



Комплексность системы сетевой защиты: декомпозиция протоколов, модульность функций, вопросы архитектуры, стандартизации и сертификации

**Рябко С.Д., генеральный директор ЗАО «С-Терра СиЭсПи», к.ф.-м.н.
Инфофорум Евразия, 5 июня 2008 г.**

ЧЕМ ХАРАКТЕРИЗУЕТСЯ СОВРЕМЕННАЯ КОМПЛЕКСНАЯ ИНФОРМАЦИОННАЯ СИСТЕМА?

Структурность, сложность архитектуры

Масштаб

количественный аспект, большое количество структурных элементов
аспект системы массового обслуживания, статистически большое количество пользователей, сложная система функций и прав доступа
информационный аспект – число контролируемых объектов давно за пределами простого человеческого восприятия, высочайшие объемы информации, скорости ее обработки и потоков данных

Распределенная информационная среда

географический аспект, требования на коммуникации
логический аспект, множество взаимодействующих иерархизированных и/или одноранговых вычислительных процессов

Гетерогенность

система «соткана» из продуктов сотен производителей
вопросы стандартизации и совместимости (грядут кросс-ведомственные системы!)
различный уровень доверия к производителям; отсутствие возможности реализовать даже высоко ответственные системы только на отечественных ИКТ-продуктах

Высокая динамика технологий

«текучесть» технических стандартов и решений
темп разработки ИКТ-продукции превышает мыслимые отечественные мощности систем аттестации и сертификации свойств безопасности
«снежный ком» обновлений: сроки разработки новых версий и обновлений ПО короче сроков их сертификации

РАСПОЛАГАЕМ ЛИ МЫ МЕТОДИКАМИ КОМПЛЕКСНОЙ ЗАЩИТЫ И ОЦЕНКИ БЕЗОПАСНОСТИ ТАКИХ СИСТЕМ?

- О техническом регулировании
- Декомпозиция стека безопасности
- Функции сетевой защиты
- VPN: СЗИ или СКЗИ?
- О комплексности

О техническом регулировании

s•terra

C S P

Cisco Solution Technology Integrator

● **Аттестация, как оценка защищенности системы**

- ★ **Попытка осмысления задач аттестации комплексной информационной системы и/или сертификации ее компонент порождает ряд методических и технических вопросов:**
 - 1. В какой системе и какую функциональность аттестовать/сертифицировать? Какую нормативную базу сертификации использовать?**
 - 2. Как трактовать в терминах требований аттестации/сертификации распределенную систему? ... многопользовательскую систему? ... взаимодействие вычислительных процессов?**
 - 3. Какова роль технических стандартов? На какие технические стандарты следует ориентироваться?**
 - 4. Допустимо ли применение международных криптографических стандартов в целях защиты? ... в целях отладки? Требуется ли совместимость отечественных и международных продуктов?**
 - 5. Должна ли аттестация комплексных систем безопасности быть массовым явлением? Если да – то как ее организовать?**



* Руководящие документы ФСТЭК России:

Добротная и наработавшая беспрецедентно широкую практику сертификации и аттестации нормативная база База сертификации комплексной системы требует развития

- есть ряд открытых вопросов по тематике коммуникационных, распределенных модульных и объектных систем

* Требования и рекомендации ФСБ России:

Детальная разработка вопросов криптографии в открытом и закрытом регулировании

Ряд нормативов по прочим вопросам (подходы подобны ФСТЭК России) при менее обширной практике сертификации и аттестации



- ★ **ГОСТ Р ИСО/МЭК 15408**
Наработан позитивный опыт и методическая база сертификации в системе ФСТЭК России
 - один из лидеров – Центр Безопасности ИнформацииОпыт труден, очень специальная декомпозиция, трудный («птичий») метаязык декомпозиции и описания функций безопасности
- ★ **Пожалуй, единственная законченная технология, на базе которой можно строить сертификацию и аттестацию таких сложных объектов, как комплексные информационные системы**
Требуются массивированные усилия для разработки типовых профилей безопасности для широкого класса комплексных систем и/или функциональных узлов в их составе
- ★ **Также интересная возможность свести воедино результаты параллельных сертификаций в системах ФСТЭК и ФСБ России**

● Актуальные технические стандарты

* Что мы стандартизуем:

Терминологию (ГОСТ Р 50922-96 + Р 50.1.053-2005, ГОСТ Р 51275-99, ГОСТ Р 51897-2002)

Методики (ГОСТ Р 51241-98, ГОСТ Р ИСО/МЭК 15408)

Процессы (ГОСТ Р ИСО/МЭК 17799-2005, ГОСТ Р ИСО/МЭК 27001-2006)

* Что осталось за скобками государственного регулирования:

Реальные технические стандарты (ITU-T, IETF, W3C, OMG, вендоры, Open Source)

* Может в этом есть глубокий замысел?

«Пусть инженеры крутят гайки»

- вполне вероятно – единственная реалистичная позиция технического регулирования в мире быстро меняющихся технологий

Но следует понимать, что без стандартизации мы не решаем вопросов совместимости, а следовательно, платим за «нестыковки»

- цена вопроса – избыточность – уже сегодня может быть значительной; в нашей области это обычно интегрированный вручную «шлюз объединения несовместимых VPN»
- с развитием кросс-ведомственных информационных систем (те же персональные данные очень быстро приведут нас к ним) цена вопроса будет прогрессивно расти

- О техническом регулировании
- Декомпозиция стека безопасности
- Функции сетевой защиты
- VPN: СЗИ или СКЗИ?
- О комплексности

Декомпозиция стека безопасности

s•terra

C S P

Cisco Solution Technology Integrator

● Декомпозиция управления коммуникациями



- * **Сетевая безопасность – это коммуникационная дисциплина**
- * **Коммуникационное управление принято декомпозировать в виде иерархической логической структуры – стека протоколов**

при этом каждый уровень управления специализируется на своих задачах, эти задачи и логические (информационные) объекты для каждого уровня существенно различны

иного нам не дано: даже бизнес коммуникационных услуг распределен по стеку и предприятия, занятые в этом стеке, выполняют независимые задачи:

