Обзор решений Cisco для обеспечения безопасности интеллектуальных систем энергоснабжения (инфраструктуры Smart Grid)

Решение задач, связанных с обеспечением безопасности инфраструктуры Smart Grid

Изменения климата, растущие расходы на топливо, устаревающие инфраструктуры сетей электроснабжения и технологии выработки энергии нового поколения стимулируют создание новой, более интеллектуальной системы управления сетями электроснабжения. В основе трансформации сетей электроснабжения лежит использование интеллектуальных коммуникационных сетей в качестве платформы, которая обеспечивает измерение всех необходимых параметров, анализ и управление всеми операциями от генерации энергии до ее продажи, передачи и распределения между конечными потребителями. Одним из основных положений концепции интеллектуальных сетей электроснабжения является взаимная совместимость, позволяющая всем устройствам, технологическим решениям, приложениям и агентам (предприятиям, вырабатывающим электроэнергию, потребителям и операторам) взаимодействовать в рамках единой интеллектуальной сети электроснабжения.

Основанные на апробированных открытых стандартах и соответствующие нормативным требованиям решения позволяют обеспечить надежность и безопасность (как физическую, так и информацию) интеллектуальной сети электроснабжения.

Хотя интеллектуальные сети электроснабжения могут помочь в преобразовании энергетической отрасли, обеспечив недоступные ранее уровни надежности, производительности и управляемости, для их успешного внедрения также требуется интегрированная инфраструктура безопасности. Множество технологических решений, используемых в проектах по созданию интеллектуальных сетей электроснабжения, включая интеллектуальные счетчики, датчики и современные коммуникационные сети, могут стать источником уязвимостей всей инфраструктуры интеллектуальной сети электроснабжения. Основные опасения в сфере безопасности, вызванные миграцией на платформу интеллектуальной сети электроснабжения, обусловлены следующими тенденциями:

- интеграция распределенных поставщиков электроэнергии, включая независимых производителей электроэнергии, возобновляемых источников энергии и распределенных энергоресурсов;
- распространение цифровых устройств, необходимых для автоматизации процессов, управления ими и полномасштабного контроля;
- нормативные требования, связанные с защитой критически важных объектов инфраструктуры;
- миграция на интеллектуальные решения для управления перебоями в подаче электроэнергии, распределения средств автоматизации, проведения технического обслуживания при наступлении определенных условий, прогнозирования нагрузки и создания интеллектуальной инфраструктуры измерительных устройств;
- требования к повышению качества обслуживания потребителей и эффективности управления передачей электроэнергии.

Создание распределенной сетевой инфраструктуры, обеспечивающей интеграцию микросегментов сети передачи электроэнергии, свободную конкуренцию в сфере сбыта электроэнергии и возможность использования управляемых по сети устройств, стимулирует создание конвергентной инфраструктуры обеспечения информационной безопасности новой интеллектуальной инфраструктуры, объединяющей коммунальные службы, коммерческие предприятия, конечных потребителей и поставщиков электроэнергии.

Для защиты объектов систем передачи электроэнергии от центрального диспетчерского пункта до подстанции, устройств подачи электропитания и абонентских счетчиков требуется сквозная инфраструктура обеспечения информационной безопасности, которая защитит множество устройств и приложений (систему SCADA в диспетчерском пункте, удаленные терминальные устройства, программируемые контроллеры, счетчики электроэнергии, цифровые реле и устройства управления), необходимых для эксплуатации, мониторинга и управления системой передачи и измерения электроэнергии.

© Cisco Systems, Inc, 2009. С сохранением всех прав. В данном документе содержится информация, свободно распространяемая компанией Cisco.

Обеспечение безопасности интеллектуальной сети электроснабжения и ее ресурсов

При разработке решений для защиты критически важных объектов инфраструктуры корпорация Cisco объединила свой обширный опыт по созданию систем управления коммунальным хозяйством с лучшими на рынке решениями в сфере обеспечения физической и информационной безопасности.

