

# Практика создания удостоверяющих центров кредитно-финансовых организаций

Ростислав Рыжков,  
**ОАО «ЭЛВИС-ПЛЮС»**

---

Москва, 2008 г.

## ЭЛВИС-Плюс – системный интегратор в сфере информационной безопасности и разработчик продуктового ряда «Застава»



The Security Division of EMC



CHECK POINT  
Software Technologies Ltd.



Юротория  
КА(ПЕР(КОГО



Профессиональный консалтинг в области построения информационных систем с обеспечением информационной безопасности

Комплексное обследование защищенности ИС, анализ угроз безопасности информации

От разработки Политики ИБ до сдачи в эксплуатацию ЗИС

Аттестация ИС на соответствие требованиям по защите информации



# Сертификаты, лицензии и награды

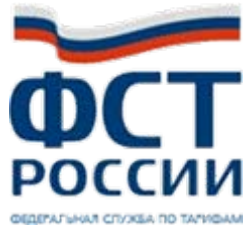
У компании имеются все необходимые лицензии и сертификаты, позволяющие осуществлять деятельность в области защиты информации



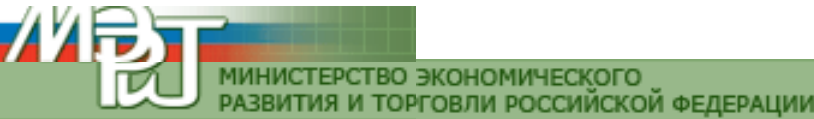
Деятельность компании отмечена рядом профессиональных наград и дипломов



РОССИЙСКИЙ  
СОЮЗ  
АВТОСТРАХОВЩИКОВ



ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО  
«РОССИЙСКИЕ ЖЕЛЕЗНЫЕ ДОРОГИ»



