и поддержку, а также сроки развертывания подсистемы криптографической защиты информации.

Высокопроизводительное VPN-решение на базе Cisco UCS C-200

Вторым совместным решением стало создание программно-аппаратного комплекса на базе вычислительной платформы Cisco UCS C-200 и сертифицированного программного обеспечения S-Terra CSP VPN Gate. Данное решение обеспечивает самую высокую среди всех российских VPN-решений производительность – свыше 3,1 Гбит/с. При этом данный показатель может быть увеличен до 10 Гбит/с за счет использования серверов Cisco UCS B Series (рис. 3).

Рисунок 3.
Вычислительная платформа Cisco UCS C200

Сертификация

Модуль Cisco NME-RVPN (MCM), производимый на территории Российской Федерации по согласованному с ФСБ России порядку производства, а также вычислительная платформа Cisco UCS C-200 с программным обеспечением CSP VPN Gate версии 3.1 сертифицированы как средство криптографической защиты информации и соответствуют «Требованиям к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» ФСБ России. Решения соответствуют требованиям к средствам криптографической защиты информации класса КС1/КС2 в зависимости от комплектации. Программное обеспечение CSP VPN Gate 3.1 обладает сертификатом соответствия ФСТЭК России, который подтверждает оценочный уровень доверия ОУД 3+, соответствие 3-му уровню контроля отсутствия недекларированных возможностей, соответствие 3-му классу для межсетевых экранов и возможность использования при создании автоматизированных систем до класса защищенности 1Г включительно и информационных систем персональных данных (ИСПДн) до 1 класса включительно. Маршрутизатор Cisco ISR и ISR G2 также сертифицирован в ФСТЭК как межсетевой экран, соответствующий 3-му классу защищенности.

Сценарии применения

Функциональность модуля NME-RVPN и вычислительной платформы UCS C-200 и достигнутый уровень сертификации позволяет применять их для защиты:

- конфиденциальной информации органов государственной власти в соответствии с СТР-К, а также совместным приказом ФСБ и ФСТЭК от 31 августа 2010 года № 416/489,
- подключения информационных систем государственных органов к Интернету

в соответствии с Указом Президента РФ от 17 марта 2008 года № 351, Постановлением Правительства РФ от 18 мая 2009 года № 424, Приказом ФСО от 7 августа 2009 года № 487,

- кредитных организаций в соответствии с требованиями СТО БР ИББС,
- персональных данных в соответствии с методическими рекомендациями ФСБ по защите персональных данных, а также в соответствии с отраслевыми стандартами Банка России, НАУФОР, НАПФ, операторов связи и др.,
- объектов инфраструктуры в соответствии с нормативными документами ФСТЭК России по защите ключевых систем информационной инфраструктуры,
- систем управления технологическими процессами (АСУ ТП),
- крупных территориально-распределенных сетей и т. п.

Кроме того, эти решения могут использоваться операторами связи для оказания услуг Managed VPN Services.

С точки зрения технологических сценариев применения указанные решения компаний Cisco и С-Терра СиЭсПи могут использоваться для:

- защиты высокоскоростных каналов связи (включая магистральные),
- построения филиальной сети,
- построения VPN-узла доступа центрального офиса,
- использования в качестве концентратора удаленного VPN-доступа,