- прокладка и сопровождение СКС и кабельного хозяйства (**Phy**)
- доступ через модемные пулы, GPRS (**L**)
- Интернет-сервис-провайдеры (**N, T**)
- аутентификация и связанные службы, например, биллинг (**S**)
- контентные контейнеры, веб-хостинг, XML (**P**)
- web, почта и прочий контент (**A**)

СТЕК ИНФОРМАЦИОННЫХ ОБЪЕКТОВ, УГРОЗ И СРЕДСТВ ЗАЩИТЫ

OSI/ISO

TCP/IP



Объекты: ДОКУМЕНТЫ, ПРИКЛАДНОЙ КОНТЕНТ
Угрозы: компрометация документов, опасный контент
Защита: авторизация доступа, анти-вирус



Объекты: T-ЗАГОЛОВОК, T-СОЕДИНЕНИЕ
Угрозы: перехват соединения
Защита: межсетевой экран, SSL/TLS



Объекты: IP-ПАКЕТ, СИСТЕМА МАРШРУТИЗАЦИИ
Угрозы: подмена адресов, НСД, перехват пакетов
Защита: IPsec VPN, межсетевой экран

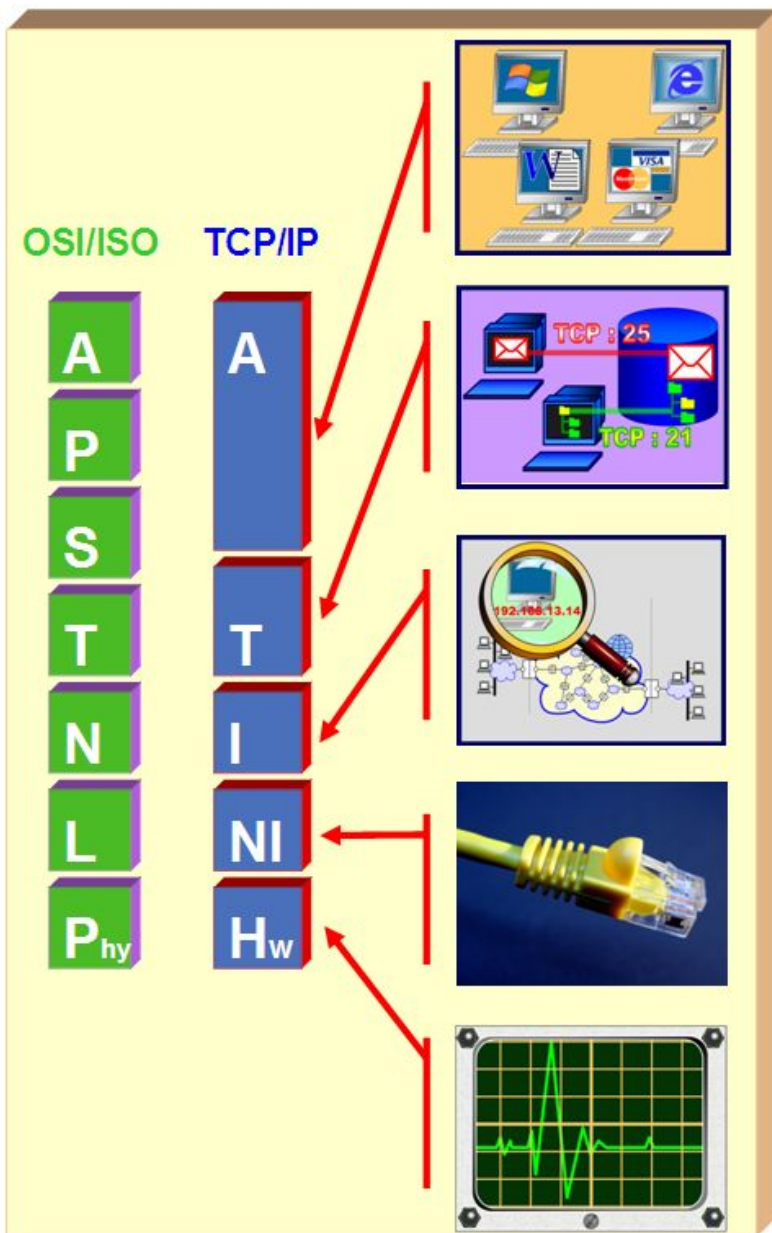


Объекты: MAC-ИНТЕРФЕЙС, ФРЕЙМ/КАДР
Угрозы: НСД к среде передачи данных, перехват
Защита: ARP/RARP мониторинг, канальный шифратор



Объекты: СРЕДА ПЕРЕДАЧИ ДАННЫХ, СИГНАЛ
Угрозы: несанкционированные подключения, ПЭМИН
Защита: физическая безопасность, экранирование

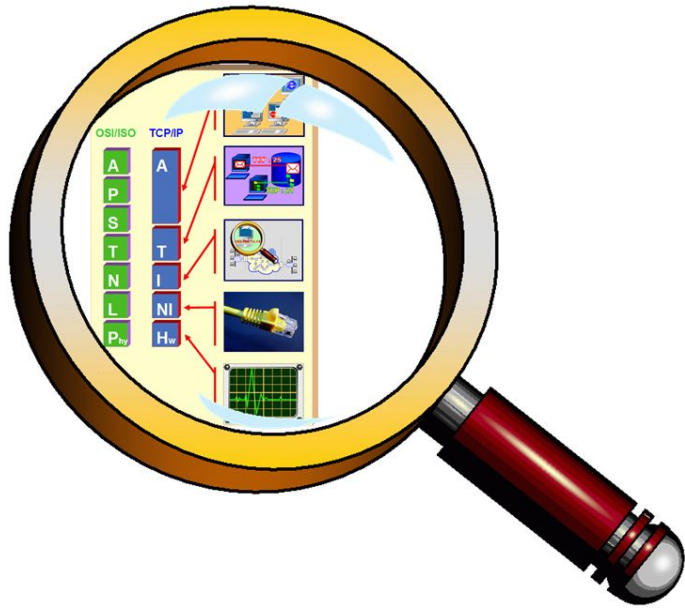
● Следствие 1. Модульность безопасности



- * Атаки (и меры защиты), применяемые на канальном уровне не применимы к прикладному уровню и наоборот
- * Следовательно, функции средств защиты информации, технические требования, критерии сертификации должны быть различными для модулей защиты, применяемых на различных уровнях управления в коммуникационном стеке