ФЕДЕРАЛЬНАЯ СЛУЖБА  
ГОСУДАРСТВЕННОЙ СТАТИСТИКИ



## УЦ и ИОК

### Состав ИОК:

#### • Удостоверяющий Центр (Центры):

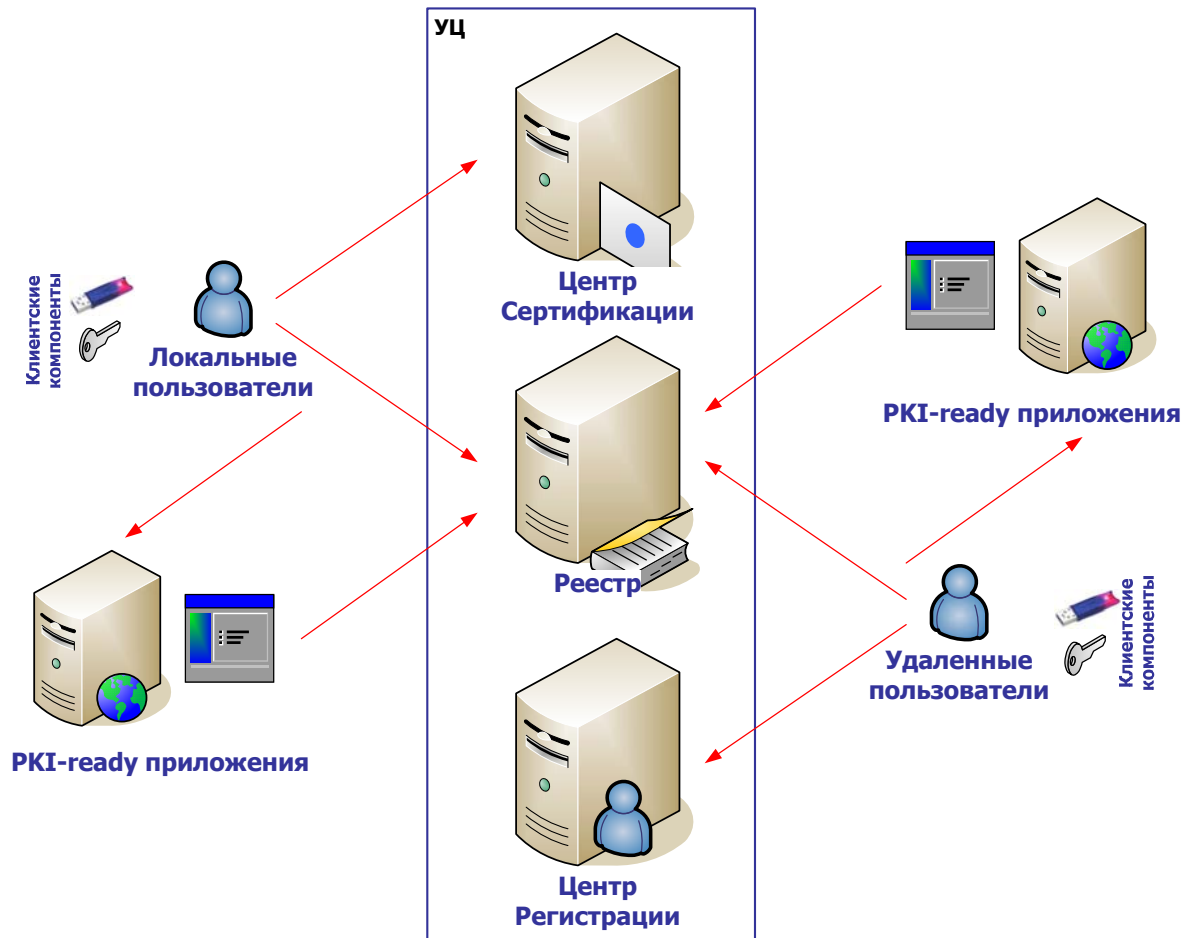
- Центр(ы) Сертификации

- Центр(ы) Регистрации

- Реестр сертификатов и CRL

- PKI-ready приложения

- Носители ключей и клиентские компоненты



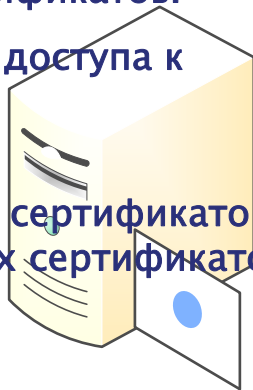
## Текущее использование в банках и финансовых организациях

- Шифрование и ЭЦП электронной почты
  - ЭЦП документов, юридически значимый электронный документооборот
  - ЭЦП в электронном архиве документов
- 
- Аутентификация в домене Active Directory на базе цифрового сертификата
  - Аутентификация при доступе к корпоративному portalу
  - Удаленный защищенный доступ, защищенный обмен данными не только внутри КИС, но и с внешними партнерами
  - Интеграция с системами физической безопасности доступа (при использовании смарт-карт или USB-токенов с RFID-метками)
  - Аутентификация во всех корпоративных приложениях - единое средство аутентификации (Single Sign-On)

## Функции Удостоверяющего Центра

### Центр Сертификации

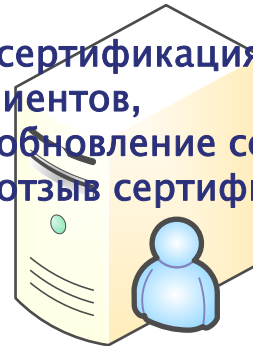
- Генерация и регистрация и ключей клиентов
- Хранение ключей СА и операции с ними:
  - сертификация ключей клиентов,
  - кросс-сертификация с другими УЦ,
  - сертификация подчиненных узлов,
  - обновление сертификатов,
  - отзыв сертификатов.
- Предоставление доступа к операциям с ключами СА
- Ведение реестра сертификатов и списка отозванных сертификатов (CRL)



### Центр регистрации

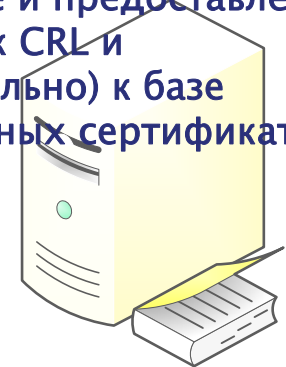
- Генерация и регистрация и ключей клиентов
- Операции с ключами СА через ЦС:

- сертификация ключей клиентов,
- обновление сертификатов,
- отзыв сертификатов.



