

Защищенные сети без границ



Стратегия
Cisco

Новые
продукты

Рекомендации
по внедрению

Оценка
соответствия

Импорт и локальное
производство

Аналитика
и исследования



ЧТО НОВОГО ПРЕДЛАГАЕТ CISCO
В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Защищенные сети без границ



ЧТО НОВОГО ПРЕДЛАГАЕТ CISCO
В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стратегия
Cisco

Новые
продукты

Рекомендации
по внедрению

Оценка
соответствия

Импорт и локальное
производство

Аналитика
и исследования



Концепция «Сети без границ» 4.0

В «Глобальном отчете Cisco по сетевым технологиям за 2010 год» (Cisco Connected Technology World Report - 2010) говорится о стремительном росте популярности работы в любой точке мира с помощью любого устройства по выбору сотрудника. При этом, говорится в отчете, резко растет спрос на использование видео для усовершенствования коммуникаций.

В полном соответствии со спросом Cisco предлагает заказчикам сетевые технологии и услуги (а также услуги своих партнеров), позволяющие ИТ-специалистам реализовать централизованное управление и автоматизировать процессы обеспечения безопасности и контроля доступа для любого устройства в своей организации, а также внедрить услуги видео- и голосовой связи в рамках новых бизнес-процессов.

«Сети без границ» (Borderless Network) – это полномасштабная архитектура, включающая решения в области маршрутизации, коммутации, обеспечения мобильности, информационной безопасности и оптимизации работы приложений в глобальных сетях. В апреле 2011 года был анонсирован новый, уже четвертый этап в развитии концепции «Сети без границ».

Архитектура SecureX

Появление организаций без границ существенно изменило представления о способах, времени и месте работы. В результате возникла необходимость пересмотра структуры и методов внедрения систем информационной безопасности. Этот процесс подстегнула новая волна мобильности, виртуализации и «облачных» вычислений, поставившая перед ИТ-специалистами многомерную комплексную проблему и заставившая их по-новому подойти к внедрению правил информационной безопасности и гарантиям их соблюдения.

Чтобы дать компаниям возможность вести бизнес без границ, Cisco предложила в феврале 2011 года новую архитектуру безопасности SecureX, позволяющую объединить межсетевые экраны, VPN-решения, средства предотвращения вторжений и системы контентной фильтрации в единый защитный комплекс, управляемый с помощью политик, учитывающих контекст и способных адаптироваться к требованиям бизнеса.

Используемые в архитектуре SecureX элементы защиты не зависят от физической инфраструктуры и могут быть реализованы как в виде отдельных устройств или модулей в сетевое оборудование, так и в виде виртуальных защитных систем или облачных услуг.

Защищенные сети без границ



ЧТО НОВОГО ПРЕДЛАГАЕТ CISCO
В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стратегия
Cisco

Новые
продукты

Рекомендации
по внедрению

Оценка
соответствия

Импорт и локальное
производство

Аналитика
и исследования

← 3 →

Новая модель Cisco ASA – 5585-X

Новая, высокопроизводительная платформа Cisco ASA 5585-X построена на базе специализированных процессоров SSP, которые оптимизированы под решение задач сетевой безопасности и, в частности, функций межсетевого экранирования, построения VPN и предотвращения вторжений.

Максимальная производительность межсетевого экрана на базе Cisco ASA 5585-X составляет 40 Гбит/сек; максимальное число соединений – 10 миллионов, а число соединений в секунду – 350 000.



Высокопроизводительная платформа Cisco ASA 5585-X

Новая версия ПО Cisco ASA – 8.4

Новая версия Cisco ASA предлагает функции межсетевого экранирования с учетом контекста. При этом учитывается локальный контекст (с помощью Cisco TrustSec), глобальный контекст (с помощью Cisco Security Intelligence Operations) и мобильные данные (с помощью Cisco AnyConnect). Пользователи, приложения, данные, уровень репутации, тип устройства, текущий уровень соответствия, угрозы, адресаты, источники и местоположения – вот лишь некоторые компоненты многостороннего комплексного контекста, который учитывает Cisco ASA и которые могут быть описаны в политиках новой версии Cisco ASA.