Модульный подход к безопасности коммуникационной системы практически не представлен в системах сертификации. Исключение составляют только документы ФСТЭК и ФСБ России по межсетевым экранам и некоторые документы, разработанные на основе ГОСТ Р ИСО/МЭК 15408

● Следствие 2. Холистический дизайн стека



- * С другой стороны, функции различных уровней в стеке не независимы
В конце 1980х ISO попыталась спроектировать стек коммуникационных протоколов с высокой декомпозицией. Это было сделано для того, чтобы логически развязать уровни управления, сделать протоколы определенного уровня взаимозаменяемыми
В результате протокол заданного уровня «не знал», что делают «смежники». Это приводило к функциональной избыточности каждого уровня, система потеряла эффективность, глобальный проект провалился
- * Индустрия извлекла из этого поражения урок: дизайн стековых модулей должен производиться в контексте общих требований к целостной архитектуре комплексной системы
- * Следовательно, технические требования и критерии сертификации модульных СЗИ должны быть гармонизированы в рамках строго определенных условий применения, указывающих, какие функции безопасности выполняет данный модуль, а какие забирает на себя смежная система на другом уровне

О техническом регулировании
Декомпозиция стека безопасности
Функции сетевой защиты
VPN: СЗИ или СКЗИ?
О комплексности

Функции сетевой защиты

s•terra

C S P

Cisco Solution Technology Integrator

● Сетевая безопасность



- * Сетевая безопасность в широком смысле – это комплекс мер защиты от атак, осуществляемых методами сетевого доступа
- * Сетевая безопасность в узком смысле – это средства защиты информации, применяемые на сетевом и транспортном уровнях, в первую очередь – межсетевые экраны и VPN
 - Эти средства защиты обрабатывают каждый сетевой пакет, обойти их невозможно и они обеспечивают полный контроль над коммуникациями любого компьютера, отдельно взятого приложения или каждого пользователя
- * Структурообразующие средства сетевой информационной безопасности высвечивают ключевые проблемы построения комплексной системы защиты

● VPN – средство шифрования данных?



- ✦ Бытует и в ряде нормативных документов прямо представлено мнение, что

«VPN – это средство шифрования данных при их распространении по открытым (недоверенным) каналам связи»

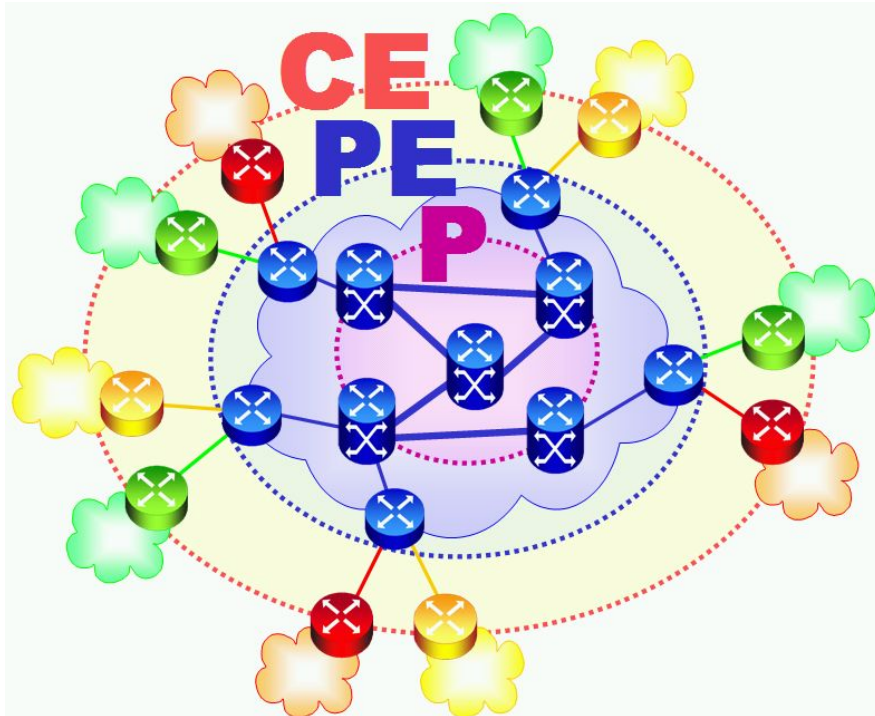
ТАК ЛИ ЭТО?