### Реестр

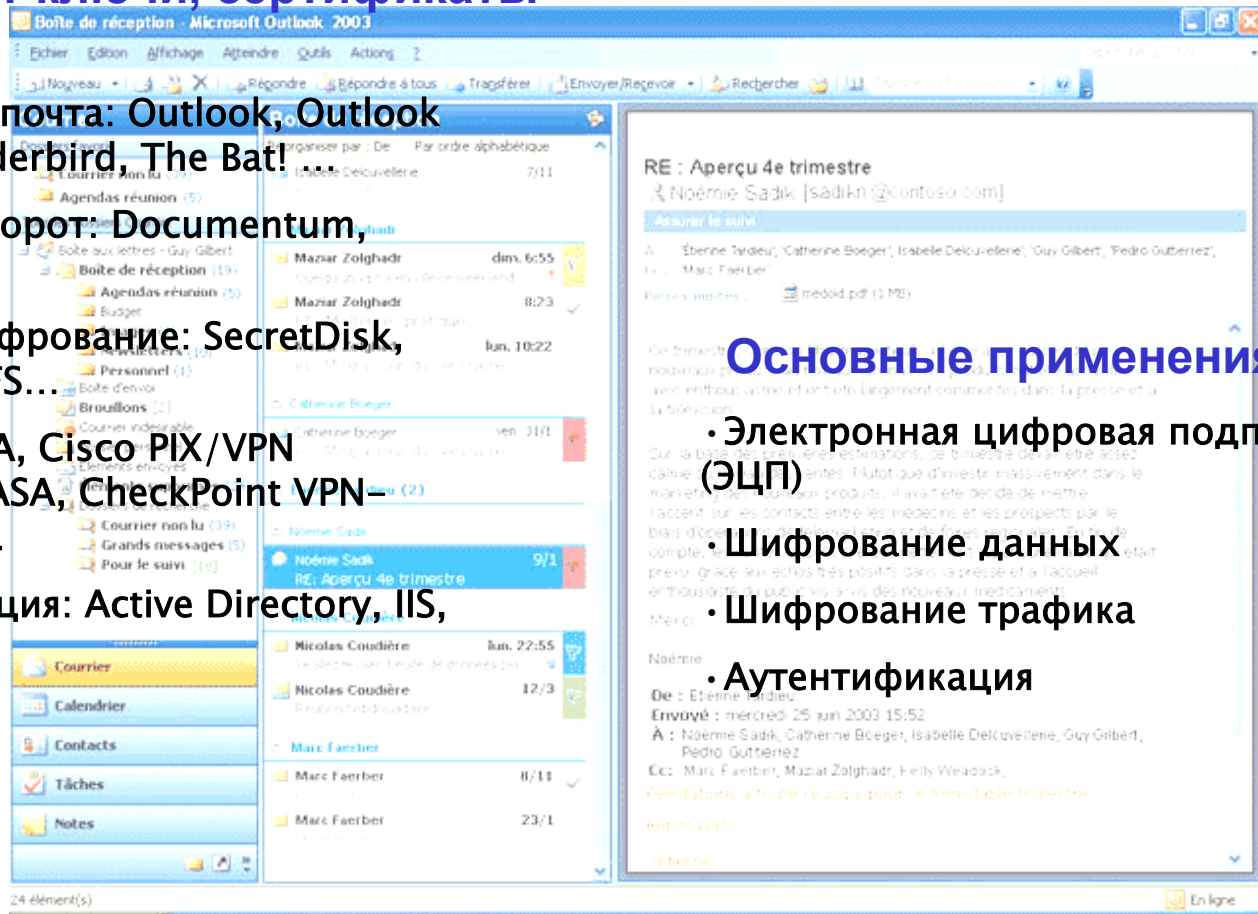
Хранение и предоставление доступа к CRL и (опционально) к базе выпущенных сертификатов