По мнению экспертов Cisco для модернизации инфраструктуры системы энергоснабжения потребуется разработка всеобъемлющей инфраструктуры обеспечения безопасности, которая обеспечит интеграцию различных цифровых устройств, возросшего числа датчиков и средств обеспечения физической и информационной безопасности интеллектуальной сети энергоснабжения. Решения, входящие в состав архитектуры обеспечения безопасности интеллектуальной сети энергоснабжения (Cisco® Grid Security), позволяют реализовать интегрированный конвергентный подход к обеспечению безопасности, в рамках которого для подсистем, данных и ресурсов системы энергоснабжения обеспечивается уровень безопасности, соответствующий требованиям к защите критически важных объектов инфраструктуры. Кроме того, предусмотрены средства мониторинга состояния сети, отражения угроз и обеспечения физической безопасности объектов системы энергоснабжения.

Объединение средств обеспечения физической и информационной безопасности в рамках интегрированной инфраструктуры безопасности интеллектуальной сети электроснабжения позволяет повысить уровень защищенности при одновременном снижении сложности и затрат на управление новой инфраструктурой. Такой подход обладает следующими преимуществами:

- Снижение вероятности нарушения физической или информационной безопасности системы (уменьшение числа уязвимостей)
- Повышение отказоустойчивости за счет снижения перебоев в работе системы, вызванных нарушением безопасности
- Обеспечение целостности и конфиденциальности данных, передаваемых по интеллектуальной сети электроснабжения
- Повышение показателей надежности, доступности вычислительных ресурсов и упрощение поддержки взаимодействия по интеллектуальной сети
- Формирование среды для обеспечения выполнения нормативных требований

Решения корпорации Cisco в сфере обеспечения безопасности интеллектуальной сети энергоснабжения позволяют коммунальным предприятиям воспользоваться:

- **системным подходом** к обеспечению безопасности, основанным на широчайшем спектре технологических решений, продуктов, услуг и партнеров Cisco, которые позволяют предотвратить, обнаружить и оперативно отразить атаки на сеть энергоснабжения;
- опытом экспертов Cisco по разработке и развертыванию **сквозных архитектур обеспечения безопасности** коммунальных предприятий, включающих средства для обеспечения физической безопасности, обнаружения и предотвращения вторжений, обеспечения безопасности ЦОД, мониторинга безопасности и управления инфраструктурой обеспечения безопасности;
- **квалифицированными услугами консалтинга в течение всего жизненного цикла решения**, позволяющими разработать бизнес-стратегию и требования к системе, оценить технологические решения в сфере обеспечения безопасности, а также спроектировать, внедрить и эффективно эксплуатировать решения для обеспечения физической и информационной безопасности интеллектуальной сети энергоснабжения.

Корпорация Cisco обладает уникальными возможностями и может помочь предприятим энергетической отрасли в трансформации существующих систем в интеллектуальные сети энергоснабжения, сформировав сквозные защищенные сети, которые позволяют предприятиям коммунального хозяйства безопасно эксплуатировать интеллектуальные сети энергоснабжения, обеспечивая соответствие развивающимся стандартам и нормативным требованиям с помощью технологических решений и услуг корпорации Cisco и ее партнеров.

Решения Cisco для защиты интеллектуальных сетей энергоснабжения

Корпорация Cisco разработала набор решений для обеспечения безопасности интеллектуальных сетей энергоснабжения. Эти решения позволяют сформировать защищенную коммуникационную платформу для осуществления бизнес-операций и операций управления для поддержки сетей генерации, включая мощные

© Cisco Systems, Inc, 2009. С сохранением всех прав. В данном документе содержится информация, свободно распространяемая компанией Cisco.

электростанции и сетей электростанций, основанных на возобновляемых источниках энергии, а также сетей передачи и распределения, диспетчерских пунктов, подстанций и муниципальных сетей.

В набор решений входят расширенные средства обеспечения информационной безопасности центральных диспетчерских пунктов и центров обработки данных, в которых размещаются критически важные приложения, системы и данные, при одновременном обеспечении соответствия нормативным требованиям.

В набор решений Cisco для обеспечения безопасности интеллектуальных сетей энергоснабжения входят следующие компоненты:

- средства управления учетными данными и идентификацией и система контроля доступа;
- система защиты от угроз;
- средства обеспечения безопасности ЦОД;
- средства обеспечения безопасности глобальных сетей;
- система мониторинга и управления информационной безопасностью;
- система обеспечения физической безопасности;
- средства обеспечения безопасности электростанций;
- средства обеспечения безопасности подстанций;
- средства обеспечения соответствия нормативным требованиям к системам коммунального хозяйства;
- услуги Cisco по планированию, созданию и эксплуатации решений для обеспечения безопасности интеллектуальных систем электроснабжения.