● Функции СКЗИ и функции VPN



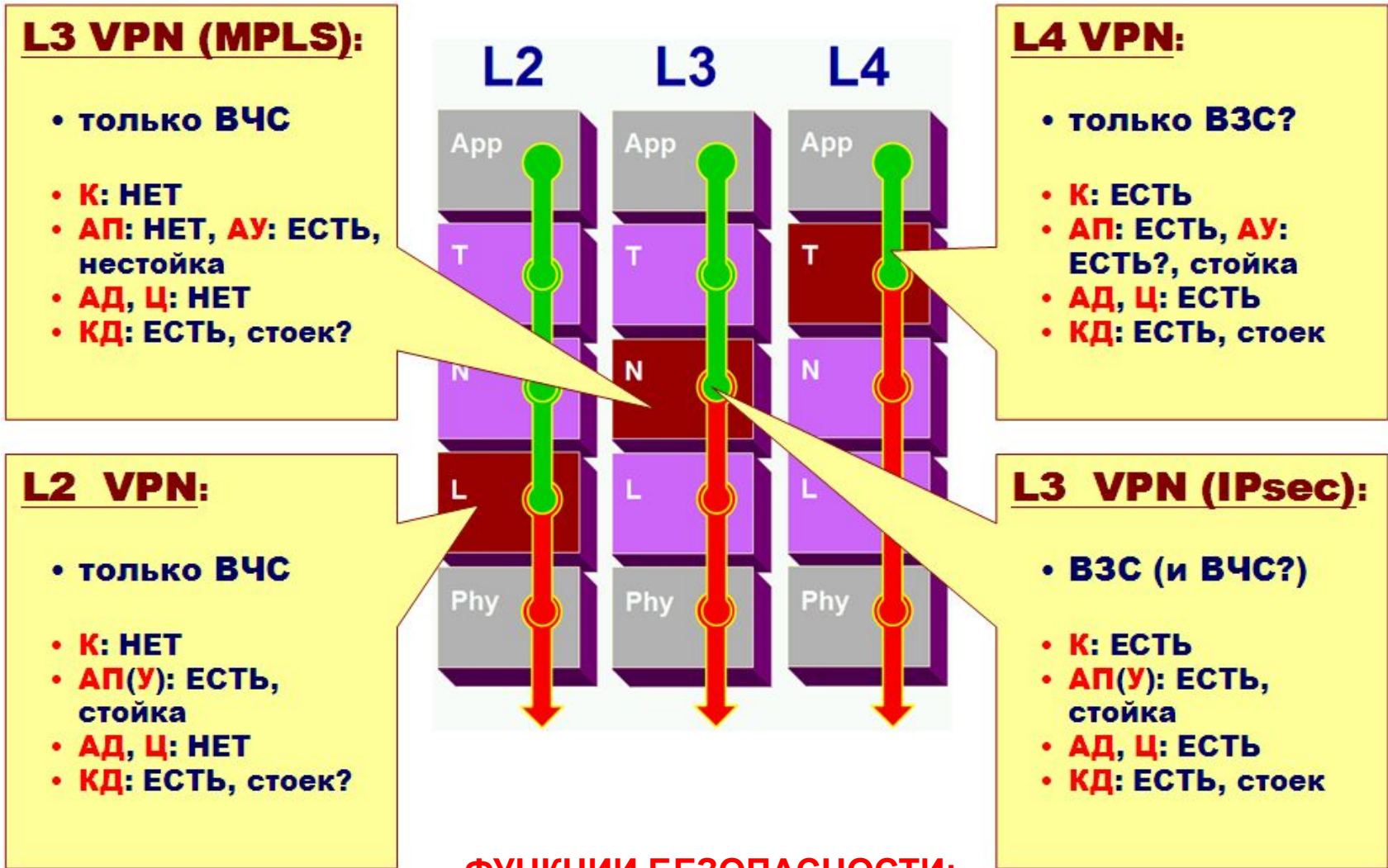
- * **СКЗИ:**
Локализуется в точке создания, обработки, модернизации, уничтожения данных
Прилагает криптографический сервис непосредственно к защищаемым данным
Обеспечивает, по мере возможности, сквозной (от отправителя к получателю данных, без разрывов и перешифрования) сервис защиты
Применяется от имени строго определенного субъекта – владельца данных
- * **VPN не соответствует ни одному из этих критериев**
Первичный документ трансформируется в пакеты
Пакеты (открытый трафик) распространяются по сложной сети, где данные могут быть компрометированы
Защита прилагается к пакетам (а не к документу) на удаленном шлюзе; шлюз может обрабатывать лишь часть пакетов
- * **Поэтому VPN должен применяться наряду с СКЗИ прикладного уровня**
Это полностью соответствует модульности и специализации уровней управления в декомпозиции OSI/ISO
Факторы модульности (наличие той или иной «смежной» функциональности) должны учитываться при сертификации модульных СЗИ/СКЗИ, как среда функционирования
- * **В ЧЕМ ЖЕ ОСНОВНАЯ ФУНКЦИЯ VPN?**

● VPN – это частное сетевое пространство



- * **Функция VPN – средство защиты сетевой инфраструктуры в совокупности**
- * **Классическое определение:**
RFC 4026, L. Andersson, T. Madsen, Acreo AB, «Provider Provisioned Virtual Private Network (VPN) Terminology»: VPN - это «способ использования открытых или частных сетей таким образом, чтобы пользователи VPN были отделены от других пользователей и могли взаимодействовать между собой, как если бы они находились в единой закрытой (выделенной) сети»
- * **Дуализм слова **Private** в VPN:**
Частный (ВЧС)
Защищенный (ВЗС)
но, с точностью до механизмов, эти сети решают одну задачу: изоляция корпоративного информационного пространства
- * **Пример: MPLS VPN**

● L2, L3, L4 VPN. Голова кругом идет...



ФУНКЦИИ БЕЗОПАСНОСТИ:
 К – конфиденциальность; Ц – целостность;
 АП – аутентификация пользователя; АУ – аутентификация устройства;
 КД – контроль доступа

● L2, L3, L4 VPN, гибриды

MPLS + IPsec:

- наиболее развитый набор коммуникационных сервисов
- требует защиты, если Вы не доверяете провайдеру

L4 VPN:

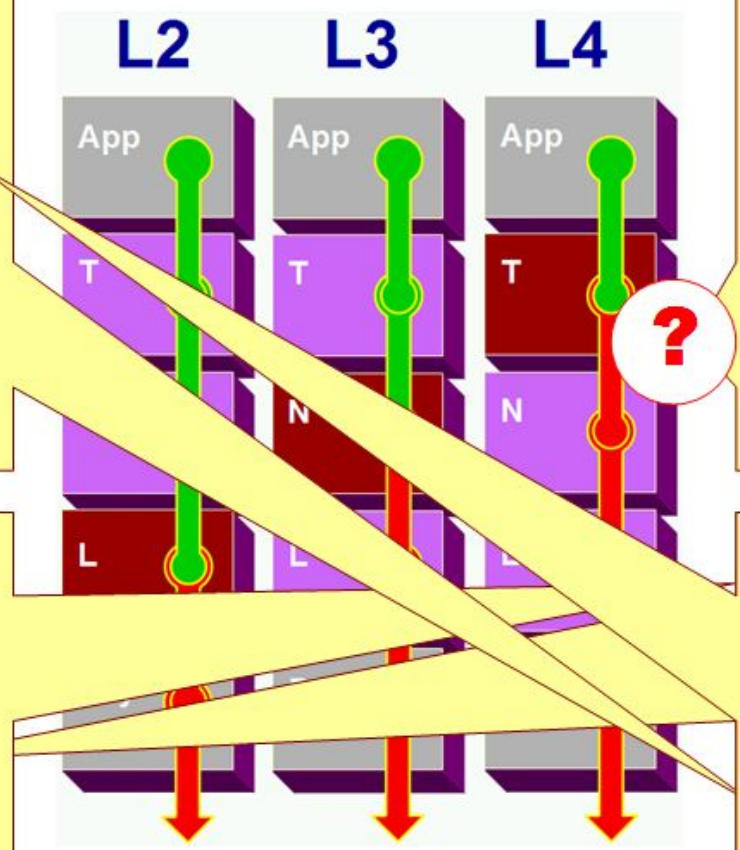
- может применяться, как доп. защита для L2, L3 ВЧС
- практические случаи применения не известны

PPP+, L2TP + IPsec:

- требует защиты, если Вы не доверяете провайдеру

IPsec:

- сервисы аутентификации, конфиденциальности, стойкого контроля доступа
- изоляция на «последней миле» при доступе к MPLS



802.1q/1x: ?

