ПРОГРАММНО–
ТЕХНИЧЕСКИЕ
КОМПЛЕКСЫ

А.О. МЕЛАЩЕНКО, О.Л. ПЕРЕВОЗЧИКОВА

УДК 681.3:002.651.028(083.73)

НАЦИОНАЛЬНАЯ СИСТЕМА ЭЛЕКТРОННЫХ ЦИФРОВЫХ ПОДПИСЕЙ КАК ОТКРЫТАЯ СИСТЕМА

Ключевые слова: *электронная цифровая подпись, интероперабельность, гармонизация стандартов, криптографический алгоритм (криптоалгоритм), валидация, верификация, политика подписания, тестовый стенд.*

ВВЕДЕНИЕ

Электронная цифровая подпись (ЭЦП) является «якорем» доверия большинства электронных бизнесов (eGoverment, eCommerce, eProcrument, eHealth, eInvoicing …). Юридическую правомочность ЭЦП в Украине гарантирует Закон Украины об электронной цифровой подписи № 852 [1], а технологически и организационно поддерживает Национальная система электронных цифровых подписей (НСЭЦП).

В настоящее время НСЭЦП не имеет внутренней интероперабельности ввиду архаичной законодательно-нормативной базы, неквалифицированно регламентирующей ее функционирование. В статье обсуждены методы достижения внутренней и внешней интероперабельности НСЭЦП как открытой системы.

СОСТОЯНИЕ НСЭЦП

Подходы «кусочно-непрерывного» регулирования (рис. 1), задействованные в НСЭЦП, привели к недееспособности задействованных норм и правил решения неотложных вопросов электронного бизнеса.

1. Де-факто НСЭЦП допускает единственный комплект подписей ДСТУ 4145 + ГОСТ 34.311, не имеющий интероперабельных реализаций криптомодулей.

2. Основной документ, регламентирующий требования к сертификату открытых ключей (Совместный приказ № 99/166 от 11.09.06 [2]), содержит множество сугубо программистских ошибок, что не позволяет однозначно реализовать его требования.

3. В Украине реализован простейший неинтероперабельный вариант ЭЦП, не допускающий параллельные и/или контрподписи, т.е. исключающий построение электронного документооборота полноценных бизнес-процессов.

4. При аккредитации не задействованы формализованные процедуры оценки интероперабельности программно-технических комплексов (ПТК) центров сертификации ключей (ЦСК).

Рис. 1. Схема правовой базы НСЭЦП Украины

НСЭЦП также лишена внешней интероперабельности (рис. 2) ввиду задействования единственного локального алгоритма подписания, регламентированного негармонизированным стандартом ДСТУ 4145. Не отвечая международным признанным криптоалгоритмам, НСЭЦП не готова к трансграничному признанию сертификатов ключей, выданных за пределами Украины, т.е. неспособна к кроссертификации с любым государством, даже с Россией, которая уже вывела свои стандарты криптоалгоритмов на международный уровень.

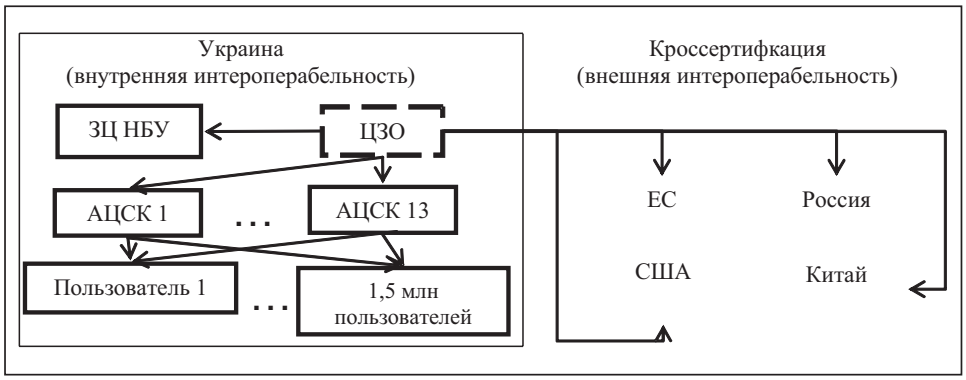

Рис. 2. Схема поддержки интероперабельности НСЭЦП

НСЭЦП функционирует согласно Закону Украины № 852 [1], реализовавшего положения Директивы 1999/93/ЕС (далее Директива). В ЕС организационная и технологическая поддержка бизнес-процессов воплощена в квалифицированной инфраструктуре открытых ключей (QPKI). В [3] описана эталонная модель QPKI и идентифицированы ключевые проблемы НСЭЦП посредством сопоставления НСЭЦП с эталонной моделью QPKI.