Средства управления учетными данными и идентификацией и система контроля доступа

Решение Cisco для управления учетными данными и идентификацией доработано для обеспечения соответствия потребностям по эксплуатации интеллектуальных систем электроснабжения и включается компоненты для аутентификации и контроля доступа. Средства аутентификации позволяют гарантировать, что доступ к центру управления, сетям передачи и системе распределения предоставляется только пользователям, группам и сервисам, прошедшим аутентификацию. Данное решение позволяет избежать трудоемкой работы по ввода учетных данных для аутентификации гостевых пользователей вручную и включает средства аутентификации без использования специализированных клиентов и средства аутентификации пользователей беспроводной сети. Средства контроля доступа обеспечивают тонкую настройку местного и удаленного доступа пользователей и приложений в сложных сетях диспетчерского центра, центра обработки данных и подстанций.

Среди компонентов решения Cisco для управления учетными данными, идентификацией и контроля доступа можно выделить следующие:

- Cisco Secure ACS. Централизованное решение для идентификации пользователей сети и контроля доступа.
- Cisco NAC. Решение для обеспечения выполнения политики безопасности для устройств, которым требуется доступ к сети.
- Сетевые сервисы Cisco, основанные на идентификации (IBNS). Решение для обеспечения аутентификации, контроля доступа и обеспечения выполнения политик безопасности для пользователей, чтобы защитить сетевые каналы и ресурсы сети.
- Нестандартные сигнатуры для протоколов SCADA для межсетевых экранов. Обеспечение контроля доступа на различных уровнях для создания многоуровневой системы защиты.

© Cisco Systems, Inc, 2009. С сохранением всех прав. В данном документе содержится информация, свободно распространяемая компанией Cisco.

Защита от угроз

Апробированные решения для защиты сетей позволят обнаружить попытки вторжений и обеспечат мониторинг и управление событиями в сфере информационной безопасности в режиме реального времени.

Решение для защиты от угроз позволяет предотвратить использование уязвимостей, поскольку зачастую трудно определить будущую форму новой угрозы. Чтобы сформировать эффективную многоуровневую систему защиты, необходимо вдумчиво реализовать принципы обеспечения безопасности во всех элементах инфраструктуры сети электроснабжения. В системах Cisco для защиты систем электроснабжения от угроз можно выделить следующие компоненты:

- средства сегментирования сети и контроля доступа для защиты от атак типа "отказ в обслуживании";
- многофункциональные устройства защиты ASA. Содержат межсетевой экран, средства защиты системы унифицированных коммуникаций, средства организации VPN-подключений, систему предотвращения вторжений (IPS) и средства обеспечения безопасности контента.
- программные компоненты подсистемы безопасности Cisco IOS®. Набор средств обеспечения информационной безопасности, включая межсетевой экран, средства организации VPN-подключений, IPS и средства обеспечения безопасности контента на маршрутизаторах Cisco ISR и Cisco ASR;
- Cisco IPS: обеспечивает интеллектуальное обнаружение угроз и защиту от них, что позволяет обнаруживать внешние угрозы ИТ-инфраструктуре и предотвращать распространение внутренних угроз в рамках ИТ-инфраструктуры.

Средства обеспечения безопасности ЦОД

Эволюция интеллектуальных систем энергоснабжения определила необходимость пересмотра устаревшей стратегии управления ИТ-инфраструктурой коммунальных систем. Значение интеграции систем управления и эксплуатации систем энергоснабжения сегодня особенно возросло. С внедрением интеллектуальных систем энергоснабжения компоненты, поддерживающие экслуатацию систем энергоснабжения (OSS), будут испытывать растущую нагрузку и рост требований к взаимной совместимости систем хранения, извлечения и обработки данных. Кроме того, нормативные требования к системам аварийного восстановления включают требования к регулярному тестированию целостности и производительности резервных диспетчерских пунктов.

