РЕШЕНИЯ CISCO SYSTEMS ДЛЯ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ СТР-К

ЧТО ТАКОЕ СТР-К?

«Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К) - это нормативно-методический документ, устанавливающий порядок организации работ, требования и рекомендации по обеспечению технической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (далее - конфиденциальная информация) на территории Российской Федерации.

Требования и рекомендации настоящего документа распространяются на защиту государственных информационных ресурсов некриптографическими методами, направленными на предотвращение утечки защищаемой информации по техническим каналам, от несанкционированного доступа к ней и специальных воздействий на информацию в целях ее уничтожения, искажения и блокирования. И хотя при проведении работ по защите негосударственных информационных ресурсов, составляющих коммерческую, банковскую, служебную и иные виды тайн (кроме государственной), требования настоящего документа носят рекомендательный характер, многие организации учитывают положения СТР-К при обеспечении информационной безопасности своих корпоративных и ведомственных сетей.

Компания Cisco Systems, являясь лидером не только мирового, но и российского рынка средств обеспечения информационной безопасности, предлагает государственных, коммерческим и иным типам организаций, работающих на территории России, широкий спектр защитных решений, учитывающих большинство требований СТР-К.

ТРЕБОВАНИЯ СТР-К И МЕТОДЫ ИХ РЕАЛИЗАЦИИ

Применение сертифицированных средств защиты информации

Согласно п.2.16 СТР-К, используемые средства защиты должны иметь сертификат Федеральной службы по техническому и экспортному контролю (ФСТЭК). Для выполнения этого требования компания Cisco Systems сертифицировала свои:

- межсетевые экраны Cisco Pix и Catalyst FWSM,
- маршрутизаторы с ОС Cisco IOS,
- коммутаторы Cisco Catalyst,
- сетевые и хостовые системы предотвращения атак Cisco IPS 42xx, Catalyst IDSM-2 и Cisco Security Agent,
- а также систему управления CiscoWorks VPN/Security Management Solution

на соответствие соответствующим руководящим документам и техническим условиям, принятым Федеральной службой по техническому и экспортному контролю (бывшая Государственная техническая комиссия при Президенте России).

Общее число выданных ФСТЭК компании Cisco Systems сертификатов давно превысило 100, что существенно превышает число сертификатов, полученных какой-либо другой компанией (российской или зарубежной), работающей на рынке информационной безопасности.

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Контролируемость защитных средств

Для регулярного (не реже одного раза в год) контроля состояния защиты информации (п.3.24), осуществляемой службой безопасности организации, компания Cisco Systems предлагает специализированное решение Cisco Security Auditor, которое предназначено для автоматизированного аудита и контроля безопасности сотен сетевых устройств и средств защиты, разбросанных по корпоративной сети защищаемого предприятия. Такая проверка позволяет оценить:

- соблюдение требований нормативно-методических документов по защите информации;
- работоспособность применяемых средств защиты;
- знания и выполнение персоналом своих функциональных обязанностей в части защиты информации.

Cisco Security Auditor может осуществлять свои проверки на соответствие заранее определенной ведомственной политике безопасности, а также лучшим в отрасли стандартам защищенной настройки решений компании Cisco (SAFE, NSA, CIS). По итогам проверки Security Auditor создает отчеты с практическими рекомендациями по устранению обнаруженных уязвимостей и слабостей в настройке сетевого оборудования и средств защиты.

Таблица 1. Основные возможности Cisco Security Auditor

Основные возможности	
• Поддержка Cisco Pix, маршрутизаторов и коммутаторов Cisco различных серий • Функционирование под управлением Windows 2000 или Windows 2003 • Web-ориентированное управление CiscoWorks VPN/Security Management Solution (VMS)	• Поддержка CiscoWorks RME, Common Service DCR и т.д. • Поддержка браузеров MS Internet Explorer, Netscape Navigator и Mozilla • Различные варианты отчетов – от высокоуровневых графических до технологических уровня конкретных устройств

Защита информации при использовании съемных накопителей

Для реализации требования 5.5.4 СТР-К, согласно которому на рабочих местах во время работы с конфиденциальной информации накопители (PCMCIA, USB, CD-RW) должны быть «закрыты на запись», компания Cisco Systems предлагает персональную систему защиты персональных компьютеров Cisco Security Agent (CSA). Это решение, предназначенное для серверов и рабочих станций, работающих под управлением ОС Windows, Solaris и Linux, объединяет различные защитные механизмы и функции в одном решении – предотвращение атак, персональный межсетевой экран, защита от вредоносного кода, контроль целостности, блокирование утечки информации через USB-порты и другие внешние устройства (PCMCIA, CD, Floppy, Zip и другие), ограничение возможностей Интернет-пейджеров (например, ICQ), обнаружение перехватчиков с клавиатуры и т.п.