Семейство защитных устройств Cisco ASA 5500

Защищенные сети без границ



ЧТО НОВОГО ПРЕДЛАГАЕТ CISCO
В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стратегия
Cisco

Новые
продукты

Рекомендации
по внедрению

Оценка
соответствия

Импорт и локальное
производство

Аналитика
и исследования



Cisco Catalyst 6500 Series ASA Services Modules

Модуль Cisco Catalyst 6500 Series ASA Services Modules – высокопроизводительный интегрированный в коммутаторы Cisco Catalyst 6500 модуль межсетевого экрана, построенный на базе той же архитектуры, что и Cisco ASA 5585-X.

Максимальная производительность межсетевого экрана на базе Catalyst 6500 Series ASA Services Modules составляет 20 Гбит/сек; максимальное число соединений – 10 миллионов, число соединений в секунду – 300 000, число виртуальных контекстов – 250, а число поддерживаемых VLAN – 1000.



Модуль Cisco Catalyst 6500 Series ASA Services Modules

Модули Cisco ASA IPS SSP

Модули Cisco ASA IPS SSP построены на базе специализированных процессоров, которые оптимизированы под решение задач сетевой безопасности и, в частности, предотвращения вторжений. 4 модуля для Cisco ASA 5585-X обеспечивают производительность системы предотвращения вторжений 2, 3, 5 и 10 Гбит/сек.



Модуль Cisco ASA IPS SSP

Защищенные сети без границ



ЧТО НОВОГО ПРЕДЛАГАЕТ CISCO
В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стратегия
Cisco

Новые
продукты

Рекомендации
по внедрению

Оценка
соответствия

Импорт и локальное
производство

Аналитика
и исследования

← 5 →

Модуль Cisco NME-RVPN для ISR G2

Модуль NME-RVPN в исполнении MCM может использоваться в составе маршрутизаторов Cisco ISR серий 2800/3800 и 2900/3900. В модуле, основанном на передовых технологиях Cisco, используется российское сертифицированное в ФСБ (по классу КС1/КС2) программное обеспечение компании «С-Терра СиЭсПи». Технологический процесс производства модуля NME-RVPN в исполнении MCM определен документом «Порядок организации производства изделия «Модуль Сетевой Модернизированный (МСМ)» в рамках подконтрольного технологического процесса на территории Российской Федерации» и согласован с регулятором (ФСБ России).



Модуль Cisco NME-RVPN для ISR G2

Высокопроизводительный VPN на базе Cisco UCS

Решение CSP VPN Gate на платформе Cisco UCS C-200 представляет собой высокопроизводительный VPN-шлюз (скорость шифрования до 3,2 Гбит/сек), реализующий стандартные механизмы защищенной передачи данных в сетях TCP/IP (IPSec) с применением российской криптографии, сертифицированной в ФСБ по классам защиты КС1/КС2.



Cisco UCS C-200 в качестве платформы для CSP VPN Gate

Защищенные сети без границ



ЧТО НОВОГО ПРЕДЛАГАЕТ CISCO
В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стратегия
Cisco

Новые
продукты

Рекомендации
по внедрению

Оценка
соответствия

Импорт и локальное
производство

Аналитика
и исследования

← 6 →

Cisco Virtual Security Gateway

Система Cisco Virtual Security Gateway (VSG) – это программный межсетевой экран для виртуализированных сред, построенных на базе коммутаторов Cisco Nexus 1000v. VSG позволяет надежно разграничивать доступ между виртуальными машинами, изолировать приложения между несколькими пользователями, а также эффективно разделять полномочия между администраторами виртуальных машин и администраторами безопасности для соблюдения нормативных требований.