Для защиты информации, циркулирующей в сети интеллектуальной системы энергоснабжения, требуется надежная защита ЦОД и уровня доступа. Кроме того, необходимо обеспечить аутентификацию и защиту диагностических сообщений, телеметрической информации и команд управления интеллектуальными устройствами.

Растущая сложность процессов, связанных с эксплуатацией системы электроснабжения, требуется создания высокомасштабируемой, отказоустойчивой и защищенной платформы сети ЦОД. Решение Cisco по обеспечению безопасности ЦОД представляет собой основной компонент подсистемы защиты ИТ-инфраструктуры системы энергоснабжения. Используя решения в области консолидации и виртуалиации, решения Cisco для ЦОД предоставляют широкий спектр средств, которые позволяют организациям превратить сетевые ресурсы, вычислительные ресурсы и ресурсы системы хранения в защищенный общий пул ресурсов, обеспечивающий целостность данных и приложений, защиту коммуникаций между современными бизнес-процессами и приложениями в рамках ИТ-инфраструктуры системы энергоснабжения, а также безопасное подключение к внешним ресурсам, например поставщикам электроэнергии, которые используют возобновляемые источники энергии.

Решение Cisco для защиты ЦОД предоставляет широкий спектр средств, позволяющих обеспечить безопасность и конфиденциальность хранилища информации, систем и данных интеллектуальной сети энергоснабжения. Архитектура этого решения основана на следующих принципах.

- Полностью резервируемая отказоустойчивая архитектура ЦОД без единой точки отказа.
- Межсетевые экраны, обеспечивающие фильтрацию входящего и исходящего трафика для ферм серверов.
- Межсетевые экраны ЦОД, обеспечивающие защиту серверов и сегментацию трафика приложений.
- Использование информации, поступающей от устройств Cisco IPS, Cisco IDS, а также маршрутизаторов и коммутаторов Cisco, для обнаружения, предотвращения и противодействия вторжениям.

© Cisco Systems, Inc, 2009. С сохранением всех прав. В данном документе содержится информация, свободно распространяемая компанией Cisco.

- Многофункциональные устройства Cisco ASA, предоставляющие сервисы межсетевого экрана, защиты системы унифицированных коммуникаций, организации VPN-подключений, IPS и обеспечения безопасности контента.
- Средства защиты сети на уровне 2, включая списки контроля доступа (ACL), встроенные средства обеспечения безопасности Cisco IOS (CISF, port security, netflow, динамический анализ ARP-трафика, IP source guard, ERSPAN, QoS и политики уровня управления (CoPP)).
- Балансировка нагрузки на серверы для защиты серверов и приложений.
- Межсетевой экран для web-приложений Cisco ACE. Объединение средств гибкого анализа трафика web-приложений со средствами анализа XML для предотвращения атак с использованием XSS, HTTP, SQL и XML.
- Управление безопасностью с использованием хостовой системы предотвращения вторжений Cisco Security Agent (CSA), межсетевых экранов, IPS, а также средств netflow и syslog.

Услуги Cisco в сфере ЦОД помогают предприятиям коммунального хозяйства строить решения на основе оптимальных методик в сфере обеспечения информационной безопасности, стандартов и нормативных требований к средам ЦОД. Среди услуг Cisco в сфере ЦОД можно выделить следующие.

- **Оценка состояния ЦОД.** Включает оценку безопасности объекта для повышения уровня защищенности физической инфраструктуры.
- **Оценка виртуализации ЦОД.** Анализ требований к безопасности и выработка рекомендаций по повышению уровня защищенности ЦОД.
- **Планирование и проектирование системы виртуализации ЦОД.** Разработка подробной архитектуры и плана развертывания виртуализованной среды ЦОД, включая требования к безопасности сетевых ресурсов, вычислительных ресурсов и ресурсов системы хранения данных.

Безопасность глобальной сети

Обеспечение безопасности глобальной сети является критически важной задачей, поскольку именно глобальная сеть используется для объединения разрозненных систем коммунальных служб, включая муниципальные сети, сети передачи и распределения, сети операторов связи, а также сети диспетчерских пунктов. При проектировании глобальной сети необходимо предусмотреть меры обеспечения доступности, безопасности и надлежащей производительности всех пользователей, устройств и приложений сети интеллектуальной системы энергоснабжения. Архитектура глобальной сети основана на следующих принципах.

- Архитектура уровня ядра для безопасной сегментации трафика.
- Встроенные средства обеспечения ИБ Cisco IOS: сервисы межсетевого экрана, организации VPN-подключений, IPS и обеспечения безопасности контента на маршрутизаторах семейств Cisco ISR и Cisco ASR.
- Средства защищенного подключения к периметру глобальной сети: VPN для изоляции трафика (DMVPN), AES для надежного шифрования и PKI.
- Средства защиты периметра глобальной сети: средства обеспечения QoS и ограничения скорости, uRPF, фильтры для борьбы с подменой адресов (RFC-2827), списки ACL для защиты инфраструктуры и средства защиты системы маршрутизации.
- Средства защищенной доставки данных в ЦОД, диспетчерский центр и центр сбора измерительной информации, включая транзитную передачу.
- Управление идентификационными данными и контроль доступа пользователей и устройств ко всем сегментам сети.

Управление безопасностью и мониторинг безопасности

По мере роста числа ресурсов системы энергоснабжения, которые используются для генерации и передачи электроэнергии (подстанции, трансформаторы и линии энергопередач) и подключены к сетям передачи данных, требования к обеспечению безопасности и отказоустойчивости получили статус нормативных документов. В соответствии со стандартами NERC-CIP при мониторинге событий безопасности должны

© Cisco Systems, Inc, 2009. С сохранением всех прав. В данном документе содержится информация, свободно распространяемая компанией Cisco.

использоваться средства автоматизации и формальные процессы.

Решение Cisco в сфере управления безопасностью и мониторинга безопасности включает широкий спектр средств управления и мониторинга, среди которых можно выделить следующие.

- **CiscoWorks Network Compliance Manager (NCM).** Позволяет обнаруживать, управлять и противодействовать угрозам безопасности путем управления конфигурацией и изменением версий ПО в сетевой инфраструктуре, построенной на оборудовании различных поставщиков. Кроме того, данное решение позволяет контролировать соответствие множеству нормативных требований, сформулированных или обусловленных регуляторами, ИТ-подразделением, корпоративными политиками и технологическими требованиями.
- **Cisco Security Manager.** Обеспечивает согласованное развертывание и обеспечение выполнения политик безопасности на маршрутизаторах, коммутаторах и устройствах обеспечения безопасности Cisco.
- **Cisco LAN Management System (LMS).** Обеспечивает аварийное восстановление и соответствие требованиям NERC CIP (CIP 009) путем резервного копирования конфигураций и образов ПО, а также путем простого отката конфигураций.

Физическая безопасность

Многие ресурсы, используемые для генерации и передачи электроэнергии, уязвимы для атак террористов и стихийных бедствий.

Решения Cisco в сфере обеспечения физической безопасности позволяют использовать сетевые механизмы для создания системы видеонаблюдения (на базе IP-камер) и внедрения системы электронного контроля доступа. Кроме того, технологические средства конвергенции голоса, данных и информации подсистемы обеспечения физической безопасности обеспечивают эффективное разрешение инцидентов с использованием распределенной сети.

Среди компонентов решения Cisco для обеспечения физической безопасности можно выделить следующие.

- **Система электронного контроля доступа.** IP-шлюзы доступа Cisco и система управления Physical Security Access Manager позволяют ограничить доступ на критически важные объекты инфраструктуры и обеспечивают журналирование доступа персонала в соответствии с требованиями NERC-CIP.
- **Система видеонаблюдения.** Корпорация Cisco предлагает широчайший спектр решений в сфере видеонаблюдения (IP-камеры, системы хранения видеоинформации и средства анализа видеоизображения) для развертывания в диспетчерских пунктах, а также на различных объектах интеллектуальной сети энергоснабжения. Эти решения поддерживают передачи видео по локальной и глобальной сети (включая беспроводные каналы) как в помещениях, так и вне помещений.
- **Коммуникации, совместная работа и обеспечение информированности.** Решение Cisco IPICS обеспечивает возможность обмена данными, а также передачи голоса и видео с использованием широкого спектра устройств и коммуникационных технологий, включая радиоканалы, VoIP-телефоны, обычные телефоны и персональные компьютеры.

Безопасность электростанций

Интеллектуальная сеть энергоснабжения позволит предприятиям коммунального хозяйства интегрировать различные источники энергии в единый пул и управлять ими таким образом, чтобы избежать дефицита электроэнергии в тех случаях, когда мощности стандартной электростанции оказывается недостаточно. Чтобы добиться такого результата, необходимо обеспечить защищенное взаимодействие между стандартными электростанциями и модернизируемыми электростанциями, находящимися под управлением предприятий коммунального хозяйства или во владении независимых поставщиков электроэнергии. Решения Cisco для обеспечения безопасности электростанций основаны на следующих принципах проектирования.

- Сегментация сети (на уровнях 2 и 3) для блоков генерации и электростанции для повышения управляемости.
- Создание защищенной ДМЗ для управления электростанцией и обеспечения ее безопасности
- Защищенный локальный и удаленный сетевой доступ к системам электростанции

© Cisco Systems, Inc, 2009. С сохранением всех прав. В данном документе содержится информация, свободно распространяемая компанией Cisco.

- Централизованная система журналирования и корреляции событий на электростанции
- Централизованный сервер AAA для аутентификации и контроля доступа пользователей.
- Система управления информационной безопасностью для управления политиками различных электростанций.
- Система обеспечения физической безопасности, включая систему видеонаблюдения и систему контроля доступа.

Безопасность подстанций

Подстанции представляют собой базовые блоки, из которых создаются сети транспортировки электроэнергии. Они обеспечивают подключение к муниципальным сетям, сетям сбора и передачи измерительной информации, сетям подключения домов на распределительных подстанциях и глобальным измерительным системам (WAMS). Защищенная передача данных от подстанций многим адресатам является источником множества критически важных задач, стоящих перед предприятиями коммунального хозяйства. Решения Cisco для обеспечения безопасности подстанций основаны на следующих принципах проектирования.

- Унифицированная архитектура глобальной сети, включая средства обеспечения безопасности, отказоусойчивости и интеллектуального взаимодействия между подстанциями, а также между подстанциями и диспетчерским пунктом.
- Маршрутизатор/межсетевой экран для формирования и защиты электронного периметра безопасности (ESP).
- Маршрутизаторы Cisco ISR для интеграции средств маршрутизации, коммутации и обеспечения безопасности в пределах ESP.
- Модуль IPS для маршрутизатора/межсетевого экрана для обнаружения вредоносного программного обеспечения и предотвращения его распространения.
- Обеспечение безопасности уровня доступа для взаимодействия подстанций.
- Управление идентификационными данными и контроль доступа пользователей и устройств для их проникновения во внутреннюю область ESP.
- Сигнатуры на уровне протоколов для межсетевых экранов и журналирования в системах, расположенных в пределах ESP.
- Система обеспечения физической безопасности, включая подсистему видеонаблюдения и подсистему контроля доступа для формирования и защиты физического периметра безопасности.

Безопасность системы управления энергоснабжением

Решение Cisco Network Building Mediator позволяет измерять энергопотребление систем здания и управлять им. Это решение, основанное на стандартной открытой сетевой платформе, которая собирает данные от разрозненных систем здания и ИТ-систем, позволяет предприятиям коммунального хозяйства лучше прогнозировать спрос на электроэнергию и соответствовать запросам потребителей, оптимизировать нагрузку на систему генерации и совершенствовать управление альтернативными источниками энергии, например, солнечными батареями.

Для интеграции решения Cisco Building Mediator в систему управления энергопотреблением необходимо обеспечить безопасное взаимодействие между контроллерами здания и сетями управления системы коммунального хозяйства, включая подключение существующего оборудования системы автоматизации здания к IP-сети. Для этого также требуется внедрение гибких средств обеспечения безопасности, позволяющих защитить доступ к интегрированным сервисам здания и ИТ-инфраструктуры.

Решение Cisco для обеспечения безопасности управления энергоснабжением основано на следующих принципах проектирования.

- Защищенная платформа Cisco Network Building Mediator
- Изоляция систем управления энергопотреблением здания от корпоративных систем.
- Защищенная передача трафика управления зданием по глобальной сети.
- Контроль доступа при обращении к приложениям управления энергоснабжением с терминалов.

© Cisco Systems, Inc, 2009. С сохранением всех прав. В данном документе содержится информация, свободно распространяемая компанией Cisco.

- Защита взаимодействия с помощью сертификатов.
- Управление идентификационными данными пользователей сетей управления энергоснабжением здания.

При внедрении решения Cisco для управления энергоснабжением здания заказчики могут воспользоваться широким спектром услуг консалтинга, включающих определение требований к интеллектуальной системе энергоснабжения, разработку нестандартных решений для управления энергоснабжением в соответствии с этими требованиями, координацию разработки и интеграции решения, а также предоставление поддержки с помощью услуг по оптимизации.

Соответствие нормативным требованиям

Сеть играет решающую роль при управлении рисками и обеспечении соответствия нормативным требованиям. Для мониторинга и формирования отчетов о бизнес-процессах и потоках информации в ИТ-инфраструктуру необходимо внедрить средства обеспечения сетевой безопасности. Если эти средства не будут внедренаы надлежащим образом, доступность, целостность и конфиденциальность данных и бизнес-процессов могут оказаться под угрозой. Защита сетей предприятий коммунального хозяйства в соответствии с нормативными требованиями помогает предприятиям не только избежать возможных штрафов, но и повысить уверенность заказчиков в высочайшем качестве их работы, а также ускорить внедрение интеллектуальных технологий.

Решения Cisco по обеспечению соответствия систем коммунальных предприятий нормативным требованиям позволяют обеспечить требуемое состояние ИТ-инфраструктры и снизить расходы.

Для обеспечения соответствия требованиям стандартов NERC CIP 002-009 необходимо внедрить полнофункциональную систему обеспечения информационной (сегментация, аутентификация, авторизация, мониторинг, журналирование и обучение) и физической (система контроля доступа и система видеонаблюдения) безопасности. Решение Cisco для обеспечения соответствия сетей предприятий коммунального хозяйства нормативным требованиям основано на следующих принципах проектирования.

- Развертывание на подстанциях маршрутизаторов Cisco ISR (сервисы межсетевого экрана и организации VPN-подключений Cisco IOS, а также модуль IPS) (CIP 005).
- Развертывание в диспетчерском пункте маршрутизаторов Cisco ISRc поддержкой MPLS и DMVPN для сегментации и шифрования в сети уровня ядра (CIP 002).
- Внедрение решения Cisco Secure MARS в диспетчерском пункте для мониторинга и журналирования событий, обнаруженных на устройствах Cisco и сторонних поставщиков (CIP 005).
- Внедрение маршрутизаторов Cisco ISR с Cisco Secure Access Control Server (ACS) и Cisco Security Manager в диспетчерском пункте для управления идентификационными данными пользователями и контроля доступа (CIP 003).
- Внедрение решений Cisco для контроля физического доступа и видеонаблюдения на базе IP-сети (CIP 006).

Услуги Cisco позволяют провести оценку соответствия нормативных требования, спроектировать ИТ-инфраструктуру, разработать решение и провести обучение персонала, чтобы устранить несоответствие нормативным требованиям, спроектировать систему ИБ, которая позволит устранить несоответствие нормативным требованиям, а также сконцентрировать усилия ИТ-специалистов на устранении рисков безопасности. Набор услуг Cisco в сфере обеспечения соответствия нормативным требованиям включает следующие услуги.

- Оценка соответствия требованиям стандартов NERC CIP. Услуга по оценке, которая позволяет устранить несоответствия сети требованиям стандартов NERC CIP (CIP 007)
- Услуги по проектированию и развертыванию системы в соответствии с требованиями NERC CIP. Услуги по созданию архитектуры, позволяющие разработать и внедрить меры обеспечения безопасности в соответствии с требованиями стандартов NERC (CIP 007) и провести обучение в сфере обеспечения безопасности сетевых устройств (CIP 004).

© Cisco Systems, Inc, 2009. С сохранением всех прав. В данном документе содержится информация, свободно распространяемая компанией Cisco.

Услуги Cisco по техническому консалтингу в сфере обеспечения безопасности интеллектуальных сетей энергоснабжения

Услуги Cisco по обеспечению безопасности интеллектуальных систем энергоснабжения позволяют реализовать комплексный подход к планированию, проектированию, реализации, эксплуатации и оптимизации интегрированного решения по обеспечению безопасности коммунальных сетей энергоснабжения.

Услуги Cisco, оказываемые с помощью наших партнеров, помогают в планировании, создании и эксплуатации сетей в соответствии с нормативными требованиями по защите интеллектуальных сетей энергоснабжения от физических и информационных угроз. Услуги Cisco по обеспечению безопасности интеллектуальных сетей энергоснабжения основаны на рекомендованных отраслевых рекомендациях и апробированной методологии Cisco по планированию, созданию и эксплуатации сквозных инфраструктур обеспечения безопасности, в которых интегрируются решения Cisco и партнеров.

В услуги Cisco по обеспечению безопасности интеллектуальных сетей энергоснабжения входят следующие компоненты:

- Бизнес-стратегия и архитектура обеспечения безопасности. Подготовка многолетнего плана трансформации инфраструктуры безопасности, включая разработку бизнес-модели будущего, высокоуровневых архитектур, планов развития и рекомендаций по успешному проведению трансформации.
- Оценка состояния инфраструктуры безопасности. Оценка состояния безопасности сред систем управления, оценка системы физической безопасности объектов, оценка общей архитектуры безопасности, разработка подробных рекомендаций по обеспечению соответствия требованиям NERC-CIP.
- Обеспечение соответствия нормативным требованиям к системам коммунального хозяйства. Усовершенствование процедур управления рисками и обеспечение соответствия нормативным требованиям благодаря услугам по оценке соответствия требованиям NERC-CIP, разработке архитектуры решения и развертыванию системы.
- Обеспечение физической безопасности. Определение общих требований к системе обеспечения физической безопасности, проведение оценок объектов, разработка архитектур будущего, координация развертывания и интеграции решения, а также поддержка системы обеспечения физической безопасности в формате управляемой услуги.
- Обеспечение безопасности ЦОД. Обеспечьте эффективную работу, производительность и безопасность центра обработки данных путем проведения оценок безопасности объекта, разработки архитектуры безопасности ЦОД, а также путем предоставления услуг по проектированию и внедрению решения для повышения уровня защищенности ЦОД.
- Обеспечение безопасности сетей передачи и распределения электроэнергии. Повышение эффективности решений для обеспечения безопасности сетей передачи и распределения электроэнергии при постоянном контроле расходов на интеграцию путем определения требований к электростанциям/подстанциям, разработки будущих архитектур обеспечения безопасности электростанций и подстанций, а также предоставления услуг по развертыванию соответствующих решений.
- Обеспечение безопасности систем управления энергопотреблением. Безопасная интеграция решения Cisco Network Building Mediator с системами управления энергопотреблением с помощью полномасштабных услуг по разработке стратегии, архитектуры, проекта системы и ее развертыванию.
- Развертывание решений для обеспечению безопасности. Ускорение развертывания интегрированных решений по обеспечению безопасности с помошью услуг по планированию, проектированию и реализации.
- Оптимизация инфраструктуры безопасности. Поддержка доверенной отказоустойчивой инфраструктуры безопасности путем проведения регулярных оценок, планированию технологических решений и постоянного анализа архитектуры.

© Cisco Systems, Inc, 2009. С сохранением всех прав. В данном документе содержится информация, свободно распространяемая компанией Cisco.

Системный подход Cisco к созданию систем безопасности и колоссальный опыт экспертов Cisco представляют собой надежную основу для решения сложных задач обеспечения безопасности интеллектуальных систем энергоснабжения и создания защищенной интеллектуальной коммуникационной сети, которая необходима для предоставления информации об энергоснабжении предприятиям коммунального хозяйства практически в режиме реального времени. Такой подход позволяет управлять всей системой энергоснабжения как единой интегрированной системой, активно реагируя на изменения энергопотребления.

© Cisco Systems, Inc, 2009. С сохранением всех прав. В данном документе содержится информация, свободно распространяемая компанией Cisco.

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, 191186, Санкт-Петербург,
бизнес-центр «Регус»,
Невский пр-т, 25, 2-й этаж, офисы 9, 30.
Телефон: +7 (812) 336 6531
Факс: +7 (812) 346 7800
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.**

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)