CSA позволяет отражать широкий спектр нападений – сканирование портов, переполнение буфера, троянцы и черви, DoS-атаки и других. При этом CSA построен по совершенно иному принципу, чем традиционные антивирусы и системы обнаружения атак и не использует сигнатуры для идентификации несанкционированных действий. Это в свою очередь обеспечивает защиту компьютера от неизвестных атак, сигнатуры для которых пока не написаны и отсутствуют в базах традиционных средств защиты.

Таблица 2. Основные возможности Cisco Security Agent

Основные возможности	
• Интеграция с ведомственными базами пользователей Active Directory, LDAP, NIS • Автоматическая смена политики контроля в зависимости от	• Управление 100.000 агентами с одной консоли управления • Инвентаризация установленного ПО • Интеграция с VPN-клиентами компаний Cisco и Check Point

© 2004 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com

имени пользователя и его местоположения в сети • 2 типа корреляции событий безопасности • Прозрачность установки, не требующая участия пользователя компьютера • Автоматизация создания политик контроля	• Интеграция с механизмами сетевого контроля доступа (Network Admission Control) • Делегирование отдельных функций управления агентом пользователю • Возможность функционирования в автономном режиме

Защита информации в локальной вычислительной сети (ЛВС)

Характерными особенностями ЛВС являются распределенное хранение информации, ее удаленная обработка и передача, а также сложность проведения контроля за работой пользователей и общей защищенностью ЛВС. Для защиты всех узлов защищаемой ЛВС (п.5.6.3), включающей не только рабочие станции и сервера, но и коммутаторы, компания Cisco предлагает целый ряд сертифицированных решений – Cisco Security Agent, Cisco FWSM и Cisco IDSM-2.

Сервисный модуль FWSM, реализующий функции межсетевого экрана, – это высокопроизводительное, интегрированное защитное решение для коммутаторов Catalyst 6500 и маршрутизаторов Cisco 7600. Этот модуль обеспечивает самую высокую в индустрии производительность – 5,5 Гбит/сек (с возможностью увеличения до 20 Гбит/сек), 1 миллион одновременно обрабатываемых соединений, 100000 соединений в секунду. Данное уникальное решение, не имеющее аналогов на рынке, ориентировано на защиту центров обработки данных и других критичных сегментов ЛВС.

Таблица 3. Основные возможности Cisco Firewall Service Module

Основные возможности	
• Базируется на зарекомендовавшей временем операционной системе реального времени PixOS • Поддержка до 4096 VLAN на один модуль • Создание политик для отдельных VLAN • Механизм виртуализации (до 100 виртуальных межсетевых экранов) • Тесная интеграция с модулями обнаружения атак, построения IPSec VPN и работы с SSL • Защита от подмены MAC/IP адресов (ARP Spoofing)	• Отказоустойчивость и высокая доступность • Возможность ограничения использования ресурсов • Ролевое управление конфигурацией модуля • Группирование сетевых объектов и сервисов для списков контроля доступа (ACL) • Масштабирование до 4-х модулей на один коммутатор • Снижение совокупной стоимости владения за счет интеграции FWSM в уже установленные в сети Catalyst 6500

Компания Cisco Systems – самый известный производитель в мире, выпускающий решение по обнаружению и предотвращению атак, интегрируемое в коммутаторы локальных сетей. Модуль IDSM-2, разработанный Cisco, устанавливается в шасси коммутатора Catalyst 6500 и обеспечивает мониторинг сетевых соединений, проходящих через него.

Таблица 4. Основные возможности Cisco Intrusion Detection Module

Основные возможности	
• Базируется на зарекомендовавшем временем программном коде системы Cisco IDS/IPS • Производительность – 600 Мбит/сек, 500.000 одновременно обрабатываемых соединений • Отсутствие снижения производительности коммутатора • Отражение атак канального уровня • Возможность мониторинга неограниченного контроля сетевых сегментов и VLAN	• Защищенное обновление сигнатур атак • Разрыв соединения, а также реконфигурация межсетевого экрана, маршрутизатора или коммутатора для блокирования атаки • Тесная интеграция с модулями межсетевого экранирования и построения IPSec VPN и обработки SSL • Единое управление с сенсорами Cisco IDS/IPS, межсетевыми экранами и средствами построения VPN

© 2004 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com

• Мониторинг отказов соединения, сервиса и устройства	• Управление с помощью IDS Device Manager или CiscoWorks VPN Security Management Solution

Для управления, распределения и контроля защищенности системных ресурсов в защищаемой ЛВС (п.5.6.5), компания Cisco Systems предлагает следующие защитные решения – Cisco Security Auditor, Cisco FWSM и CiscoWorks VPN/Security Management Solution.