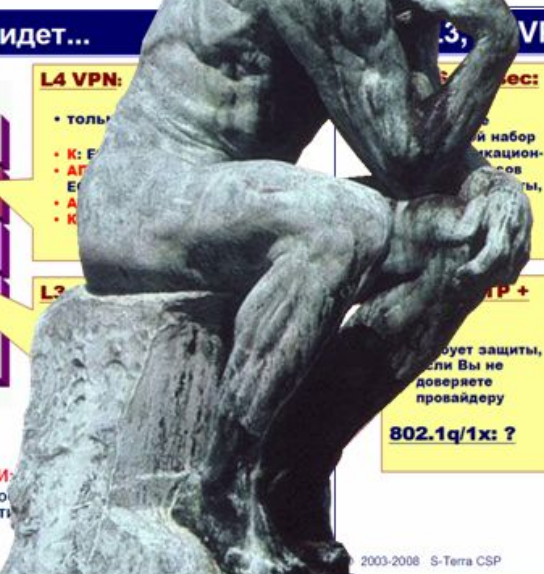
IP[IPsec[IP[L2TP[Ethernet+]]]]

IP[IPsec[PPP[IP]]]

IP[IPsec[GRE[IP+]]]

IP/MPLS[IPsec[IP]]

● Промежуточный финиш: комплексность VPN



● L2, L3, L4 VPN. Голова кругом идет...

L3, L4 VPN, гибриды

L3 VPN (MPLS):

- только ВЧС
- К: НЕТ
- АП: НЕТ, АУ: ЕСТЬ, нестойка
- АД, Ц: НЕТ
- КД: ЕСТЬ, стоек?

L2 VPN:

- только ВЧС
- К: НЕТ
- АП(У): ЕСТЬ, стойка
- АД, Ц: НЕТ
- КД: ЕСТЬ, стоек?

L4 VPN:

- только ВЧС
- К: ЕСТЬ
- АП: ЕСТЬ
- АД: ЕСТЬ
- Ц: ЕСТЬ
- КД: ЕСТЬ

L4 VPN:

- может применяться, как доп. защита для L2, L3 ВЧС
- практические случаи применения не известны

IPsec:

- сервисы аутентификации, конфиденциальности, стойкого контроля доступа
- изоляция на «последней миле» при доступе к MPLS

ФУНКЦИИ БЕЗОПАСНОСТИ:
К – конфиденциальность; Ц – целостность;
АП – аутентификация пользователя; АУ – аутентификация;
КД – контроль доступа

802.1q/1x: ?

IP[IPsec[IP[L2TP[Ethernet+]]]]
IP[IPsec[PPP[IP]]]
IP[IPsec[GRE[IP+]]]
IP/MPLS[IPsec[IP]]

© 2003-2008 S-Terra CSP

Только функциональность VPN – комплексная система защиты, декомпозированная по нескольким уровням управления OSI/ISO, интегрированная с общесетевой функциональностью, свойства безопасности которой существенно зависят от состава применяемых технологий (протоколов), модульной архитектуры системы и множества прочих факторов

КАК ОЦЕНИТЬ КАЧЕСТВО ЗАЩИТЫ ЭТОГО СЕРВИСА?

О техническом регулировании
Декомпозиция стека безопасности
Функции сетевой защиты
VPN: СЗИ или СКЗИ?
О комплексности

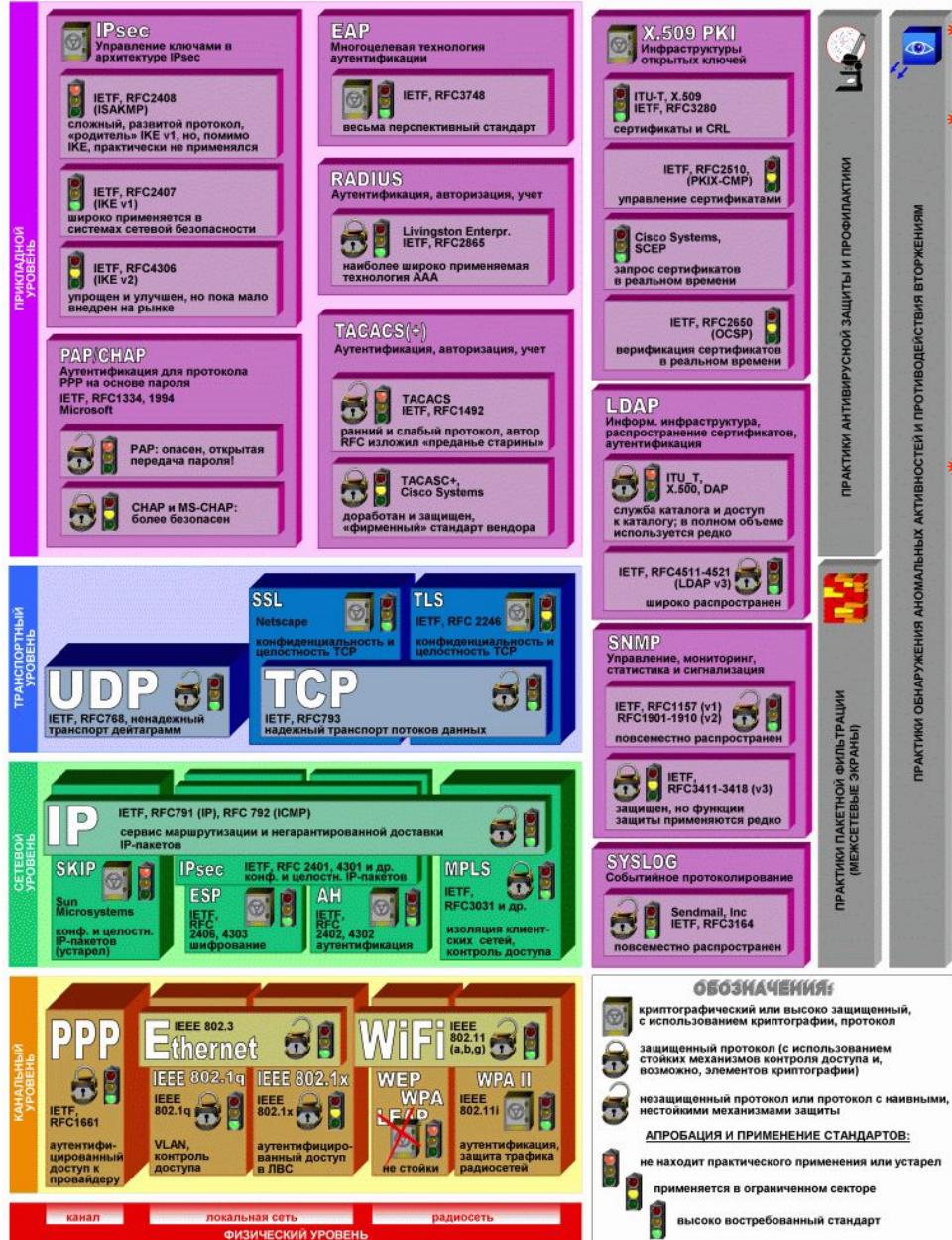
VPN: СЗИ или СКЗИ?