Коммутаторы для центров обработки данных Cisco Nexus

Cisco ISR Web Security с Cisco ScanSafe

В маршрутизаторы Cisco ISR G2 встроены различные защитные механизмы, сертифицированные по требованиям ФСТЭК, – межсетевой экран, система предотвращения вторжения и т. д. Новая функция Cisco ISR Web Security with Cisco ScanSafe позволяет прозрачно перенаправлять весь Web-трафик в облако Cisco ScanSafe, в котором и будут реализовываться все защитные механизмы, что позволяет существенно снизить издержки на защиту Web-взаимодействия.



Маршрутизаторы Cisco ISR G2

Защищенные сети без границ



ЧТО НОВОГО ПРЕДЛАГАЕТ CISCO
В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стратегия
Cisco

Новые
продукты

Рекомендации
по внедрению

Оценка
соответствия

Импорт и локальное
производство

Аналитика
и исследования



TrustSec 2.0

Cisco TrustSec – это набор технологий и продуктов, обеспечивающих контроль доступа пользователей и устройств в сеть на основе контекста.

Данное решение включает в себя аутентификацию и авторизацию пользователей и устройств, оценку соответствия, профилирование устройств, обеспечение гостевого доступа, обеспечение целостности и конфиденциальности передаваемых по проводным и беспроводным сетям данных, централизованное управление, а также мониторинг, генерацию отчетов, отслеживание и устранение проблем и неполадок.

Развертываться Cisco TrustSec может как на базе отдельных устройств (Cisco NAC Appliance или Cisco ISE), так и на базе встроенной в сетевое оборудование функциональности 802.1x.

Ключевым компонентом новой версии TrustSec 2.0 является новый продукт Cisco ISE. Помимо этого в рамках TrustSec 2.0 реализованы разграничение доступа по ролям пользователей на базе Cisco Catalyst, Cisco ASR и Cisco VDI, а также ряд других нововведений.

Cisco Identity Service Engine 1.0

Cisco Identity Services Engine (ISE) – решение для централизованного управления политиками в рамках решения Cisco TrustSec. Оно позволяет эффективно определять политики доступа к различным сетевым ресурсам и управлять ими в масштабе всей организации.

Cisco ISE:

- решает задачу поддержки «любого устройства» с помощью политики контроля доступа с учетом контекста;
- различает корпоративные и личные пользовательские устройства;
- автоматизирует функции обеспечения информационной безопасности по всей организации с помощью средств контроля доступа и шифрования, реализованных на уровне сети;
- упрощает повседневную работу ИТ-подразделения, позволяя разрабатывать политики, отражающие правила ведения бизнеса с учетом пользователей, устройств, приложений и местоположения;
- интегрируется с системой управления корпоративной ИТ-инфраструктурой Cisco Prime, обеспечивая управление подключением конечных устройств.

Защищенные сети без границ



ЧТО НОВОГО ПРЕДЛАГАЕТ CISCO В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стратегия
Cisco

Новые
продукты

Рекомендации
по внедрению

Оценка
соответствия

Импорт и локальное
производство

Аналитика
и исследования

← 8 →

Cisco AnyConnect Secure Mobility Client 3.0

Cisco AnyConnect Secure Mobility Client – это унифицированный программный клиент, обеспечивающий сразу несколько важных задач для конечного пользователя: VPN-доступ, персональный межсетевой экран, аутентификацию и авторизацию пользователей и интеграцию с облачной безопасностью Cisco ScanSafe.

AnyConnect функционирует не только на платформе Windows (XP 32/64, Vista 32/64, Windows 7 32/64), но также на MacOS, Linux, Windows Mobile и Apple iOS.

Новая версия дополнила AnyConnect следующими возможностями:

- VPN-доступ обеспечивается за счет выбора одного из трех протоколов, лучше подходящего под конкретную задачу, – TLS, DTLS и IPSec/IKEv2.
- Автоматическое перенаправление трафика через защищенное облако Cisco ScanSafe с целью снижения нагрузки на пользовательское устройство.
- Встроенный расширенный клиент 802.1X для контроля доступа в проводных и беспроводных сетях.