CiscoWorks VPN Security Management Solution (VMS) является централизованным инструментом настройки, мониторинга и отладки всех решений по безопасности компании Cisco – средств построения VPN, межсетевых экранов, сетевых и хостовых систем предотвращения атак и т.д. Основными компонентами системы являются:

Инструменты управления:

- CiscoWorks Management Center for Firewalls,
- CiscoWorks Management Center for IDS Sensors,
- CiscoWorks Management Center for VPN Routers,
- CiscoWorks Management Center for Cisco Security Agents,
- CiscoWorks Auto Update Server.

Инструменты мониторинга:

- CiscoWorks Monitoring Center for Security,
- CiscoWorks Monitoring Center for Performance
- CiscoWorks Resource Manager Essentials.

В отличие от встроенных в каждое защитное устройство собственных систем управления (Cisco Pix Device Manager, Cisco Security Device Manager и Cisco IDS Device Manager) CiscoWorks VMS, имеющий удобный графический Web-интерфейс, позволяет эффективно настраивать и контролировать десятки и сотни средств защиты, что достигается за счет механизма их группирования.

Таблица 5. Основные возможности CiscoWorks VMS

Управление МСЭ Cisco Pix и Catalyst FWSM	Управление Cisco IDS/IPS, NM-IDS и IDSM-2
• Управление до 1000 МСЭ Cisco Pix • Уникальный механизм создания правил Smart Rules, сокращающий время настройки групп межсетевых экранов • Группирование МСЭ по различным признакам (география, тип, владелец и др.) • Наследование настроек и правил для групп • Автоматическое обновление конфигурации и ОС МСЭ • Периодическая проверка конфигурации удаленных МСЭ	• Управление несколькими сотнями сенсоров с одной консоли • Задание иерархии сенсоров, содержащей группы и подгруппы • 5 ролей администраторов, имеющих доступ к консоли управления • Создание и настройка сигнатур атак • Настройка вариантов реагирования на обнаруженные нападения • Доступ к энциклопедии сетевой безопасности, описывающей все атаки
Управление Cisco Security Agent	**Управление Cisco VPN Router, VPNSM, IOS VPN**
• Управление до 100.000 агентов CSA • Создание и настройка политик контроля • Генерация и распределение дистрибутивов CSA, размещаемых	• Создание, настройка и распределение защитных политик с помощью Smart Rules • Настройка отказоустойчивости

© 2004 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com

на защищаемых ПК без участия их владельца • Группирование агентов	• Ролевое управление доступом к консоли • Импорт конфигурации устройств • Резервирование и восстановление конфигурации VPN-устройств
Мониторинг средств защиты	**Мониторинг производительности**
• Сбор, отображение, анализ, корреляция событий безопасности • Посылка уведомлений • Анализ статистики и генерация отчетов	• Мониторинг состояния всех VPN-устройств (включая VPN 3000, SSLSM, VPNSM и т.д.) • Анализ статистики и генерация отчетов • Обнаружение и изоляция проблем

Защита информации при межсетевом взаимодействии

Для постоянного контроля взаимодействия ЛВС с другими вычислительными сетями (п.5.7) компания Cisco Systems предлагает следующие сертифицированные решения по информационной безопасности – Cisco Pix Firewall, Cisco IPS 4200 Series, Cisco Network Module IDS, Cisco IOS Firewall, Cisco IDSM-2.

Программно-аппаратный межсетевой экран Cisco Pix Firewall – лидер мирового рынка, обеспечивает многоуровневую защиту, используя широкий набор интегрированных защитных возможностей, включая контроль состояния с помощью алгоритма адаптивной защиты Adaptive Security Algorithm и глубокий анализ сетевых и прикладных протоколов с помощью механизма Deep Packet Inspection. Широкий спектр моделей Cisco Pix Firewall, ориентированных на защиту сетей предприятий разного масштаба, обеспечивает их безопасность, производительность и надежность.