s•terra

C S P

Cisco Solution Technology Integrator

Криптография применяется повсеместно



На рисунке показана структура стека протоколов защиты информации
Приняты обозначения:



криптографический протокол
защищенный протокол (почти всегда применяются средства криптографии)
слабозащищенный или «сломанный» протокол

Из рисунка видны доводы в пользу применения технических стандартов:

1. Стандарт обеспечивает совместимость
 - совместимость – сама по себе слабый довод в пользу безопасности, но она обеспечивает важный технологический фактор качества защиты: кросс-отладку с третьим производителем
2. На проработку архитектуры стандарта брошены ресурсы, которых нет ни у одного, даже крупного, производителя
3. Стойкость защиты стандартного протокола подвергается массовому публичному анализу, его «проверяет на зуб» масса производителей и «ломает» армия хакеров
4. Стандарт обеспечивает уровень документированности поведения, который не обеспечивает техническая документация ни одного производителя «частных» решений

● Границы криптографического приложения



* Пример

Пароль при логине в операционную систему – казалось бы, «чистый НДС»?

- но пароль передается между модулями в зашифрованном виде или как хэш
- но файл с паролями обязательно должен быть зашифрован...

Может быть, все-таки, пароль – это СКЗИ?

* Вопрос о VPN

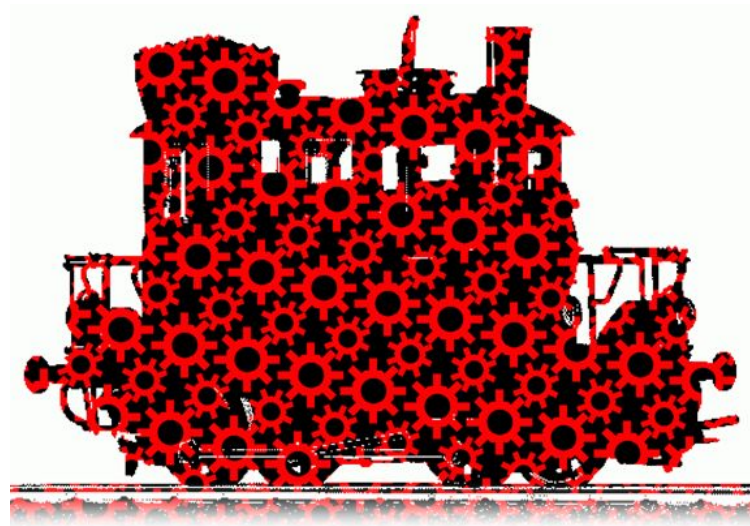
Протоколы криптографически нейтральны

Встроенные криптобиблиотеки вызываются через штатный интерфейс и сертифицированы как СКЗИ

VPN-протокол «просто» заводит буфер, таймауты и счетчики, применяет к данным выполняемые во внешнем СКЗИ преобразования и передает данные в сеть в определенном порядке...

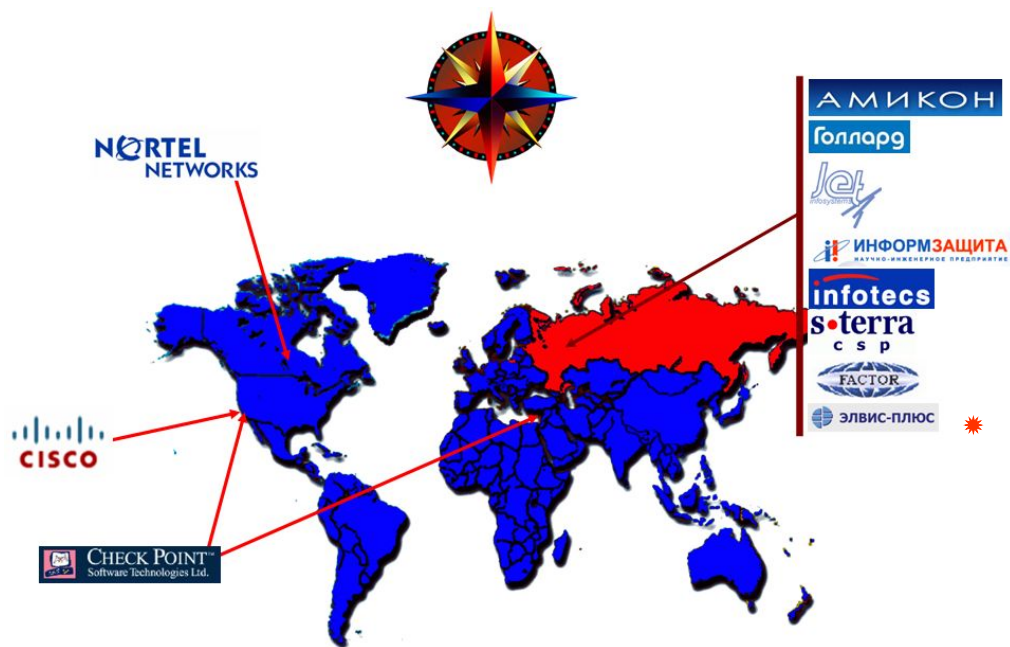
Может, все-таки, VPN – это не СКЗИ?

