

IX ежегодная международная
конференция
«РКИ-ФОРУМ РОССИЯ 2011»

Доступные СКЗИ для электронных услуг

Алексей Уривский

руководитель научно-исследовательской группы

ОАО «ИнфоТеКС»

urivskiy@infotecs.ru

© 2011, ОАО «ИнфоТеКС».

**VIPNet**
Virtual Private Network

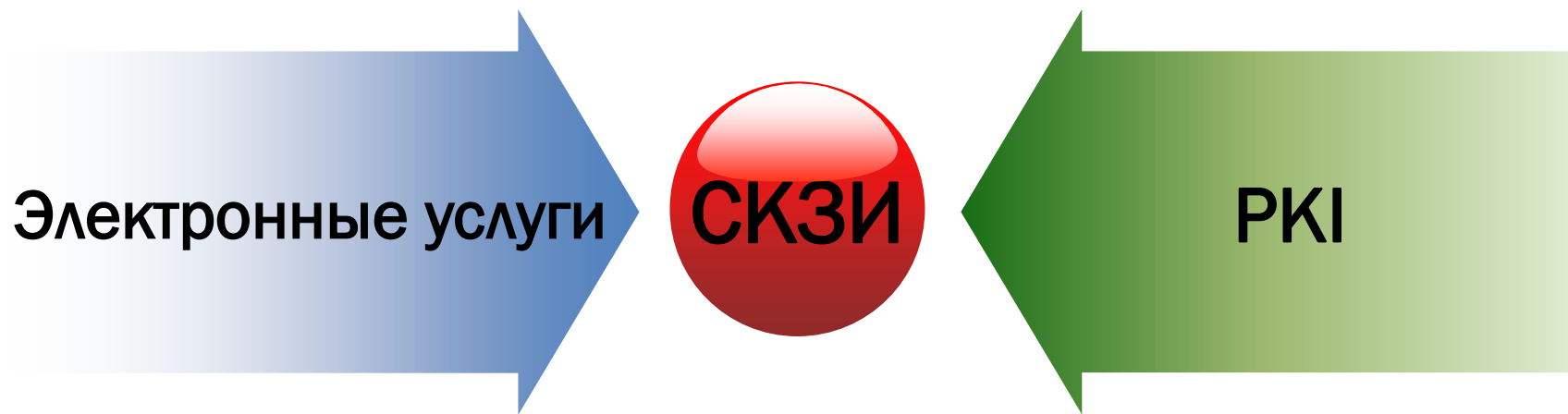
**infotecs**

Электронные услуги и СКЗИ

- ❑ Адресное предоставление услуг:
идентификация и аутентификация
 - ❑ потребитель
 - ❑ поставщик услуги / функции
- ❑ Защита каналов взаимодействия:
шифрование и имитозащита обмена
 - ❑ сети общего пользования
 - ❑ территориальная распределенность
- ❑ Юридическая значимость услуг:
электронная подпись
 - ❑ потребитель
 - ❑ поставщик



СКЗИ – основа безопасного электронного государства



Стоимость владения РКИ (точка зрения организатора)

❑ Системное ядро

- ❑ Лицензии на ПО
- ❑ Аппаратные средства
- ❑ Организационно-документальное обеспечение

❑ Пользователи

- ❑ Обслуживание и техподдержка пользователей
- ❑ Выпуск сертификатов
- ❑ Прикладное ПО
- ❑ **СКЗИ для пользователей**



Стоимость использования РКИ (точка зрения пользователя)

- Сертификат и его обслуживание
- Прикладное ПО
- СКЗИ



Практические аспекты и внешние факторы

- ❑ Стандартизация интерфейсов взаимодействия СКЗИ с прикладным ПО
- ❑ Стандартизация интерфейсов взаимодействия СКЗИ с ключевыми носителями и форматы хранения ключей
- ❑ Стандартизация СКЗИ по алгоритмам и протоколам
- ❑ Вопросы распространения СКЗИ
- ❑ Вопросы безопасного применения СКЗИ



Компания ИнфоТеКС предлагает



безвозмездную передачу права
на использование СКЗИ **ViPNet CSP**
конечным пользователям –
физическим лицам,
юридическим лицам и
государственным структурам