Таблица 6. Основные возможности Cisco Pix

Основные возможности	
• Производительность до 1,67 Гбит/сек • Поддержка технологии VPN • Встроенная система обнаружения атак • Фильтрация URL и блокирование ПО для Instant Messaging (IM) и P2P • Поддержка протокола GTP/GPRS • Прозрачный МСЭ второго уровня	• «Виртуальные» МСЭ • Отказоустойчивость (включая поддержание VPN-туннелей) • Скрытие топологии защищаемой сети с помощью трансляция адресов (NAT) и портов (PAT) • Контроль всего спектра протоколов для IP-телефонии и мультимедиа – H.323, SIP, SCCP, MGCP, RTSP и т.д. • Поддержка IPv6

Таблица 7. Модельный ряд Cisco Pix

	Pix 501	Pix 506E	Pix 515	Pix 525	Pix 535
Производительность, Мбит/сек	60	100	190	330	1667
Максимальное число соединений	7500	25.000	130.000	280.000	500.000
Количество одновременно поддерживаемых сессий	19.500	53.000	176.000	625.000	1.000.000
Поддерживаемые физические интерфейсы	1 10/100 Ethernet и 4-хпортовый	2 10/100 Ethernet	До 6 10/100 Ethernet	До 8 10/100/1000 Ethernet	До 10 10/100/1000 Ethernet

© 2004 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com

	Pix 501	Pix 506E	Pix 515	Pix 525	Pix 535
	коммутатор 10/100				

Программное обеспечение Cisco IOS Firewall – это межсетевой экран с контролем состояния, интегрированный в операционную систему Cisco IOS и поддерживаемый на широком спектре моделей маршрутизаторов Cisco 800, 1600, 1700, 1800, 2500, 2600, 2800, 3600, 3700, 3800, 7100, 7200, 7300. Cisco IOS Firewall использует эффективный механизм, называемый Context Based Access Control (CBAC), позволяющий контролировать информационные потоки, проходящие через маршрутизатор, на всех уровнях, начиная с сетевого и заканчивая прикладным. На всех уровнях фильтрация осуществляется динамически, основываясь на направлении трафика, состоянии соединения и информации о предыдущих пакетах и сессиях, пропущенных маршрутизатором с Cisco IOS Firewall.

Таблица 8. Основные возможности Cisco IOS Firewall

Основные возможности	
• Поддержка большого числа протоколов, включая мультимедиа • Поддержка различных механизмов аутентификации - RADIUS, TACACS+ и т.д. • Контроль доступа по времени • Тесная интеграция с механизмами обнаружения атак, контроля качества (QoS) и построения VPN • Поддержка различных политик и списков контроля доступа для разных интерфейсов	• Поддержка анализа протоколов на нестандартных портах • Трансляция сетевых адресов • Блокирование Java-апплетов • Поддержка отказоустойчивости за счет динамической смены маршрута на резервный маршрутизатор • Механизм «прозрачности» МСЭ (функционирование на канальном уровне) • Расширенная регистрация событий безопасности

Cisco IPS 4200 является центральным компонентом решений Cisco Systems по отражению атак. На базе данного ПО построены системы обнаружения атак Cisco IDSM-2 и Cisco IDS Network Module. Наряду с традиционными механизмами в Cisco IDS/IPS используются и уникальные алгоритмы, отслеживающие аномалии в сетевом трафике и отклонения от нормального поведения сетевых приложений. Это позволяет обнаруживать как известные, так и многие неизвестные атаки. Встроенные технологии корреляции событий безопасности Cisco Threat Response, Threat Risk Rating и Meta Event Generator помогают не только существенно снизить число ложных срабатываний, но и позволяют администраторам реагировать только на действительно критичные атаки, которые могут нанести серьезный ущерб ресурсам ведомственной сети.