С юридической точки зрения Директива однозначно «вписывает» нормы закона в конкретные требования и компоненты ИТ. В ЕС это называют «новым подходом», обеспечивающим установление нарушений положений законов через нарушения конкретных норм или требований стандартов, и наоборот. Важность такой двухсторонней связи обусловлена необходимостью однозначной реализации описанных в законе бизнес-процессов с применением формально-алгоритмических инструментов в реализации любой ИТ в целом или ее отдельных компонентов.

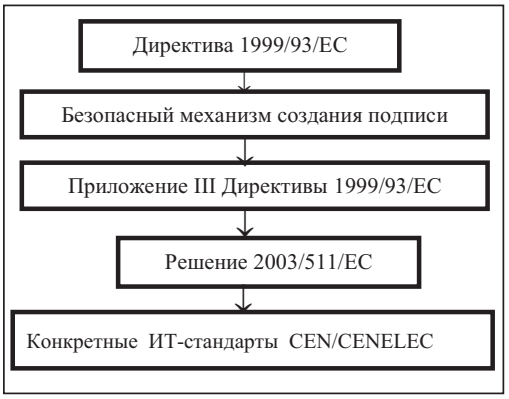

Рис. 3. Схема механизма описания нормы Директивы

Воплощение «нового подхода» (рис. 3) демонстрирует, например, регламентация требований к «безопасному механизму создания подписи». Это понятие определено как «…механизм создания подписи, отвечающий требованиям, изложенным в Приложении III Директивы… Статья 10 (Приложение III). Комитет уточняет требования, предусмотренные в Приложениях к Директиве, указанные в статье 3(4) критерии и общепризнанные стандарты продукции электронных подписей, установленные и опубликованные в соответствии со статьей 3(5) по процедуре, предусмотренной в статье 9(2).»

Как отрытая система НСЭЦП допускает взаимодействие всех субъектов (государства, бизнеса и граждан), обладая четырьмя свойствами:

1) интероперабельность — способность к взаимодействию или функциональной совместимости всех компонентов ПТК всех ЦСК — достигается через четвертое свойство;

2) мобильность — достигается задействованием стандартных нотаций в описании базовых объектов (в данном случае ASN.1-нотаций и XSD-схем XML-документов);

3) масштабируемость — достигается стандартизацией интерфейсов ПТК;

4) стандартизация всех объектов и процессов обслуживания ЭЦП.

Качество услуг НСЭЦП. Рассмотрим влияние на НСЭЦП как открытую систему разработки Технического регламента НСЭЦП согласно Закону Украины № 3164 [4]. Оформленный как законодательный акт Технический регламент обязует всех участников НСЭЦП выполнять требования и нормы стандартов. В настоящее время гармонизировано свыше 50-ти ДСТУ (рис. 4), необходимо разработать еще 37 для стандартизации всех компонентов НСЭЦП.

В основе иерархии субъектов НСЭЦП находится центральный удостоверяющий орган ЦЗО, проводящий аккредитацию ЦСК и технический надзор за АЦСК, что в полной мере отвечает процедурам оценки соответствия серии ISO 9000. Технический регламент НСЭЦП сводит в целостный комплекс нормы, правила, эталоны, образцы и требования, а соответствие им конкретных продуктов устанавливают независимые и компетентные оценщики. Полное соответствие процедур QPKI стандартам ISO 9000 имеет особую ценность, поскольку от имени государства ЦЗО гарантирует всемирно признанными методами качество услуг ЭЦП.