## PKI-ready приложения

### Используют ключи, сертификаты и CRL:

- Электронная почта: Outlook, Outlook Express, Thunderbird, The Bat!
- Документооборот: Documentum, LANDocs...
- Файловое шифрование: SecretDisk, КристоАРМ, EFS...
- VPN: ЗАСТАВА, Cisco PIX/VPN Concentrator/ASA, CheckPoint VPN-1/Connectrix...
- Аутентификация: Active Directory, IIS, Apache...



### Основные применения:

- Электронная цифровая подпись (ЭЦП)
- Шифрование данных
- Шифрование трафика
- Аутентификация

## Федеральный Закон № 152-ФЗ «О персональных данных»

**Оператор обязан принимать** организационные и технические **меры**, для защиты ПД от НСД, уничтожения, изменения, блокирования, копирования, распространения и иных **неправомерных действий** (ст. 19, ч. 1)

**Правительство РФ устанавливает требования** к обеспечению безопасности ПД при их обработке (ст. 19, ч. 2)

**Требования должны быть выполнены до 1.01.2010 г.** (ст. 25)

**Федеральные органы** в области обеспечения безопасности и ПД ИТР и ТЗИ (ФСБ России и ФСТЭК России) **осуществляют контроль и надзор**

**Лица**, виновные в нарушении требований **несут** гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ **ответственность**

### Установлены категории ПД:

- ✓ **категория 1** - ПД, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни
- ✓ **категория 2** - ПД, позволяющие *идентифицировать субъекта ПД и получить о нем дополнительную информацию, за исключением ПД, относящихся к категории 1*
- ✓ **категория 3** - персональные данные, позволяющие идентифицировать субъекта ПД
- ✓ **категория 4** - обезличенные и (или) общедоступные ПД.

Пункт 6 Приказа №55/86/20

## Классификация ИС персональных данных

В зависимости от последствий нарушений безопасности ПД, типовой ИС присваивается один из классов:

- ✓ **класс 1 (К1)** - ИС, для которых нарушения могут привести к **значительным негативным последствиям** для субъектов ПД;
- ✓ **класс 2 (К2)** - ИС, для которых нарушения могут привести к **негативным последствиям** для субъектов ПД;
- ✓ **класс 3 (К3)** - ИС, для которых нарушения могут привести к **незначительным негативным последствиям** для субъектов ПД;
- ✓ **класс 4 (К4)** - ИС, для которых нарушения **не приводят к негативным последствиям** для субъектов ПД.

*Пункт 14 Приказа №55/86/20*

Класс **типовой ИС** выбирается по таблице:

Количество субъектов Категории ПД	<1000	1000 – 100 000	> 100 000
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

Класс **специальной ИС** определяется на основе **модели угроз**

## Оператор персональных данных обязан:

- уведомить Россвязьохранкультуру до начала обработки ПД
- принять организационные и технические меры для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения
- провести классификацию ИС ПД с оформлением акта
- до 1.01.2010 г. создать СОБИ и реализовать комплекс мер по защите ПД
- провести оценку соответствия ИС ПД требованиям безопасности
- получить лицензию на деятельность по технической защите конфиденциальной информации (для ИС 1 и 2 класса)

## УЦ и ИОК в защите персональных данных

Цифровые ключи и сертификаты используются для решения задач:

- Противодействие хищениям баз и хранилищ данных
- Шифрование и ЭЦП электронной почты
- ЭЦП документов, юридически значимый электронный документооборот и архив
- Строгая многофакторная аутентификация с использованием цифровых сертификатов
- Удаленный защищенный доступ

# Опыт компании – УЦ и ИОК

## Создание УЦ

- СО «ЦДУ ЕЭС»
- ОАО «КАМАЗ»
- ГК ПИК
- УЦ Электроэнергетики
- ОАО «СОГАЗ»
- УЦ ХМАО (Комитет по информационным ресурсам)
- Казкоммерцбанк