Таблица 9. Основные возможности Cisco IPS 4200

Основные возможности	
• Широкий спектр алгоритмов обнаружения атак (сигнатуры, аномалии, эвристика, отклонения от RFC и т.п.) • Защита от методов обхода • Возможность работы в двух режимах – обнаружения и предотвращения атак • Обнаружение атак в IP-телефонии • Обнаружение работы Интернет-пейджеров в Web-трафике	• Технология микромодулей T.A.M.E. для каждого типа обнаруживаемых атак • Автоматический выбор реагирования в зависимости от опасности угрозы • Интеграция с IDS/IPS других производителей с помощью протокола SDEE • Производительность – 8 Гбит/сек в кластере

© 2004 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com

Таблица 10. Модельный ряд Cisco IPS 4200

	IDS 4215	IPS 4240	IPS 4255	IDS 4250-XL
Производительность, Мбит/сек	80	250	600	1000
Интерфейс для мониторинга	10/100BASE-Tx	Четыре 10/100/1000BASE-TX	Четыре 10/100/1000BASE-TX	Два 1000BASE-SX с MT-RJ
Опциональный интерфейс для мониторинга	Четыре 10/100BaseTx (всего 5 интерфейсов)	Четыре 10/100/1000BaseTx (всего 8 интерфейсов) или четыре оптических 1000BASE SX	Четыре 10/100/1000BaseTx (всего 8 интерфейсов) или четыре оптических 1000BASE SX	1000BASE-SX (оптика)
Размер шасси	1RU	1RU	1RU	1RU
Дополнительный блок питания	Нет	Нет	Нет	Да
Мониторинг отказов				
• Линии связи	Да	Да	Да	Да
• Соединения	Да	Да	Да	Да
• Сервиса	Да	Да	Да	Да
• Устройства	Да	Да	Да	Да

Cisco IDS Network Module – единственное решение для обнаружения атак, предназначенное для интеграции в маршрутизаторы. Этот модуль, устанавливаемый в слот маршрутизаторов Cisco 2600XM, 2691, 2800, 3660, 3700 и 3800, обнаруживает вредоносную активность в трафике, проходящем через периметр удаленного филиала организации.

Таблица 11. Основные возможности Cisco IDS Network Module

Основные возможности	
• Базируется на зарекомендовавшем временем программном коде системы Cisco IDS/IPS • Производительность – от 10 Мбит/сек для Cisco 2600XM до 45 Мбит/сек для Cisco 3700 • Широкий выбор настраиваемых параметров для каждой сигнатуры атак • Поддержка трафика VLAN 802.1q • Интеграция со всеми защитными функциями операционной системы IOS маршрутизатора • Автоматизированное обновление сигнатур	• Мониторинг отказов соединения, сервиса и устройства • Разрыв соединения, а также реконфигурация межсетевого экрана, маршрутизатора или коммутатора для блокирования атаки • Защищенное управление с помощью SSH, SSL и IPSec • Единое управление с сенсорами Cisco IDS/IPS, межсетевыми экранами и средствами построения VPN • Управление с помощью IDS Device Manager или CiscoWorks VPN Security Management Solution

© 2004 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com

Сегментация трафика с учетом решаемых пользователем задач (п.5.7.3) и подключение ЛВС к другим автоматизированным системам (п.5.7.4) осуществляется с помощью сертифицированного механизма виртуальных локальных частных сетей (VLAN) и сертифицированных межсетевых экранов Cisco Pix, Cisco FWSM и Cisco IOS Firewall.

Защита информации при работе с базами данных

Согласно п.5.8.2 при выборе СУБД рекомендуется ориентироваться на операционные системы и СУБД, включающие штатные сертифицированные средства защиты информации от НСД либо имеющие соответствующие сертифицированные дополнения в виде СЗИ НСД. Таким дополнением может являться Cisco Security Agent. В этом случае выбираемая СУБД должна функционировать под управлением любой из перечисленных операционных систем – Windows 2000, Windows 2003, Linux, Solaris.

Защита информации при взаимодействии с сетями общего пользования

При подключении защищаемых абонентов к информационным сетям общего пользования СТР-К рекомендует следующие методы обеспечения безопасности (п.6.1.4):

- Межсетевое экранирование
- Мониторинг вторжений
- Анализ защищенности
- Использование аутентификации
- Применение средств антивирусной защиты
- Централизованное управление системой информационной безопасности.

Межсетевые экраны Cisco Pix, Cisco FWSM и Cisco IOS Firewall позволяют

- Предотвратить необоснованное подключение технических средств (серверы, рабочие станции), имеющих выход в сети общего пользования к другим техническим средствам или сетям (п.6.3.10).
- Обеспечить фильтрацию входящих/исходящих сетевых пакетов по по правилам, заданным администратором безопасности (п.6.3.12.1).
- Скрыть внутреннюю структуру защищаемой сети (п.6.3.12.1).
- Блокировать предоставление не определенных в политике безопасности сервисов (п.6.3.13.2 и 6.3.14.2).