Процедуры оценки соответствия поддержаны двумя условиями (рис. 5):

1) модульность разработки — оцениваются не только ПТК в целом, но и их компоненты, выполняющие конкретные функции А(ЦСК), например компоненты штемпелевания времени или обработки сертификатов открытых ключей. Тогда могут конкурировать не только ПТК, но и их компоненты, и можно независимо развивать разные аспекты НСЭЦП;

2) инфраструктура аккредитованных независимых и компетентных оценщиков, выдающих сертификаты соответствия на компоненты и/или ПТК в целом и выполняющих требования компетентности (обладают достаточной квалификацией для оценки соответствия) и независимости (непосредственно не

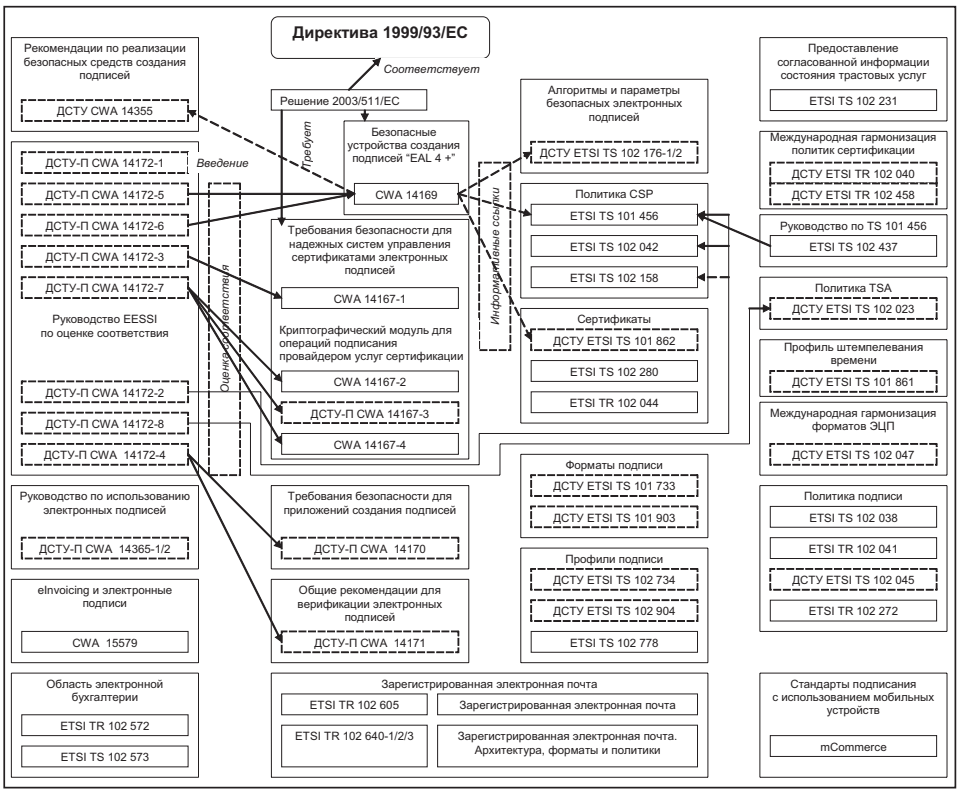

Рис. 4. Схема состояния гармонизации стандартов для интероперабельности НСЭЦП

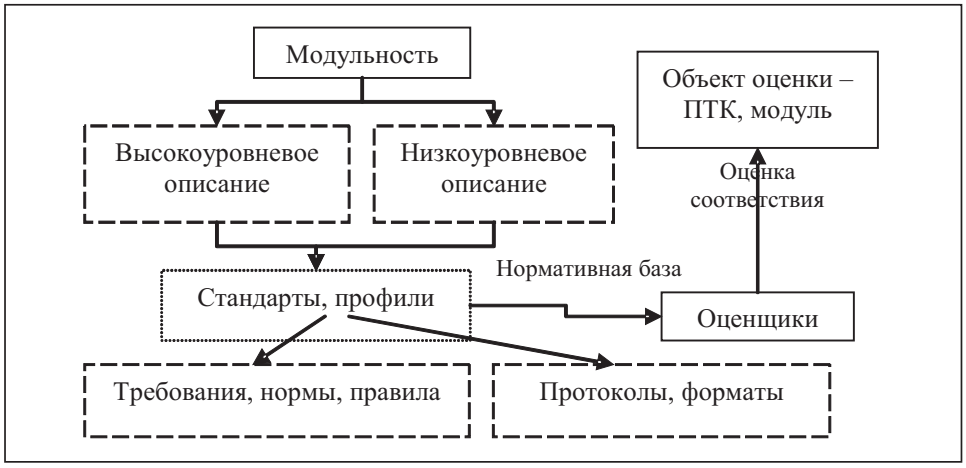

Рис. 5. Схема принципов QPKI

связаны с разработкой любых компонентов ПТК).

