XI ежегодная международная конференция
«PKI-FORUM Россия 2013»

Вопросы построения публичных удостоверяющих центров

Алексей Уривский
ОАО «ИнфоТеКС»
urivskiy@infotecs.ru

Требования приказа ФСБ РФ № 796 к средствам УЦ

Приложение 2 пункт 35:
«При подключении средств УЦ
к информационно-телекоммуникационной
сети, доступ к которой не ограничен определенным кругом лиц, указанные средства должны соответствовать требованиям к средствам УЦ класса **КВ2** или **КА1**».

Любой **УЦ с разделенными компонентами,**
взаимодействующими через открытые сети,
как публичный, так и корпоративный.

Реализуемо?

Буква закона

Более **300 аккредитованных УЦ** =
признанных соответствующими требованиям ФЗ 63.

Ни одного сертифицированного средства УЦ класса КВ2 или КА1
(открытая выписка ЦЛСЗ из перечня СЗИ, сертифицированных ФСБ России по состоянию на 15 июня 2013 года).

Дух закона

Высокий класс сертифицированных средств связан с наличием информационного обмена через открытые каналы связи:

- взаимодействие физически разделенных компонент УЦ (напр. центры регистрации и центр сертификации)
- импорт данных в УЦ (запросы на сертификат)
- экспорт данных из УЦ (сведения о статусе сертификатов)

Защита взаимодействия компонент

- п 24.6 «в средствах УЦ должен быть реализован механизм защиты данных при передаче их между физически разделенными компонентами на основе использования СКЗИ».
- п. 33 «Для ограничения возможностей по построению каналов атак на средства УЦ с использованием каналов связи должны применяться средства межсетевого экранирования».

Криптошлюз класса КВ2 и межсетевой экран обеспечивают необходимый уровень защиты

Компания ИнфоТеКС предлагает

ViPNet Coordinator KB2

- сертифицированный криптошлюз (шифрование и имитозащита);
- сертифицированный межсетевой экран;
- без ограничений числа одновременных соединений;
- 2 варианта исполнения:
  - компактный **ViPNet Coordinator KB100 X2** (~ 25 Мбит/сек);
  - производительный **ViPNet Coordinator KB1000 Q2** (~ 200 Мбит/сек).

ViPNet Coordinator KB2

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-1920* от "*20*" *августа* 2012 г.

Действителен до "*20*" *августа* 2015 г.

Выдан открытому акционерному обществу «ИнфоТеКС».

Настоящий сертификат удостоверяет, что изделие **«Программно-аппаратный комплекс «ViPNet Координатор-КВ2»** (вариант исполнения 2: ПАК ViPNet Coordinator КВ1000 Q2) в составе согласно формуляру ФРКЕ.00028-02 30 01 ФО

соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94 и требованиям ФСБ России к средствам криптографической защиты информации класса КВ2 и может использоваться для криптографической защиты (шифрование и имитозащита данных, передаваемых в IP-пакетах по сети связи общего пользования) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных обществом с ограниченной ответственностью «Центр сертификационных исследований»
сертификационных испытаний образцов продукции №№ 587В-001001, 587В-001002.

Безопасность информации обеспечивается при использовании изделия, изготовленного в соответствии с техническими условиями ФРКЕ.00028-02 97 01 ТУ, выполнении требований нормативных документов формуляра ФРКЕ.00028-02 30 01 ФО и сохранении в тайне ключей шифрования.

Временно исполняющий обязанности
начальника Центра защиты информации
и специальной связи ФСБ России **А.С.Кузьмин**