Cisco Secure Desktop 3.6

Программное обеспечение Cisco Secure Desktop – это апплет, загружаемый в момент подключения к корпоративной сети по SSL VPN при помощи любого браузера (в т. ч. и с мобильных устройств). Он позволяет обеспечить безопасность всех обрабатываемых в процессе сеанса данных – файлов, web-страниц, паролей, электронной почты и т. п. Это обеспечивается за счет создания защищенного виртуального раздела на диске, а также контроля всех процессов и обращений к реестру или жесткому диску.

К возможностям новой версии относятся:

- Поддержка Windows 7.
- Новые возможности по обнаружению перехватчиков ввода с клавиатуры.
- Расширение возможностей по сканированию локального узла на предмет соответствия требованиям политики безопасности и политики ИТ.

Cisco Security Manager 4.1

CSM – это система централизованного управления и мониторинга средств защиты Cisco. Она облегчает конфигурирование, мониторинг и выявление проблем в настройках средств корпоративной защиты Cisco – межсетевых экранов Cisco ASA, Cisco IOS Firewall, Cisco FWSM и Cisco ASA SM, систем предотвращения вторжений Cisco IPS, средств построения VPN (включая и S-Terra CSP VPN Gate для Cisco ISR G2 и Cisco UCS), а также функций защиты маршрутизаторов Cisco ISR/ASR и коммутаторов Cisco Catalyst.

К новым возможностям программного обеспечения Cisco Security Manager относятся:

- Расширенная система генерации отчетов (включая пользовательские).
- Расширенные возможности по выявлению и отслеживанию неисправностей.
- Помощник по созданию сценариев VPN для бизнес-партнеров (extranet/partner VPN).
- Новые возможности по импорту и экспорту политик в крупных сетях.
- Поддержка Windows 2008 R2 (64-х разрядная).

Защищенные сети без границ



**ЧТО НОВОГО ПРЕДЛАГАЕТ CISCO
В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Стратегия
Cisco

Новые
продукты

**Рекомендации
по внедрению**

Оценка
соответствия

Импорт и локальное
производство

Аналитика
и исследования

← 9 →

Архитектура Cisco PCI 2.0 (Cisco Validated Design)

Новая версия стандарта PCI DSS 2.0 вызывает немало вопросов у заказчиков компании Cisco, которые впервые сталкиваются с требованиями платежных систем Visa и MasterCard по безопасности данных владельцев платежных карт. Чтобы помочь своим заказчикам, Cisco разработала новую версию детального руководства по выполнению требований стандарта PCI DSS 2.0 в инфраструктуре Cisco.

Данное руководство может быть найдено по адресу:
<http://www.cisco.com/go/pci> и http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html

Руководство по внедрению SIEM-решений в инфраструктуру Cisco

Cisco сотрудничает с компаниями, разработавшими лучшие в своем классе средства мониторинга и управления событиями безопасности и сигналами тревоги (SIEM). Это партнерство помогает нам лучше учесть потребности заказчиков и помочь им эффективно использовать сетевые решения и средства защиты Cisco вместе с SIEM-решениями компаний RSA, ArcSight, LogLogic, netForensics, SenSage и Splunk. Результат данного сотрудничества описан в соответствующих руководствах, свободно доступных на сайте Cisco.

Данные руководства могут быть найдены по адресам:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/ns1090/landing_siem.html
и http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html

Руководство по защите данных

Сосредоточившись на защите сетевой инфраструктуры, виртуализированных сред и центров обработки данных, компания Cisco не забывает и о защите персональных рабочих мест. Помимо технологии TrustSec и системы Cisco AnyConnect Secure Mobility Client компания Cisco разработала несколько руководств по защите конфиденциальной информации, хранимой на персональных компьютерах и защищаемых с помощью решений наших партнеров – компаний Credant и Lumension.