## Работы в существующих УЦ

- Аудит нормативно-правового обеспечения безопасности информации УЦ «Недвижимость»
- Аудит и аттестация УЦ Правительства г. Санкт-Петербург
- Модернизация ИС РУЦ ЯНАО
- Настройка УЦ ЛукОйл-ИНФОРМ

## Пользоваться услугами стороннего УЦ или создавать свой?

- «Политические» факторы
- Экономика. Планируете использовать более 1000 сертификатов?
- Организационные аспекты. Иерархия УЦ, доверительные отношения

# Основные статьи затрат и возможных выгод при создании собственного УЦ

## Статьи затрат

- Единовременные
  - Аппаратное и программное обеспечение
  - Обучение сотрудников
  - Предпроектные и пуско-наладочные работы
  - Разработка пакета документов
- Ежегодные
  - Зарплата администраторов
  - Обучение администраторов
  - Сопровождение программного и аппаратного обеспечения
  - Накладные расходы (200-500% от заработной платы)

## Выгоды

- Нет необходимости закупать и восстанавливать сертификаты при:
  - компрометации (5-10% от общего числа)
  - приеме на работу новых сотрудников
  - плановом обновлении
- Возможность оказывать услуги сторонним организациям на коммерческой основе

## Используемые продукты и их производители

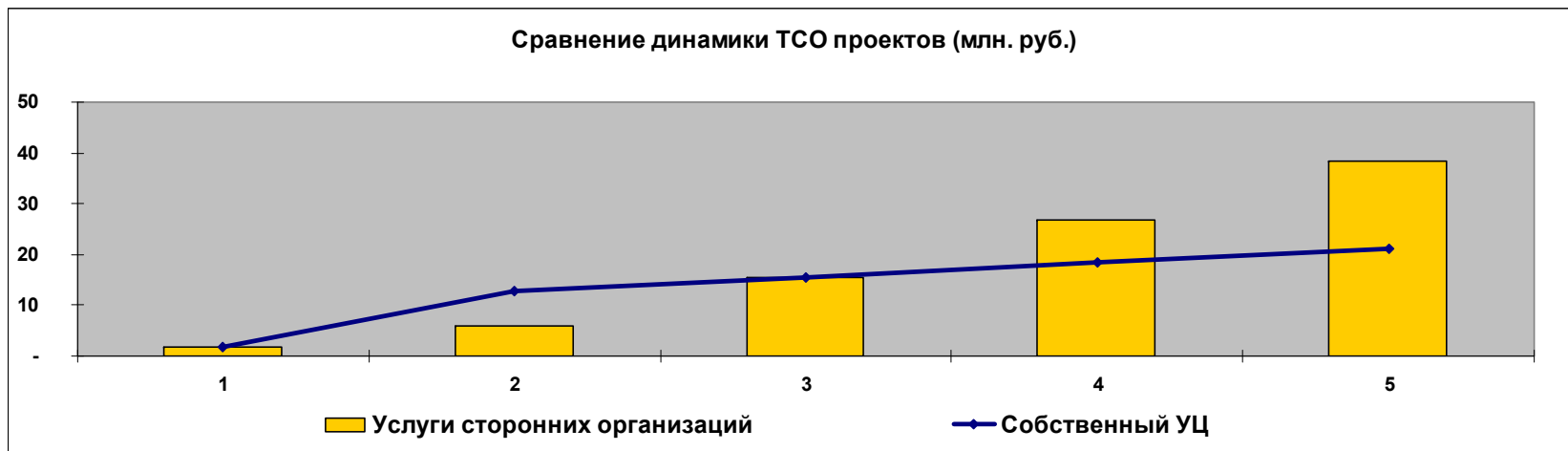
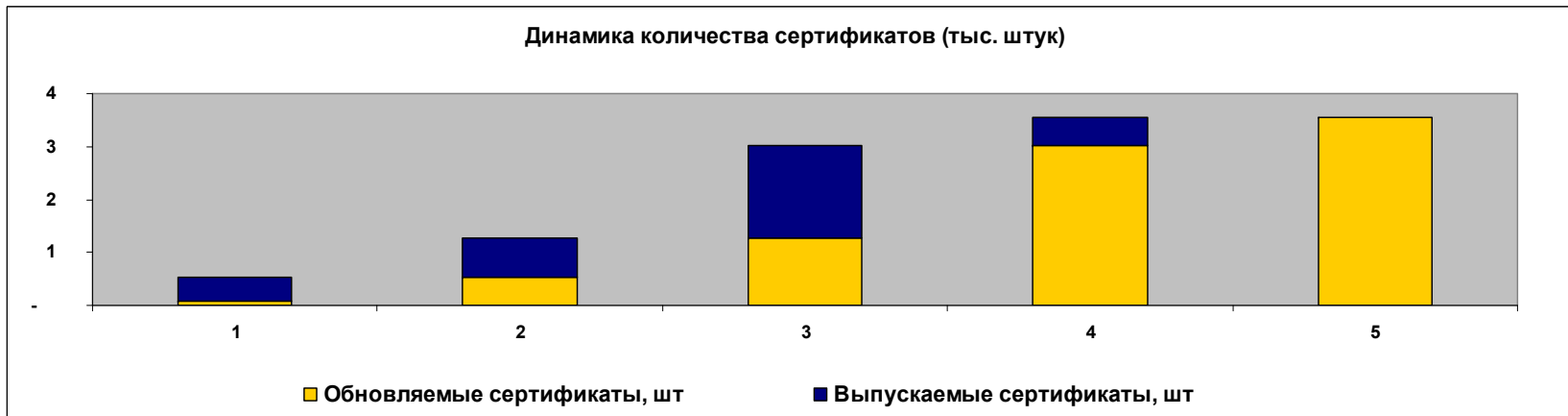
Отечественные :