Системы обнаружения вторжений Cisco IPS 4200, Cisco IDSM-2, Cisco NM-IDS позволяют осуществлять активный аудит безопасности на предмет обнаружения в режиме реального времени несанкционированной сетевой активности (п.6.3.12.1).

Анализ принимаемой из сетей общего пользования информации, в т.ч. и на наличие компьютерных вирусов (п.6.3.12.1), осуществляют системы предотвращения вторжений компании Cisco (Cisco IPS 4200, Cisco IDSM-2, Cisco NM-IDS), система персональной защиты Cisco Security Agent, а также устройства Content Engine и Content Engine Network Module.

Устройства Content Engine с программным обеспечением Cisco Application and Content Networking System (ACNS) помогают организациям любого размера снизить опасность, которую несет доступ в Интернет по протоколу HTTP. Content Engine, помимо кэширования данных, решают 3 основные задачи:

- Аутентификацию пользователей
- Контроль содержимого Интернет-трафика (HTTP, FTP, HTTPS и т.д.)
- Интеграцию с антивирусными решениями по протоколу ICAP (Internet Content Adaptation Protocol).

© 2004 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com

Таблица 12. Основные возможности Cisco Content Engine

Основные возможности	
• Контроль всех действий сотрудников в сети Интернет • Методы аутентификации – RADIUS, TACACS+, NTLM, LDAP (включая расширения) и Active Directory • Фильтрация Web-трафика с помощью Websense, SmartFilter или N2H2 • Прозрачность для пользователей • Ограничение доступа к сетевым приложениями/ресурсам (например, Web-серверам) на основе имени пользователя или группы, а также по времени	• Обнаружение и блокирование использования Интернет-пейджеров (например, ICQ), P2P-сетей и IRC-чатов • Ограничение полосы пропускания для отдельных приложений/сервисов • Перенаправление трафика на антивирусные и фильтрующие сервера TrendMicro, Symantec, SurfControl, Finjan • Большое число отчетов о деятельности сотрудников в сети Интернет

Cisco Content Engine Network Module – единственное решение для фильтрации Web-трафика и аутентификации пользователей, обращающихся в Интернет, предназначенное для интеграции в маршрутизаторы. Этот модуль, устанавливаемый в слот маршрутизаторов Cisco 2600, 2800, 3700 и 3800, обнаруживает нарушения политики безопасности в трафике, проходящем через периметр удаленного филиала или небольшого офиса.

Таблица 13. Основные возможности Cisco Content Engine Network Module

Основные возможности	
• Базируется на зарекомендовавшем временем программном коде устройства Cisco Content Engine • Кэширование и ускорение обработки Web-трафика • Интеграция со всеми защитными функциями операционной системы IOS маршрутизатора	• Поддержка протокола WCCP (Web Cache Communication Protocol) • Оптимизация распределения файлов и программного обеспечения большого объема • 3 модели с жестким диском в 40 или 80 Гб, а также SCSI-интерфейсом для подключения внешнего дискового массива

Для защиты небольших предприятий или удаленных филиалов ведомств компания Cisco Systems предлагает многофункциональные адаптивные защитные устройства Cisco ASA 5500 Series, объединяющие в одном комплексе межсетевой экран (на базе Cisco Pix), систему предотвращения атак (на базе Cisco IPS 4200), средство построения VPN и другие защитные механизмы. Гибкая архитектура Cisco ASA 5500 Series позволяет легко расширить эти устройства новыми возможностями, например, антивирусом, антиспамом, контролем содержимого, защитой от атак типа «фишинг» и др.

Таблица 14. Основные возможности Cisco ASA 5500

Основные возможности	
• Встроенный сетевой антивирус • Возможность построения IPSec и SSL VPN (на базе Cisco VPN 3000 Series) • Неограниченная расширяемость за счет использования специальных модулей Security Services Module (SSM) • Всесторонняя инспекция потоков на 2-7 уровнях на базе механизма Deep Packet Inspection • Фильтрация URL • Защита от шпионского и рекламного ПО и широкого спектра	• Поддержка механизмов Risk Rating и Meta Event Generator • Поддержка «виртуальных» и прозрачных межсетевых экранов • Поддержка протоколов OSPF, PIM, IPv6 и др. • Различные механизмы обеспечения отказоустойчивости • Поддержка технологии VLAN и QoS • Единое управление всеми защитными механизмами с помощью Adaptive Security Device Manager