Коротко о ViPNet CSP

- ❑ **Реализация российских криптографических алгоритмов**
 - ГОСТ 28147-89
 - ГОСТ Р 34.10-2001, Р 34.11-94
- ❑ **Встраивание в прикладное ПО**
 - ❑ MS Crypto API
 - ❑ PKCS#11
- ❑ **Поддержка протоколов SSL/TLS**
- ❑ **Поддержка продуктов MS Office 2003, 2007, 2010**
- ❑ **Web-утилита создания запросов на сертификат PKCS#10**
- ❑ **Версии для Windows и Linux**



ViPNet CSP: сертификация и распространение



- ❑ Сертификат соответствия
ФСБ России СФ/124-1691
 - СКЗИ класса КС1/КС2
 - вычисление квалифицированной ЭП

- ❑ Согласованное с ФСБ
распространение: загрузка
с сайта производителя
www.infotecs.ru

- ❑ Нотификация Таможенного
союза RU0000005976



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-1691 от "17" июня 2011 г.

Действителен до "17" июня 2014 г.

Выдан _____ открытому акционерному обществу «ИнфоТеКс».

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) «ViPNet CSP», версия 3.2 (варианты исполнения 1, 2, 3) в составе согласно формуляру ФРКЕ.00061-01 30 01 ФО _____

соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 и требованиям ФСБ России к СКЗИ класса КС1 (для варианта исполнения 1) и класса КС2 (для вариантов исполнения 2, 3) и может использоваться для криптографической защиты (генерация и управление ключевой информацией, шифрование данных, содержащихся в областях оперативной памяти, вычисление инверсии для данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти, вычисление квалифицированной электронной подписи для данных, содержащихся в областях оперативной памяти, защита TLS-соединений) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных обществом с ограниченной ответственностью «Центр сертификационных исследований» сертификационных испытаний образца продукции № 637-001001.

Безопасность информации обеспечивается при использовании СКЗИ в соответствии с требованиями нормативных документов формуляра ФРКЕ.00061-01 30 01 ФО и сохранении в тайне ключей шифрования и закрытых ключей квалифицированной электронной подписи.

Заместитель руководителя Научно-технической
службы – начальник Центра защиты информации
и специальной связи ФСБ России



А.Е.Андреечкин

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию,
сертификации и защите государственной тайны ФСБ России



А.Н.Ковалев



ViPNet CSP: совместимость

Совместим с сертифицированными ключевыми носителями PKCS#11

- eToken ГОСТ
(сертификат совместимости)
- ruToken ECP
(сертификат готовится)



Совместим с Windows 7

Аладдин РД

infotecs

СЕРТИФИКАТ СОВМЕСТИМОСТИ

электронных ключей eToken ГОСТ и программного обеспечения ViPNet CSP

от 26.07.2011

г. Москва

Настоящим сертификатом компании ЗАО «Аладдин РД» и ОАО «ИнфоТекС» подтверждают корректность работы электронных ключей eToken ГОСТ производства компании ЗАО «Аладдин РД» с ПО ViPNet CSP версии 3.2.

Электронные ключи eToken ГОСТ сертифицированы ФСБ России по требованиям к СКЗИ класса КС1 и КС2 и могут использоваться для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну (сертификат соответствия № СФ/124-1671 от 11 мая 2011 г.).

Программное обеспечение ViPNet CSP версии 3.2 сертифицировано ФСБ России по требованиям к СКЗИ класса КС1 и КС2 и может использоваться для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну (сертификат соответствия № СФ/124-1691 от 17 июня 2011 г.).

ПО ViPNet CSP позволяет создать на устройстве eToken ГОСТ квалифицированную электронную подпись с использованием аппаратного СКЗИ электронного ключа.

Удостоверение сертификата электронной подписи проводилось в Удостоверяющем Центре КриптоПро и Удостоверяющем Центре ViPNet.

Настоящий сертификат выдан на основании результатов испытаний, проведенных компаниями ЗАО «Аладдин РД» и ОАО «ИнфоТекС». Таблица совместимости различных типов электронных ключей eToken ГОСТ с ПО ViPNet CSP версии 3.2 приведена в Приложении №1.