В Украине нарушен принцип независимости оценщиков, поскольку де-факто технический надзор проводит контролирующий орган, причем через нормативно неурегулированный механизм «позитивных экспертных заключений». В настоящее время этот орган обслуживает ПТК ЦЗО.

Целесообразно рассматривать НСЭЦП во взаимодействии трех сущностей или ключевых объектов QPKI (рис. 6):

1) политика подписания как набор правил для создания и валидации ЭЦП; когда ЭЦП считают валидной в конкретном контексте транзакций электронного бизнеса;

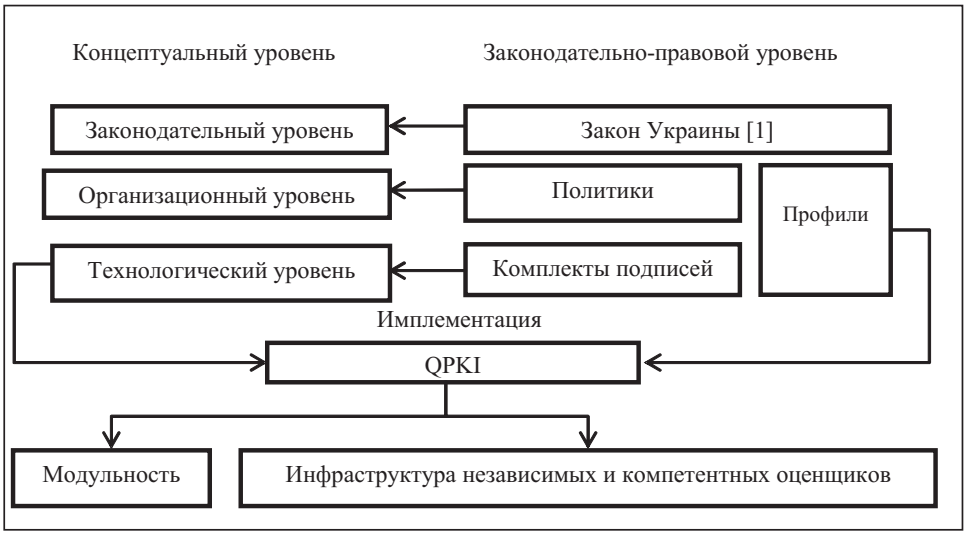

Рис. 6. Схема сущности QPKI

2) комплект подписи как сущность состоит из алгоритма подписания, хеш-функции и алгоритма дополнения; цель создания комплекта подписей — гарантия эквивалентного уровня доверия к хеш-функции и алгоритму подписания;

3) профиль задает единый набор применимых опций.

КОМПЛЕКТЫ ПОДПИСЕЙ

Математические выкладки алгоритма подписания ДСТУ 4145 составляют необходимое, но недостаточное условие реализации интероперабельных криптомодулей. Достаточное условие — выверенная реализация математических алгоритмов в гетерогенной сетевой среде разных ОС (Linux и Windows с учетом их версий, чем обусловлена специфика конфигурирования с дополнительными API), применение схем кодирования (BER, DER, CER, XER), профилей, генераторов случайных чисел и т.п. Отметим «качество» эмулирования арифметики сверхбольших чисел на разрядной сетке, в десятки раз превышающей традиционную разрядность компьютеров.

Интероперабельности комплекта подписей ДСТУ 4145 + ГОСТ 34.311 можно достичь, задействовав пока отсутствующий профиль этого комплекта. Тогда для однозначного представления параметров алгоритма в сертификате открытого ключа необходимы тип и схема кодирования параметров. К профилю параметров ДСТУ 4145 относятся:

— значение хеш-функции данных, для которых вычисляется ЭЦП, заданное ASN.1 типом OCTET STRING со схемой кодирования Big Endian;

— ЭЦП, заданная ASN.1 типом BIT STRING со схемой кодирования Big Endian;

— личный и открытый ключи, заданные ASN.1 типом OCTET STRING;

— общие параметры, закодированные согласно п. 1.3.11 [2];

— таблица заполнения узлов замены блоков подстановки, закодированная ASN.1 типом OCTET STRING.