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

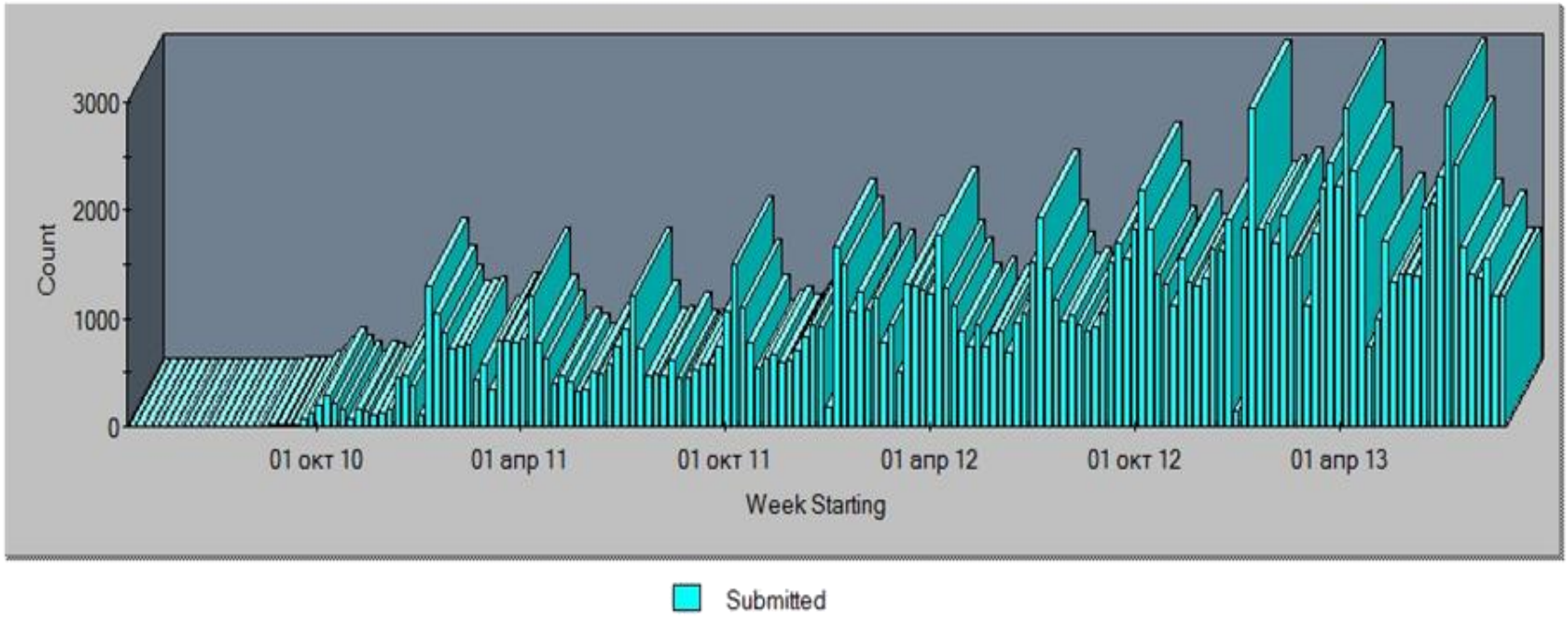
Заместитель начальника Центра по лицензированию,
сертификации и защите государственной тайны ФСБ России А.Н.Ковалев

Данные, поступающие в УЦ и экспортируемые из УЦ

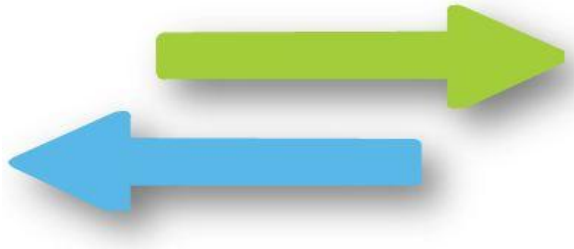
- **межсетевого экрана не достаточно –** требуется глубокая инспекция пакетов на прикладном уровне
- **криптошлюза не достаточно:**
  - второй участник взаимодействия не имеет средств защиты канала
  - сложное управление системой шифрованной связи
  - слишком большое число участников

Что доступно пользователям

109000 зарегистрированных копий **ViPNet CSP**



Данные, поступающие в УЦ и экспортируемые из УЦ



необходим **двунаправленный шлюз прикладной фильтрации** поступающих в УЦ из открытых сетей данных (с контролем ЭП согласно п. 24.3),

- запросы на сертификат/сведения о статусе;
- персональные данные пользователей;
- сертификаты и САС из других УЦ;
- квитанции о доставке данных;

и отправляемых в такие сети данных

- сертификаты пользователей;
- сведения о статусе сертификатов.

Сервер подписи как средство ЭП?

Аутентификация на сервере подписи

Приказ 796 пункт 23.6 (требования к идентификации и аутентификации для средств УЦ класса КВ1 и выше)

«при осуществлении удаленного доступа к средствам УЦ использование только символьного пароля не допускается, должны использоваться механизмы аутентификации на основе криптографических протоколов»

удаленная аутентификация пользователя при высоком уровне угрозы в канале связи **требует пользовательских криптографических средств**.

Замкнутый круг сервера подписи

Сервер подписи

Нет пользовательской криптографии

Пользовательская криптография

Криптографическая аутентификация пользователя

infotecs

Спасибо за внимание!
Вопросы?

Алексей Уривский
ОАО «ИнфоТеКС»
urivskiy@infotecs.ru