Таблица 1. Преимущества VPN-решений Cisco и С-Терра СиЭсПи

Преимущество	Описание
Стандартизация	Полная и протестированная поддержка протоколов и алгоритмов IPSec (RFC 2401-RFC 2412), IKE (включая расширения – DPD, XAUTH и т.д.), ГОСТ 28147-89, RFC 2628, RFC 4357, MS CryptoAPI и др., обеспечивающая совместимость с решениями третьих фирм.
Совместимость с существующей сетевой инфраструктурой Cisco	Протестированная интеграция с маршрутизатором Cisco ISR G1 и G2, вычислительной платформой Cisco UCS, IP-телефонией Cisco, решениями Cisco TelePresence и Cisco Tandberg, беспроводными решениями и т.д. Поддержка GRE, NAT, VLAN 802.1q и т.д.
Высокая производительность и масштабируемость	Пиковая производительность до 95 Мбит/с на модуле NME-RVPN и до 3,1 Гбит/с на Cisco UCS C-200. Возможность построения решения для каналов до 10 Гбит/с на базе Cisco UCS B Series. Возможность построения высокоскоростных решений на относительно низкопроизводительных (недорогих) платформах.
Высокая надежность и отказоустойчивость	Отказоустойчивость сети (множество сценариев обеспечения надежности). Высокая утилизация вычислительных мощностей (резервные шлюзы не простаивают). Малая (регулируемая) деградация производительности кластера шлюзов при единичном отказе.
Поддержка качества сетевого обслуживания (QoS)	Возможность построения и поддержка качества функционирования мультисервисных сетей. Защита IP-телефонии и видеоконференцсвязи. Устойчивая работа медийных сервисов в условиях избыточной загрузки системы трафиком данных. Поддержка спутниковых каналов.
Централизованное и удаленное управление	Централизованное управление с помощью собственной консоли управления. Управление с помощью CLI. Единая платформа управления для коммуникационного оборудования Cisco, средств защиты Cisco и VPN-шлюзов С-Терра СиЭсПи – Cisco Security Manager.
Интеграция с PKI	Применение единой ключевой системы для прикладных систем (например, документооборота) и сетевой защиты. Удобство, простота администрирования и масштабируемость ключевой системы. Поддержка PKCS#7,10,12, X.509 v.3 (RSA, DSA, ГОСТ), CRL, LDAP. Протестированная интеграция с MS CA, КриптоПро УЦ, NotaryPRO, Keon и др.
Мониторинг и аудит безопасности	Централизация мониторинга и аудита. Поддержка SNMP и Syslog. Применение мощных современных индустриальных платформ мониторинга и аудита, например, CiscoWorks LMS, HP OpenView, Tivoli и др.
Простота эксплуатации и низкая TCO	Удобство и простота эксплуатации. Экономия затрат на эксплуатацию. Единство технологического процесса для эксплуатации средств защиты информации и коммуникаций. Непрерывность бизнес-процессов.
Обучение специалистов	Авторизованный учебный курс по сетевой информационной безопасности в решении Cisco с учебным разделом по продуктам С-Терра СиЭсПи
Сертификация	Сертификат ФСБ – СКЗИ КС1/КС2 Сертификат ФСТЭК – 3-й уровень НДВ, 3-й класс МСЭ, ОУД 3+ Применение в АС класса 1Г и в ИСПДн 1-го класса включительно

- защиты ПК удаленного (мобильного) пользователя,
- защиты беспроводных сетей,
- защиты решений на базе унифицированных коммуникаций (видеоконференцсвязи, IP-телефонии, TelePresence и т.д.),
- защиты спутниковых каналов и т.д.

Преимущества

В таблице 1 перечислены ключевые преимущества VPN-решений Cisco и С-Терра СиЭсПи – модуля NME-RVPN для ISR и вычислительной платформы UCS C-200.

Заключение

Рассмотренные в этой брошюре VPN-решения – модуль сетевой модернизированный Cisco NME-RVPN и вычислительная платформа Cisco UCS C-200, которые разработаны компаниями Cisco и С-Терра СиЭсПи, – это инновационные решения, не только обеспечивающие всю необходимую для VPN-решения функциональность, но и полностью соответствующие требованиям регулирующих органов к средствам криптографической защиты. С помощью указанных решений можно не только выполнить требования по безопасности, указанные в Государственной программе «Информационное общество (2012-2020)», но и соблюсти требования отраслевых (например, СТО БР ИББС) и корпоративных стандартов в области построения виртуальных частных сетей.

Дополнительная информация

Дополнительные сведения о сертифицированных в ФСБ России криптографических решениях Cisco могут быть получены на сайте Cisco: **www.cisco.ru/go/rvpn**

Cisco
Россия,115054, Москва
бизнес-центр «Риверсайд Тауерс»
Космодамианская наб., 52, стр.1, 4-й этаж
Телефон: +7 (495) 961 1410
Факс: +7 (495) 961 1469
www.cisco.ru
www.cisco.com

Cisco
Россия, 197198, Санкт-Петербург
бизнес-центр «Арена Холл»
пр. Добролюбова, 16, лит. А, кор. 2
Телефон: +7 (812) 313 6230
Факс: +7 (812) 313 6280
www.cisco.ru
www.cisco.com

Cisco
Россия, 630099, Новосибирск
бизнес-центр «Росевроплаза»
Димитрова пр-т, 2, 5-й этаж
Телефон.: +7 (383) 230 2670
Факс: +7 (383) 230 1795
www.cisco.ru
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**