Генеральный директор

ЗАО «Аладдин РД»



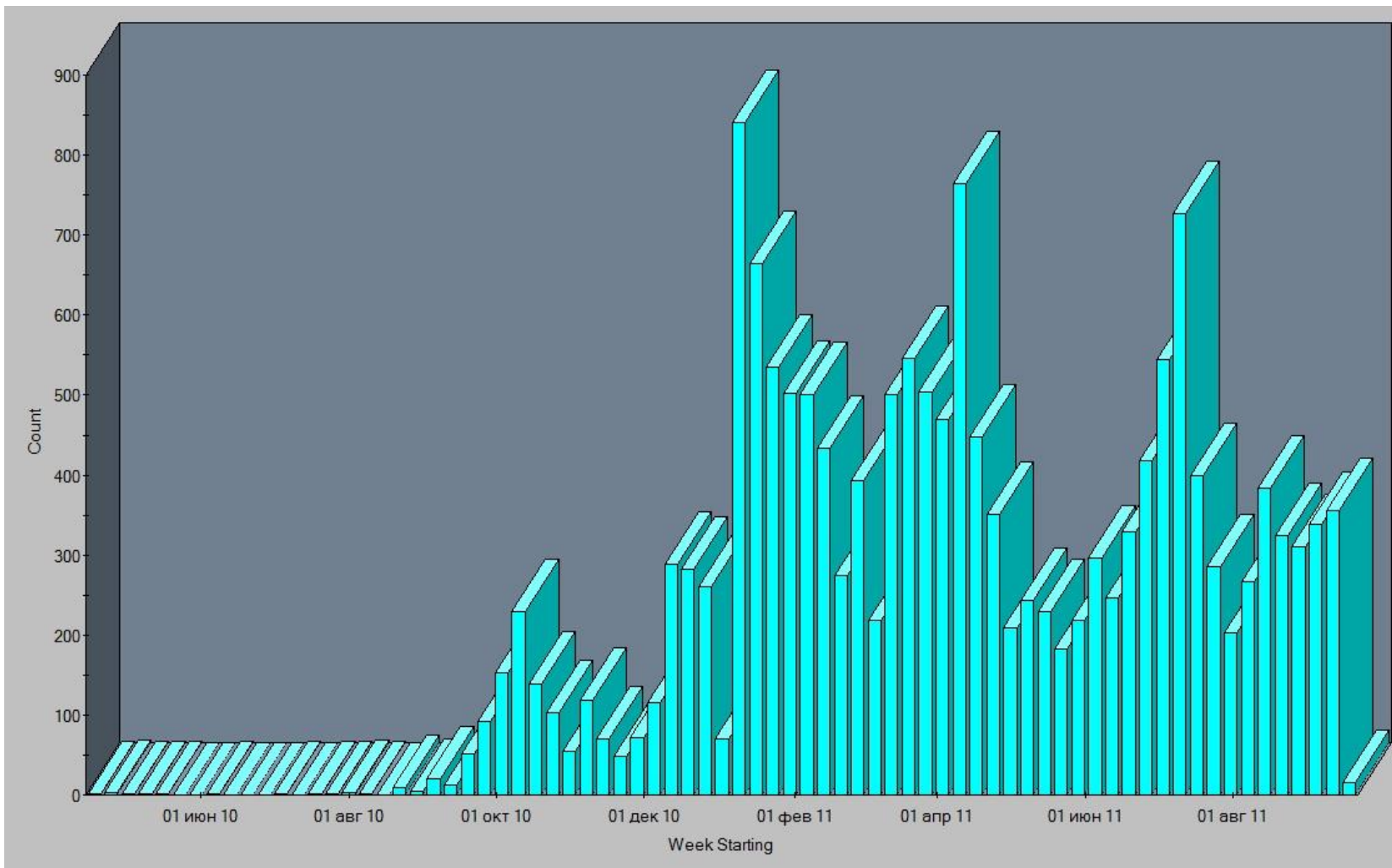
Генеральный директор


ОАО «ИнфоТекС»





ViPNet CSP: статистика регистрации





IX ежегодная международная
конференция
«РКІ-ФОРУМ РОССИЯ 2011»

Спасибо за внимание! Вопросы?

Алексей Уривский

руководитель научно-исследовательской группы

ОАО «ИнфоТеКС»

urivskiy@infotecs.ru

© 2011, ОАО «ИнфоТеКС».

**VIPNet**
Virtual Private Network

**infotecs**