Данные руководства могут быть найдены по адресам:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/ns1090/landing_dSecuritysys.html
и http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html

Защищенные сети без границ



ЧТО НОВОГО ПРЕДЛАГАЕТ CISCO В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стратегия
Cisco

Новые
продукты

Рекомендации
по внедрению

Оценка
соответствия

Импорт и локальное
производство

Аналитика
и исследования

← 10 →

Сертификация в ФСБ

Центр защиты информации и специальной связи ФСБ России в феврале 2011 года выдал компании «С-Терра СиЭсПи» сертификаты, удостоверяющие, что решение CSP VPN Gate версии 3.1, работающее на модуле NME-RVPN для маршрутизаторов Cisco ISR и серверах Cisco UCS, соответствует требованиям к средствам криптографической защиты информации классов КС1 и КС2 (в зависимости от исполнения).

Если раньше модуль NME-RVPN был сертифицирован по классу защиты КС1, то сейчас уровень защиты был повышен до класса КС2, что позволило эффективно применять данное решение в финансовых организациях, которым стандартом Банка России было предписано применение VPN-решение классом не ниже КС2. Теперь и модуль NME-RVPN и VPN-решение компании «С-Терра СиЭсПи» на базе Cisco UCS C-200 сертифицированы по классу КС2.

Дополнительная информация доступна по адресу:
<http://www.cisco.ru/go/rvpn>

Новые сертификаты ФСТЭК

За прошедшие полгода были получено свыше 50 новых сертификатов соответствия требованиям по безопасности ФСТЭК на оборудование компании Cisco.

К числу новых сертифицированных решений могут быть отнесены Cisco ASA 5550, Cisco 5580, модули предотвращения вторжения AIP-SSM для Cisco ASA, высокопроизводительные сенсоры предотвращения вторжений Cisco IPS 4270, маршрутизаторы Cisco GSR, различные модели маршрутизаторов Cisco ISR и коммутаторов Cisco Catalyst, система управления Cisco Security Manager, система мониторинга Cisco MARS, а также система авторизации и контроля доступа Cisco ACS.

Общее число сертифицированных линеек продукции Cisco превысило 95, а общее число выданных на продукцию Cisco сертификатов превысило 500 (из 2500 сертификатов ФСТЭК, выданных за 18 лет существования этого органа исполнительной власти).

Список сертификатов ФСТЭК на оборудование Cisco может быть загружен с сайта <http://www.cisco.com/web/RU/broch.html> или с официального сайта ФСТЭК – <http://www.fstec.ru/>

Сертифицированное производство ФСТЭК

Серийное производство в контексте сертификации ФСТЭК не означает ни производства комплектующих, ни их сборки на территории Российской Федерации; речь идет только об оценке соответствия массово поставляемого оборудования.

Для сертификации средств защиты по схеме единичного образца или партии (именно эти схемы преимущественно используются иностранными производителями средств защиты) требуется от 9 до 12 недель. При сертификации по схеме «серия» время поставки сертифицированного изделия значительно сокращается (до 2 недель); также снижается и стоимость сертификации.

По данной схеме сертификация (совместно с ЗАО «АМТ Групп» и ЗАО «Крафтвэй корпорейшн ПЛС») проведена для 20 с лишним линеек оборудования:

- межсетевых экранов серии Cisco PIX 500;
- межсетевых экранов Cisco FWSM;
- программно-аппаратных комплексов серии Cisco ASA 5500;
- маршрутизаторов серии Cisco 1800, 2800, 2900, 3800, 3900, 7200, 7600;
- коммутаторов серии Cisco Catalyst 2960, 3750, 6509;
- устройств обнаружения вторжений Cisco IPS 4200.