● Переход количества в качество



- ✦ До недавнего времени такая точка зрения доминировала на отечественном рынке
 - Модель «внешней модульной криптографии в VPN» эксплуатируется пятью ведущими производителями на рынке и соответствует современным требованиям регулирования
- ✦ Однако по инициативе ФСБ России этот взгляд на комплекс функциональности VPN изменяется
 - Приложения VPN предлагается трактовать, как СКЗИ
 - Основания для такого взгляда: стойкость сервиса VPN существенно зависит от структуры и корректности реализации криптографического протокола
- ✦ Мы полностью разделяем этот взгляд и по рекомендации ФСБ России начали движение в направлении сертификации в системе ФСБ России наших VPN-продуктов, выполненных на основе международных стандартов архитектуры IP Security

«Наши» и «их» криптографические стандарты



- ✦ Тем не менее, ряд вопросов остается для проработки

Один из них – применение западных криптоалгоритмов

В сетевой защите есть как минимум две задачи, в которых мы не можем полностью от них отказаться:

- Совместимость, как со средствами инфраструктуры, так и с западными продуктам
- Защита радиосетей на канальном уровне, где западная криптография «вшита в железо» и где нет возможности «перепрошить» микрокод тысяч производителей

Кстати

Уже лет пять российского производителя пугают ВТО: «с ВТО придет западный вендор, упадет крыша протекционизма и все вы умрете»

А причем тут ВТО? В сетевой безопасности Cisco, Nortel и Check Point уже в России – и с российскими криптоалгоритмами...

- ✦ **СЛЕДУЕТ ЛИ ПОЛНОСТЬЮ ОТРИЦАТЬ СВОЙСТВА БЕЗОПАСНОСТИ, ОБЕСПЕЧИВАЕМЫЕ ЗАПАДНЫМИ КРИПТОАЛГОРИТМАМИ?**

В любом случае – нельзя пренебрегать кросс-отладкой стандартных протоколов, это – вопрос качества отечественного продукта

- О техническом регулировании
- Декомпозиция стека безопасности
- Функции сетевой защиты
- VPN: СЗИ или СКЗИ?
- О комплексности**

О комплексности

s•terra

C S P

Cisco Solution Technology Integrator

● Итак, комплексная система защиты...



- * **ТРЕБОВАНИЯ ПО УРОВНЮ ЗАЩИЩЕННОСТИ (ЦЕЛЯМ АТТЕСТАЦИИ) СЛЕДУЕТ ЗАКЛАДЫВАТЬ НА ЭТАПЕ ФОРМИРОВАНИЯ ТЗ**

Проект хорошо бы завершать этапом аттестации системы

- * **Однако:**

В отечестве есть добротные руководящие и методические документы по частным вопросам

Практика аттестаций комплексных систем не распространена и пока базируется на частных методических наработках и энтузиазме органов аттестации

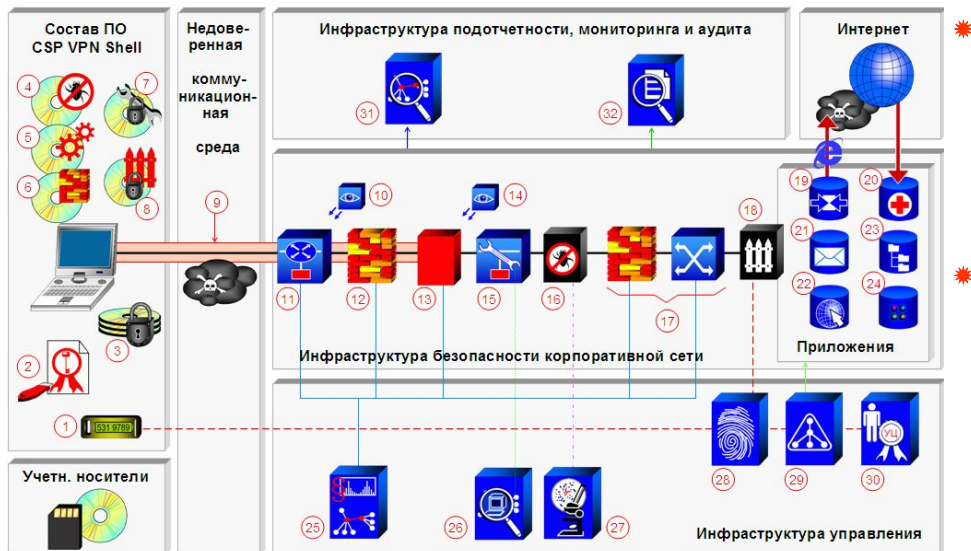
Нет рекомендованной методики оценки защищенности, адресованной к комплексной системе в целом

● Проблема модульности комплексной системы



- * Система формируется из ИКТ-продуктов, СЗИ и СКЗИ
Свойства их безопасности, уровни сертификации различны
Защищенность системы зависит от комбинации продуктов
Функции защиты каждого продукта определяются его политикой безопасности (внутренними настройками)
- * Руководства по подбору «деталей» для сборки комплексной системы (т.е. рекомендаций по применению технологических стандартов) нет
Задача технологической стандартизации в принципе решаемая, но требует более активной позиции органов стандартизации
- * Руководства, как «сшить» функции защиты моделей воедино, нет
Разработка такого универсального руководства вряд ли технически реализуема