© 2004 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com

других атак с помощью технологии Anti-X	

Таблица 15. Модельный ряд Cisco ASA 5500

	ASA 5510	ASA 5520	ASA 5540
Производительность МСЭ, Мбит/сек	300	450	650
Производительность про параллельном использовании МСЭ, IPS и других защитных модулей, Мбит/сек	До 150 с AIP-SSM-10	До 375 с AIP-SSM-20	До 450 с AIP-SSM-20
Максимальное число соединений	64.000	130.000	280.000
Физические интерфейсы	5 Fast Ethernet	4 Gigabit Ethernet + 1 Fast Ethernet	4 Gigabit Ethernet + 1 Fast Ethernet

Для проверки подлинности удаленных пользователей и управления доступом к защищаемым ресурсам с помощью атрибутов безопасности (п.6.3.13.1) компания Cisco Systems предлагает систему аутентфикации Cisco Cisco Secure Access Control Server (ACS). Это программное или программно-аппаратное решение, предназначенное для централизованной идентификации, аутентификации, авторизации и управления доступом. При этом данные защитные механизмы реализуются через все устройства и решения компании Cisco Systems. При помощи ACS можно управлять доступом на маршрутизаторах и коммутаторах, средствах построения VPN и межсетевых экранах, узлах IP-телефонии и беспроводных точках и клиентах, устройствах хранения и контроля контента, а также на различных типах удаленного доступа (широкополосный, DSL, dialup) и т.д.

Таблица 16. Основные возможности Cisco Secure Access Control Server

Основные возможности	
• Поддержка аутентификации LDAP и ODBC, Active Directory и NDS, RADIUS и TACACS+, CHAP и MS-CHAP, PAP и ARA, и т.д. • Поддержка стандарта 802.1x (режимы EAP-TLS, PEAP, Cisco LEAP, EAP-FAST и EAP-MD5 • Авторизация команд на устройствах • Ограничение доступа по времени, числу сессий и другим контролируемым параметрам • Создание профилей пользователей и групп • Интеграция с решениями для однократных паролей и токенов	• Возможность проверки дополнительных условий перед разрешением доступа в сеть • Интеграция с технологией контроля доступа в сеть Network Admission Control • Интеграция с PKI и поддержка списка отозванных сертификатов (CRL) • Регистрация всех попыток доступа пользователей • Генерация отчетов • Возможность поставки в виде специального устройства с защищенной ОС

Регистрация действий пользователей и обслуживающего персонала

В п.5.1.3 СТР-К указано требование регистрации попыток несанкционированного доступа. Такая регистрация необходима для контроля несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц. Любое решение компании Cisco Systems в области информационной безопасности – системы предотвращения атак, межсетевые экраны, системы аутентификации, системы контроля содержимого и т.д., содержат в себе расширенные механизмы регистрации позволяющие фиксировать все необходимую для внутреннего аудита информацию – дату и время наступления события, адреса

© 2004 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com

или имена пользователей, связанных с событием (атакуемые или атакующие), а также дополнительные детали вплоть до записи всего сетевого трафика, в котором зафиксированы следы несанкционированной активности.

Централизованное управление системой информационной безопасности

Для реализации централизованного управления системой информационной безопасности, прописанного в пп.5.6.5 и 6.1.4, компания Cisco Systems предлагает 2 решения – CiscoWorks VPN/Security Management Solution (VMS) и Cisco Monitoring, Analysis and Response System (MARS).

Программно-аппаратный комплекс Cisco MARS предназначен для управления угрозами безопасности. В качестве источников информации о них могут выступать - сетевое оборудование (маршрутизаторы и коммутаторы), средства защиты (межсетевые экраны, антивирусы, системы обнаружения атак и сканеры безопасности), журналы регистрации ОС (Solaris, Windows NT, 2000, 2003, Linux) и приложений (СУБД, Web и т.д.) , а также сетевой трафик (например, Cisco Netflow). Cisco MARS поддерживает решения различных производителей – Cisco, ISS, Check Point, Symantec, NetScreen, Extreme, Snort, McAfee, eEye, Oracle, Microsoft и т.д.

Механизм ContextCorrelation™ позволяет проанализировать и сопоставить события от разнородных средств защиты. Визуализация их на карте сети в реальном времени достигается с помощью механизма SureVector™. Данные механизмы позволяют отобразить путь распространения атаки в реальном режиме времени. Автоматическое блокирование обнаруженных атак достигается с помощью механизма AutoMitigate™, который позволяет реконфигурировать различные средства защиты и сетевое оборудование.