Защищенные сети без границ



ЧТО НОВОГО ПРЕДЛАГАЕТ CISCO В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стратегия
Cisco

Новые
продукты

Рекомендации
по внедрению

Оценка
соответствия

**Импорт и локальное
производство**

Аналитика
и исследования

← 11 →

Импорт шифровальных средств

Республика Беларусь, Республика Казахстан и Российская Федерация в соответствии с Договором от 6 октября 2007 года формируют таможенный союз. В соответствии с соглашениями между этими странами было разработано «Положение о порядке ввоза на таможенную территорию таможенного союза и вывоза с таможенной территории таможенного союза шифровальных (криптографических) средств». Данное Положение действует с 1 января 2010 года.

Положение касается любых производителей средств, имеющих встроенные функции шифрования. Для перемещения любого шифровального средства через таможенную границу обязательными документами являются зарегистрированная нотификация или заключения Центра лицензирования, сертификации и защиты государственной тайны ФСБ России (при необходимости требуется также лицензия Минпромторга России). Исключений из данной процедуры нет.

Проверить законность ввоза продукции с функциями шифрования можно, запросив соответствующее заключение ФСБ или просмотрев список зарегистрированных нотификаций на сайте Комиссии Таможенного союза по адресу:
<http://www.tsouz.ru/db/entr/notif/Pages/default.aspx>

Импорт продукции Cisco

Компания Cisco имеет четкую классификацию шифровальных средств, основанную на требованиях экспортного законодательства США.

С целью защиты интересов российских потребителей в компании Cisco была введена система внутренней классификации и контроля импортируемой в Россию продукции. Она облегчает ввоз в Россию средств, содержащих функции шифрования. В частности, к лету 2011 года компания Cisco оформила разрешительные документы на более чем 5300 наименований своей продукции, среди которых маршрутизаторы, коммутаторы, межсетевые экраны, средства унифицированных коммуникаций, беспроводное оборудование и т. д.

Компания Cisco регулярно оповещает своих партнеров, осуществляющих импорт на территорию России, обо всех новых наименованиях, получивших разрешение на ввоз.

Каждый покупатель продукции Cisco может быть уверен, что его оборудование ввезено с соблюдением требований законодательства России.

FAQ по вопросам импорта оборудования Cisco может быть загружен с сайта
<http://www.cisco.com/web/RU/broch.html>

Локальное производство в России

В начале апреля 2011 года компания Cisco анонсировала свое первое устройство, производимое в России, – аппаратный VPN-модуль. Запуск этого производства вытекает из долгосрочных договоренностей по поддержке инновационного развития России, достигнутых во время прошлогоднего визита Президента РФ Д. Медведева в штаб-квартиру компании Cisco.

В России VPN-модуль Cisco будет производиться по лицензии Cisco с помощью многоуровневой высокотехнологичной цепочки поставок, в которую входят российские партнеры Cisco. В их числе – ООО «ГК Альтоника», ставшее первым независимым российским производителем основных электронных узлов для этого продукта. Следует отметить уникально высокую степень локализации этого производства: на территории России будет осуществляться как монтаж печатных плат, так и финишная сборка и тестирование.

Официальное открытие данного производства состоялось в Зеленограде 26 апреля 2011 года. Видеорепортаж об этом событии размещен по адресу:
<http://www.youtube.com/watch?v=J8ewYJudFg4>

Защищенные сети без границ



**ЧТО НОВОГО ПРЕДЛАГАЕТ CISCO
В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Стратегия
Cisco

Новые
продукты

Рекомендации
по внедрению

Оценка
соответствия

Импорт и локальное
производство

**Аналитика
и исследования**

← 12 →

Следуя курсом на поддержку инноваций в России, компания Cisco вошла в состав двух технических комитетов (ТК) по стандартизации при Федеральном агентстве по техническому регулированию и метрологии. В декабре 2010 года Cisco вступила в ТК362 «Защита информации», а в январе 2011 года – в ТК22 «Информационные технологии». Участие лидера мировой индустрии сетевых технологий в деятельности этих комитетов будет способствовать дальнейшему распространению передового опыта в области информационных технологий и информационной безопасности в различных отраслях российской экономики.