● Проблема интеграции инфраструктуры



Ключевое значение имеет единая инфраструктура безопасности комплексной системы

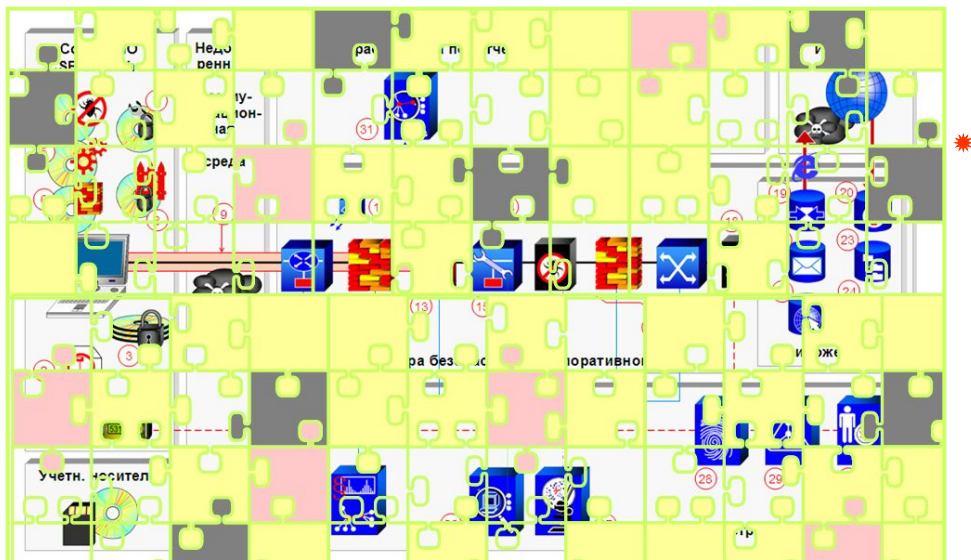
Основной вопрос – видите Вы картину безопасности системы в целом или как набор разрозненных фрагментов

Факторы безопасности, связанные с единством инфраструктуры системы в регулировании не рассмотрены

В то же время для крупной системы эти факторы определяющим образом влияют на ее безопасность: начиная с некоторого уровня развития политику безопасности в масштабах системы и мониторинг событий безопасности невозможно осуществлять иначе, чем с применением централизованных автоматизированных систем

В области создания доверенной инфраструктуры безопасности существует проблема масштаба для отечественного разработчика: задача разработки собственных инфраструктурных продуктов ему не по силам

Мы вынуждены либо отказываться от применения этих продуктов, либо допускать определенный уровень доверия импортным продуктам



● Проблема отставания нормативов

- ✦ **Существующие нормативы оценки защищенности автоматизированных систем требуют**

Доработки для применения к распределенным, модульным, объектным системам

Развития понятий «доверие», «доверенная вычислительная/коммуникационная среда», «доверенное устройство»

Адаптации ряда технических параметров для применения в высокоскоростных вычислительных системах, гигабитных каналах связи, мультисервисных сетях

Учета темпа разработки и обновления современных ИКТ-продуктов, ускорения процессов и адаптации технологий сертификации к разработке отдельно поставляемых модулей и обновлений программных продуктов, усложнению процессов управления конфигурациями устройств



● Где мы находимся?

Итак, комплексная система защиты...

- ТРЕБОВАНИЯ ПО УРОВНЮ ЗАЩИЩЕННОСТИ (ЦЕЛЫЙ АТТЕСТАЦИИ) СЛЕДУЕТ ЗАКЛАДЫВАТЬ НА ЭТАПЕ ФОРМИРОВАНИЯ ИС
- Проект хорошо бы завершить на этапе аттестации системы
- Однако:
 - В отечестве есть руководящие документы и вопросы
 - Практика комплексной защиты баз данных не имеет ни одного примера



© 2003-2008 S-Terra CSP 28

Проблема интеграции инфраструктуры

- Ключевым фактором сложности является единая инфраструктура безопасности
 - Основной вопрос – видите Вы картину безопасности системы в целом или как набор разрозненных фрагментов
- Факторы безопасности, связанные с единой инфраструктурой системы в регулировании не рассмотрены
- В то же время эти факторы для крупной системы весьма существенны: начиная с некоторого уровня развития попытку безопасности в масштабах системы и мониторинг событий безопасности невозможно осуществлять иначе, чем с применением централизованных автоматизированных систем
- В области создания доверенной инфраструктуры безопасности существует проблема масштабности для ответственного разработчика: задача разработки собственных инфраструктурных продуктов ему не по силам
- Мы вынуждены либо отказываться от применения этих продуктов, либо допускать определенный уровень доверия импортным продуктам



© 2003-2008 S-Terra CSP 30

Проблема модульности



© 2003-2008 S-Terra CSP 29

Адаптация нормативов

- Существующие нормативы оценки защищенности технических средств и автоматизированных систем требуют
 - Доработки для применения к распределенным, модульным, объектным системам
 - Развития понятий «доверие», «доверенная вычислительная коммуникационная среда», «доверенное устройство»
 - Адаптации ряда технических параметров для применения в высокоскоростных вычислительных системах, гигабитных каналах связи, мультисервисных сетях
 - Учета темпа разработки и обновления современных ИКТ-продуктов, ускорения процессов и адаптации технологий сертификации к разработке отдельно поставленных модулей и обновлений программных продуктов, усложнению процессов управления конфигурациями устройств



© 2003-2008 S-Terra CSP 31

- Чтобы построить защищенную систему надо уметь задать требования по ее защищенности и оценить ее защищенность
- Современное состояние ИТ индустрии таково, что множество комплексных информационных систем существует как факт адекватно защищенные системы и аттестованные комплексные системы, скорее, единичны
- защита комплексных систем в стадии развития «лоскутная информатизация»
- рейтинги информатизации России [Ю.Е.Хохлов, Инфофорум Евразия 2008] – в середине списка, соседи – Турция, Колумбия, Румыния, Беларусь

● Что делать?



- * [Ю.Е.Хохлов, Инфофорум Евразия 2008]: «Главный барьер – не технологические, а нормативные и организационные вопросы»
- * Проблема не решается усилиями отдельного ведомства или комитета
- * Нужна осознанная государственная техническая политика, устанавливающая
 - Приоритеты развития:
 - технологичность ...
 - безопасность ...
 - ... или то и другое?
 - Статус технических стандартов, профили рекомендованных технологий
 - Статус требований безопасности
- * В реализации такой политики – нужно сотрудничество государственных органов технического регулирования, ведомств, технических комитетов и представителей индустрии
 - ... Но первая скрипка принадлежит государству, не индустрии и не ведомствам

КОНТАКТЫ

e-mail: information@s-terra.com
автор: rsd@s-terra.com

web: <http://www.s-terra.com/>

Тел.: +7 (495) 531 9789

+7 (495) 726 9891

Факс: +7 (495) 531 9789

Вопросы?

Обращайтесь к нам!

s•terra

C S P

Cisco Solution Technology Integrator