К профилю параметров хеш-функции ГОСТ 34.311-95, заданных ASN.1 типом OCTET STRING со схемой кодирования Big Endian, в общем случае относятся:

— входной текст, подлежащий хешированию;

— значение хеш-функции;

— ключевые данные (в том числе таблица заполнения узлов замены блоков подстановки);

— стартовый вектор хеширования.

Использование комплектов подписей в рамках НСЭЦП требует постоянной поддержки их работоспособности в гетерогенной среде, которая изменяется каждые 15–18 месяцев. НСЭЦП подразумевает гарантии того, что через десятки лет можно доказать юридическую правомочность электронного документа. Проанализируем возможность «сворачивания» действующего в НСЭЦП комплекта подписи ДСТУ 4145 + ГОСТ 34.311 к всемирно признанным комплектам.

Уникальный криптоалгоритм ДСТУ 4145, разработанный в конце 1990-х годов как первый NP-полный алгоритм, использует эллиптические кривые над расширенным полем Галуа $GF(2m)$, а немецкий криптоалгоритм ECGDSA — над $GF(p)$, где p — простое целое.

Группа точек эллиптической кривой определена над конечным полем. Групповая операция довольно проста, но это верно только для эллиптических кривых, определенных над конечным полем характеристики 2, а использование GF(p) для достаточно большого p не дает преимуществ криптостойкости алгоритму, поэтому целесообразнее применение эллиптических кривых над $GF(2m)$ по сравнению с применимыми в ДСТУ 4145.

Если кривая определена над конечным полем GF($2m$), то алгебраически замкнутое поле, содержащее все точки эллиптической кривой, объединяет все расширения этого конечного поля, т.е. $\overline{K} = \bigcup_{k \geq 1} GF(2^{km})$. Когда коэффициенты уравнения эллиптической кривой принадлежат основному полю, она содержит бесконечное число точек, а криптоалгоритмы строятся на конечной кривой, координаты точек которой принадлежат основному полю. Так достигается сложность полного перебора на актуальной бесконечности.

ПОЛИТИКА ПОДПИСАНИЯ

В бумажном мире в зависимости от должности подписанта и места подписания можно установить семантику подписи как визу, ознакомление либо принятие обязательства. Относительно электронного документа такая возможность исключена, а политика подписания, отражая семантику конкретной ЭЦП, пока слабо стандартизирована. Имеем составляющие политики подписания SignaturePolicy (рис. 7):

— базовые свойства (Core Properties), без которых невозможна публикация политики подписания;

— базовые правила (Core Rules) задают базовые критерии, выполнение которых гарантирует валидность подписи;

— правила уровня транзакции (Transaction Context Rules) задают базовые критерии, идентифицирующие фиксацию транзакции.

Конкретная спецификация базовых правил и правил уровня транзакции зависит от контекста использования политики подписания. Для представления спецификаций политики целесообразен язык OWL [3].

Формальная методика аккредитации ЦСК необходима для оценки уровня интероперабельности ПТК и его компонентов. Но, к сожалению, экспертная комиссия ЦЗО по аккредитации проверяет только компетентность персонала зарегистрированных ЦСК, не оценивая функциональность и работоспособность ПТК.

В Евросоюзе процедура оценки соответствия максимально формализована согласно системе стандартов ISO 9000 и выполняется он-лайн по Интернету. Такая методика аккредитации ЦСК также необходима для доверия иностранных

партнеров ЦЗО. Кроме экспертных оценок, в основном информации из документов ЦСК, такую методику целесообразно поддержать специальным тестовым стендом для выполнения требований разд. IV Закона Украины № 3164 [4].