ТК22

Технический комитет по стандартизации «Информационные технологии» (ТК22), созданный в 2010 году на базе НИИ «Восход», занимается подготовкой и экспертизой стандартов в области информационных технологий. Деятельность комитета ориентирована на проведение работ по стандартизации на государственном, межгосударственном и международном уровнях.

ТК362

Деятельность технического комитета «Защита информации» (ТК362) направлена на организацию и координацию работ по стандартизации в сфере информационной безопасности (ИБ). Комитет действует на базе Государственного научно-исследовательского испытательного института проблем технической защиты информации ФСТЭК и на сегодняшний день объединяет ряд ведущих компаний и организаций, работающих в области защиты информации по всей России.

ПКЗ

Целью работы ПКЗ является формирование и реализация государственной политики Российской Федерации в области защиты информации в кредитно-финансовой сфере через организацию и управление процессами стандартизации, а также обобщение и адаптация к отечественным условиям международного опыта соответствующих организаций по стандартизации. Специалисты Cisco вошли в состав ПКЗ и активно участвуют в разработке нормативной базы по информационной безопасности для российских банков.

Защищенные сети без границ



ЧТО НОВОГО ПРЕДЛАГАЕТ CISCO В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стратегия
Cisco

Новые
продукты

Рекомендации
по внедрению

Оценка
соответствия

Импорт и локальное
производство

Аналитика
и исследования

← 13 →

Исследования в области безопасности Cisco Security Intelligence Operations

Без исследований невозможно разрабатывать решения, которые бы удовлетворяли как требованиям заказчиков, так и рекомендациям различных регулирующих органов и нормативных документов. Именно поэтому компания Cisco инвестирует около 10% своего общего бюджета на исследования и разработки на нужды, связанные с информационной безопасностью.

Для поддержания систем защиты наших заказчиков в актуальном состоянии компания Cisco обновила целый набор своих платных и бесплатных сервисов, облегчающих ежедневную деятельность служб информационной безопасности.

Данная информация может быть получена как на сайте компании Cisco (<http://www.cisco.com/security>), так и с помощью бесплатного приложения Cisco SIO Go to iPhone, которое можно загрузить с сайта Apple AppStore или через программу Apples iTunes.

Название	Описание
Cisco IntelliShield Alert Manager Service	Web-сервис (http://www.cisco.com/go/intellishield), позволяющий освободить технических специалистов от постоянного поиска и отслеживания уязвимостей в продуктах, используемых в корпоративной сети компании. На данный момент база данных уязвимостей содержит свыше 20 000 записей о 5500 программных продуктах 1700 разработчиков по всему миру.
Cisco Security Intelligence Operations	Web-ресурс (http://www.cisco.com/go/sio) с девизом «Информировать, защищать, реагировать» (Inform, Protect, Respond) является единой точкой контакта по всем вопросам информационной безопасности Cisco. На данном, недавно обновленном портале (http://www.cisco.com/security) можно найти информацию об уязвимостях в программно-аппаратном обеспечении разных производителей, сигнатурах атак для Cisco IPS, рекомендации по отражению вторжений и устранению уязвимостей, аналитику по ИБ, источникам и уровне текущих угроз, вирусов, спама и т. д.
Cisco Applied Mitigation Bulletin	Регулярно публикуемые бюллетени Cisco, описывающие использование различных технологий Cisco, защищающих от новых уязвимостей.
Cisco Global Threat Report и Cisco Annual Security Report	Ежеквартальные и ежегодный отчеты (http://www.cisco.com/go/securityreport), подробно описывающие тенденции в области угроз и методов злоумышленников.