Таблица 17. Основные возможности Cisco MARS

Основные возможности	
• Обработка до 10000 событий в секунду или свыше 300000событий Netflow в секунду • Сигнатурные и «поведенческие» методы обнаружения аномалий и других атак • Возможность создания собственных правил корреляции	• Эскалация инцидентов (идентификация, реагирование, расследование, контроль, генерация отчетов) • Уведомление об обнаруженных проблемах по e-mail, SNMP, через syslog и на пейджер • Ролевое управление через Web-интерфейс

Обучение персонала

Для обучения назначенных лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации (п.3.16) компания Cisco Systems предлагает авторизованное обучение по целому ряду программ и курсов в области информационной безопасности. Такое обучение можно пройти в в авторизованных учебных центрах компании Cisco Systems, а также в сетевых академиях Cisco Systems (Cisco Networking Academy), расположенных на территории России.В данных учебных центрах:

- Используются различные формы обучения: очная, заочная (дистанционная), индивидуальная.
- Преподавательский состав представлен инструкторами, имеющими звания CCSI (Certified Cisco Systems Instructor), имеющими большой опыт практической работы в разработке и обслуживании сетей в России и за рубежом, а также имеющими квалификационное звание CCIE (Cisco Certified Internetwork Expert).
- Осуществляется подготовка к сдаче квалификационных экзаменов по программе Cisco Career Certification.

По информационной безопасности компания Cisco Systems предлагает две сертификации, ценящиеся во всем мире:

- Cisco Certified Internetwork Expert (CCIE Security)
- Cisco Certified Security Professional (CCSP)

© 2004 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com

ЗАКЛЮЧЕНИЕ

Защита информации, обрабатываемой с использованием технических средств в государственных и негосударственных информационных системах, является составной частью работ по созданию и эксплуатации объектов информатизации различного назначения и должна осуществляться в виде комплексной системы обеспечения информационной безопасности. Компания Cisco Systems, в отличие от других поставщиков, предлагает своим заказчикам не точечные продукты для защиты отдельных участков автоматизированной системы и ее абонентов, а комплексное решение, интегрируемое в инфраструктуру ведомства для обеспечения безопасности речевая информации и информации, обрабатываемой техническими средствами.

Self-Defending Network (SDN) – стратегия компании Cisco Systems, нацеленная на защиту информационных ресурсов в условиях растущей угрозы со стороны вредоносных программ, закладочных устройств и нарушителей, воздействующих на автоматизированную систему предприятия изнутри и извне. Учитывая скорость распространения современных угроз, например червей и вирусов, средства защиты компании Cisco Systems строятся на основе проактивного подхода, заключающегося в предвосхищении угроз, а не в борьбе с их последствиями. В основе SDN лежит интеграция механизмов безопасности в сетевую инфраструктуру, в которой все ее элементы – от персонального компьютера до сетевого оборудования, участвуют в процессе обеспечения защищенности, устойчивости и непрерывности бизнеса. Стратегия Self-Defending Network заключается в автоматизации процесса обеспечения информационной безопасности за счет обнаружения угроз, реагирования соответственно уровню критичности, изолирования зараженных или взломанных узлов, и реконфигурации сетевых устройств с целью предотвращения повторных атак.

ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ

Решения Cisco Systems по информационной безопасности

http://www.cisco.com/go/security

© 2004 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com

Cisco Systems
Россия, 113054 Москва
бизнес центр “Риверсайд Тауэрз”
Космодамианская наб., 52
Стр. 1, 4-й этаж
Тел.: +7 (095) 961 14 10
Факс: +7 (095) 961 14 69
Internet: www.cisco.ru
www.cisco.com

Cisco Systems
Казахстан, 480099 Алматы
бизнес центр “Самал 2”
Ул. О. Жолдасбекова, 97
блок А2, этаж 14
Тел.: +7 (3272) 58 46 58
Факс: +7 (3272) 58 46 60
Internet: www.cisco.ru
www.cisco.com

Cisco Systems
Украина, 252004 Киев
бизнес центр “Горайзон Тауэрз”
Ул. Шовковична, 42-44, этаж 9
Тел.: (044) 490 36 00
Факс: (044) 490 56 66
Internet: www.cisco.ua
www.cisco.com

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on
Cisco Connection Online Web site at http://www.cisco.com/
http://www.cisco.ru/

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems Inc. All rights reserved. Printed in Russia. Cisco IOS is the trademark; and Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners.