

Cisco Security Academy

Moscow 2007

Программа на 26 сентября

my.cisco.ru

Время	Название доклада, ответственный	Описание
10.00-11.00	Архитектура безопасности Cisco Алексей Лукацкий	В рамках доклада рассматриваются различные аспекты архитектуры безопасности Cisco: – Стратегия безопасности Cisco Self-Defending Network 3.0 – Архитектура построения защищенной сети SAFE 3.0 – Сервисы безопасности: консалтинг, обучение, поддержка, сертификация и т. д.
11.00-12.00	Как обеспечить соответствие узлов сети политике ИТ и ИБ Михаил Кадер	В данной сессии мы обсудим технологию контроля сетевого доступа – NAC (Network Admission Control). Эта технология предназначена для обеспечения соответствия состояния компьютеров корпоративной политике безопасности. Она является ключевой для снижения вредоносного влияния разнообразных вирусов и «червей» на современные сети. Мы обсудим как саму технологию, так и варианты ее использования. В ходе нашего обсуждения будут затронуты как инфраструктура NAC, реализованная на инфраструктурном оборудовании компании Cisco, таком как маршрутизаторы, коммутаторы локальной сети, точки беспроводного доступа, концентраторы VPN, так и ее совместимость с технологией Microsoft NAP (Network Access Protection). Мы также остановимся на использовании основного специализированного продукта по контролю сетевого доступа – системе NAC appliance и обсудим рекомендации по ее внедрению в существующих сетях.
12.00-13.00	ИТ и ИБ. Как избежать конфликта с помощью Cisco Михаил Кадер	В рамках этого доклада будет обсуждаться вопрос эффективного построения систем управления и мониторинга информационной безопасности, а также их совместного использования и разграничения доступа для сотрудников различных подразделений, таких как ИТ и ИБ. Будут затронуты вопросы построения системы внеполосного управления. Мы обсудим примеры построения систем управления на базе концепции построения защищенных сетей Cisco SDN, а также вопросы управления непосредственно устройствами, обеспечивающими безопасность Вашей сети, включая межсетевые экраны, системы обнаружения вторжений и т. п. Мы также остановимся на продуктах Cisco Security Manager, Cisco MARS и Cisco Secure ACS, предназначенных для полнофункционального управления средствами сетевой безопасности.
13.00-14.00	От мониторинга средств защиты к Security Operations Center (включая «живую» демонстрацию) Женя Линькова	Сессия посвящена основным аспектам построения Security Operations Center. В рамках доклада рассматриваются следующие вопросы: – роль SOC в жизни сети – требования к SOC – основные компоненты SOC и их интеграция между собой
14.00-15.00	Безопасность центров обработки данных Олег Самарин	Создание центров обработки данных (ЦОД) – одного из важнейших компонентов информационной системы современного предприятия – невозможно без учета факторов, влияющих на безопасность информации, хранимой и обрабатываемой в ЦОД. Компания Cisco Systems, ведущий производитель решений в области информационной безопасности, всегда уделяла пристальное внимание выработке наиболее эффективных решений задач, возникающих при построении ЦОД. В предлагаемой презентации рассматриваются различные аспекты обеспечения информационной безопасности в центрах обработки данных, особенности архитектурных решений, применяемых при их построении, продукты и технологии Cisco Systems для решения задач ИБ в ЦОД.
15.00-16.00	Безопасность органов государственной власти Руслан Иванов	В сессии рассматриваются решения Cisco Systems для органов государственной власти в области ИБ, анализируется текущее законодательство в области ИБ применительно к продуктам компании, а также рассказывается о сертификации продукции в соответствии с требованиями российских стандартов и регламентов по безопасности.
16.00-17.00	Безопасность в коммутируемых сетях (L2) Алексей Жуков	В сессии рассматриваются как типовые атаки, реализуемые злоумышленниками в коммутируемых сетях, так и методы защиты от них. При этом упор будет сделан на встроенных возможностях коммутационного оборудования Cisco, которые позволяют многократно повысить уровень защиты сети, не прибегая к внедрению дополнительных и дорогостоящих средств защиты.

Cisco Security Academy

Moscow 2007

Программа на 27 сентября

my.cisco.ru

Время	Название доклада, ответственный	Описание
10.00-11.00	Неизвестная безопасность Cisco Алексей Лукацкий	В рамках доклада обсуждаются вопросы, очень редко рассматриваемые на различных мероприятиях по безопасности. Среди них: – Как Cisco защищает сама себя? – Программа SafeHarbor – Подразделение Critical Infrastructure Assurance Group (CIAG) – Бюллетени по безопасности (в сервисах IntelliShield, PSAR, PSIRT) – Финансирование проектов по безопасности с помощью Cisco
11.00-12.00	Безопасность оператора связи Павел Антонов	В последние годы происходит бурный рост числа разнообразных угроз информационной безопасности в сети Интернет. Далеко не все пользователи сети Интернет правильно настраивают и регулярно обновляют программные средства защиты на своих компьютерах, а во многих случаях персональные компьютеры вообще никак не защищены. В этой ситуации на операторов связи ложится задача по обеспечению эффективной защиты от вирусов, зомби-сетей, распределенных атак типа «отказ в обслуживании», рассылок спама и интернет-мошенничества. Предлагаемые компанией Cisco Systems технологии и продукты позволяют оператору связи и абонентам принять непосредственное участие в обеспечении безопасности как персональных компьютеров абонентов, так и сети оператора в целом.
12.00-13.00	Безопасность не только сети. Защита ПК, сервера, ноутбука и... коммуникатора Владимир Илибман	В рамках сессии будут рассмотрены актуальные вопросы защиты серверов, рабочих станций, ноутбуков и современных персональных коммуникационных устройств. В частности, в презентации предлагаются типичные сценарии использования решений Cisco Network Admission Control, Cisco Security Agent, технологий безопасного удаленного доступа к корпоративной сети предприятия.
13.00-14.00	Обеспечение безопасности в промышленности и ТЭК Андрей Гречин	В первой части презентация освещает основные тенденции в развитии современных автоматизированных систем управления технологическими процессами (АСУ ТП) и связанные с этим риски информационной безопасности и безопасности технологических процессов. Во второй части будут рассмотрены несколько практических примеров построения защищенных сегментов ЛВС для нужд АСУ ТП, построения территориально распределенных сетей АСУ ТП, вопросы объединения сетей АСУ ТП и ЛВС предприятий.
14.00-15.00	Безопасность электронной почты и Web-доступа Павел Антонов	Электронная почта является на сегодняшний день доминирующей формой делового общения. Распространенность этого средства передачи информации также привлекает большое и постоянно растущее количество угроз безопасности – спам, подделка писем, вирусы и кража интеллектуальной собственности. Web давно перестал быть просто средством ведения домашних страниц. Сегодня, в эпоху XML, SOAP, RSS, Web 2.0 и т. д., Web превращается в среду ведения бизнеса и, как следствие, мишень для различных атак. В этом докладе мы расскажем о стратегии Cisco в области безопасности E-mail и Web и решениях, ее реализующих.
15.00-16.00	SecureEverything – безопасность везде Алексей Жуков	Безопасность для Cisco не ограничивается только межсетевыми экранами, системами предотвращения атак, VPN-решениями и т. п. В первую очередь безопасность для Cisco – это неотъемлемое свойство всех наших технологий – унифицированных коммуникаций, систем хранения данных, беспроводных сетей, коммутаторов и маршрутизаторов и т. д. О встроенных защитных возможностях этих технологий и пойдет речь в данной сессии.
16.00-17.00	Открытая дискуссия с экспертами Cisco Алексей Лукацкий, Михаил Кадер, Женя Линькова, Владимир Илибман, Павел Антонов, Андрей Гречин, Алексей Жуков, Руслан Иванов, Олег Самарин	В рамках данной сессии вы сможете задать любые интересующие вас вопросы ведущим экспертам Cisco по безопасности и получить на них исчерпывающие ответы.