- "КриптоПро УЦ" (ООО "Крипто-Про");
- "УЦ ViPNet" (ОАО "Инфотекс");
- "Юнисерт-ГОСТ" (ЗАО "НИП "Информзащита");
- "Стандарт УЦ" (ФГУП "НТЦ "Атлас");
- "Изделие Кеон УЦ" (совместной разработки ООО "Компания Демос" и ОАО "Элвис-плюс");
- "VCERT MV" (совместной разработки ЗАО "МО ПНИЭИ" и ООО "Валидата");
- "Верба УЦ" (ФГУП ПНИЭИ);
- "УЦ КИ" (ФГУ РНЦ "Курчатовский институт").

Среди зарубежных PKI-продуктов наиболее популярны на нашем рынке:

- Baltimore Technologies - продукт- UniCERT;
- Entrust – продукт -Entrust Authority;
- Microsoft – продукт-Microsoft Advanced Server;
- RSA Security - продукт - RSA Keon.

# Экономическая целесообразность создания собственного УЦ



## Экономические показатели. Два примера

Первоначальные вложения в УЦ (от 3 до 5 тысяч клиентов ):

- Ввод системы в эксплуатацию 90-150 тыс. долл. США -;
- Накладные расходы и заработная плата специалистов 50-100 тыс. долл. США в год
- Стоимость выдачи сертификата 50-60 долл. США
- Стоимость сопровождения сертификата 20-30 долл. США в год,

Затраты на организацию УЦ должны окупиться в течение первого года эксплуатации

Создание собственного УЦ в территориально-распределенной структуре окупается:

- При обслуживании 4 тысяч сертификатов - за 1,5-2,5 года
- При обслуживании 2-3 тысяч сертификатов за 3 года

Ваши вопросы ?  
Спасибо за внимание!

E-mail: [RRyshkov@elvis.ru](mailto:RRyshkov@elvis.ru),  
Тел.: 777-42-90, а также  
531-8863, 531-1622, 531- 4633