Защищенные сети без границ



ЧТО НОВОГО ПРЕДЛАГАЕТ CISCO В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стратегия
Cisco

Новые
продукты

Рекомендации
по внедрению

Оценка
соответствия

Импорт и локальное
производство

Аналитика
и исследования

← 14 →

Защита персональных данных

Защита персональных данных (ПДн) последние годы была и остается одной из острейших проблем в информационной сфере и взаимоотношениях государства, граждан и бизнеса. Для защиты основных свобод и прав граждан Россия приняла Федеральный Закон РФ от 27 июля 2006 года №152-ФЗ «О персональных данных».

В соответствии с данным законом Правительство Российской Федерации выпустило Постановление от 17 ноября 2007 г. № 781, которое определило общие требования по защите персональных данных. Дальнейшая детализация этих требований была дана в нормативных правовых актах и методических документах ФСБ России и ФСТЭК России. Помимо исполнения указанных нормативных актов сегодня наметилась тенденция разработки и применения отраслевых стандартов

и рекомендаций в области защиты персональных данных. Такие стандарты есть у Банка России, ЕАУФОР, НАПФ, операторов связи и т. д.

Помимо предложения эффективных технических решений по защите персональных данных, входящих в архитектуру SecureX и позволяющих выполнять все перечисленные выше требования, компания Cisco активно участвует и в нормотворческой деятельности по данному вопросу. В частности, сотрудники российского офиса Cisco:

- участвуют в экспертизе и выработке предложений по изменению законопроектов в области персональных данных;
- входят в оргкомитет Общественных слушаний по совершенствованию законодательства в области персональных данных;

- входят в Консультационный центр Ассоциации Российских Банков (АРБ) по вопросам применения отдельных норм Федерального закона №152-ФЗ «О персональных данных»;
- участвовали в работе рабочей группы Банка России и АРБ по разработке 4-й версии Комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» в части требований по защите персональных данных;
- участвуют в экспертизе отраслевых стандартов и требований федеральных органов исполнительной власти по защите персональных данных.

Защищенные сети без границ



**ЧТО НОВОГО ПРЕДЛАГАЕТ CISCO
В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Стратегия
Cisco

Новые
продукты

Рекомендации
по внедрению

Оценка
соответствия

Импорт и локальное
производство

**Аналитика
и исследования**

← 15 →

Выполнение требований СТО БР ИББС

По данным опроса Межбанковского Финансового Дома и Ассоциации Российских Банков, бизнес-процессы 88% российских финансовых организаций полностью опираются на информационные технологии. Такая зависимость не позволяет эффективно реализовывать бизнес-процессы без решения вопросов безопасности информационной инфраструктуры.

Понимая данную проблему и являясь ответственным за банковскую систему страны, Банк России с 1 декабря 2004 года ввел в действие стандарт «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», нацеленный на повышение уровня защищенности российских банков и защиту банковской тайны. С 21 июня 2010 года

вводится в действие уже 4-я редакция данного стандарта – СТО БР ИББС-1.0-2010, а также иных документов, входящих в Комплекс документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации».

Решения Cisco, входящие в архитектуру SecureX, позволяют эффективно выполнить технические требования, заложенные в требованиях Банка России. Помимо этого компания Cisco активно участвует и в нормотворческой деятельности в области безопасности финансовых организаций. В частности, сотрудники российского офиса Cisco входят в состав:

- ПКЗ «Защита информации в кредитно-финансовых учреждениях» в ТК362 при Ростехрегулировании;

- Консультационного центра Ассоциации Российских Банков (АРБ) по вопросам применения отдельных норм Федерального закона №152-ФЗ «О персональных данных» и требований СТО БР ИББС;
- рабочей группы Банка России и АРБ по разработке 4-й версии Комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»

Эта работа позволяет компании Cisco не только участвовать в разработке новых требований по информационной безопасности, но и заранее знать о готовящихся нормативных актах в области защиты информации, заблаговременно подготавливая свои решения к новым требованиям.



Cisco
Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауэрс»,
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, д. 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., 2, 5-й этаж.
Телефон: +7 (383) 230 2670
Факс: +7 (383) 230 1795
www.cisco.ru
www.cisco.com