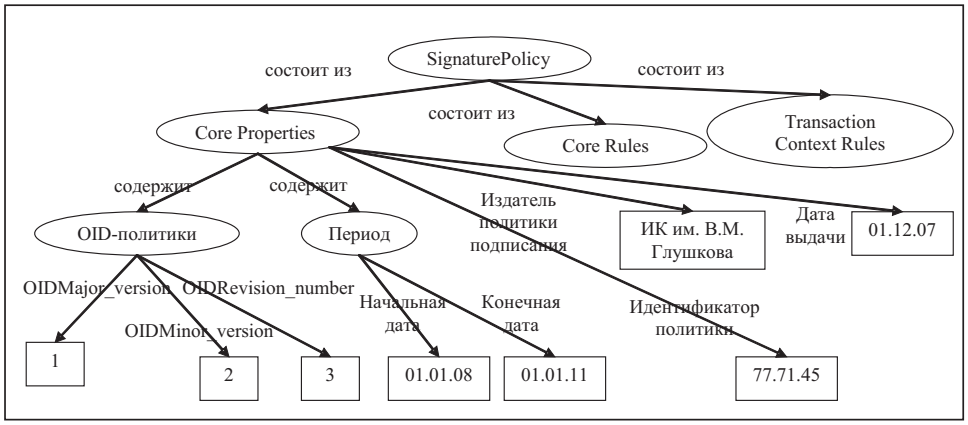

Рис. 7. Схема иерархии сущности политики подписания

О важности процедур оценки соответствия для организации НСЭЦП впервые в Украине заговорили в 2004 г. [5]. Правда, с тех пор из-за отсутствия полноценного электронного документооборота в Украине мало изменились нормативно-правовая и организационно-технологическая базы НСЭЦП.

В рамках построенного прототипа тестового стенда [3] для оценки соответствия ПТК эталонной модели QPKI [1] реализованы наборы программ тестирования и верификации поведения ПТК, его протоколов, форматов, API-компонентов НСЭЦП. Для достижения интероперабельнсти (рис. 8) наборы программ для специальных и/или контрольных испытаний базовых объектов НСЭЦП разделены на две группы: специальные и контрольные, что обусловлено уровнем требований в стандартах: «обязательные» и «опциональные». Примером может служить опциональное поле «subjectAltName» сертификата открытого ключа, содержащее согласно RFC 5280 псевдоним владельца.

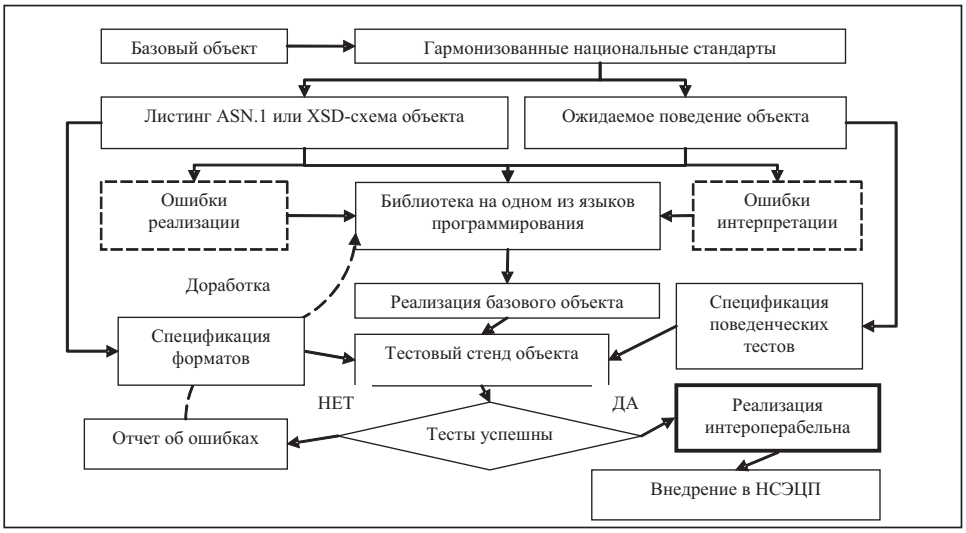

Рис. 8. Общая схема функционирования тестового стенда НСЭЦП

В прототипе реализованы наборы для оценки таких базовых объектов НСЭЦП.

1. Профили сертификатов и списков аннулированных сертификатов (CRL). Должны соответствовать основополагающим стандартам ISO/IEC 9594-8:2008 и RFC 5280. Стенд верифицирует семантику и соответствующие расширения или значения ограничений, т.е. проверяет полную совместимость с ДСТУ ETSI TS 101 862:2009.

2. Управление PKI. Стенд верифицирует он-лайн-взаимодействие между компонентами PKI, определяя профиль компонентов PKI, основанных на RFC 5272, RFC 5273, RFC 5274.

3. Форматы сообщений, основанные на CMS. Согласно ДСТУ ETSI TS 101 733:2009 и ДСТУ ETSI TS 101 734:2009 проверяются форматы сообщений, используемые в обмене данными между компонентами PKI.

4. Форматы сообщений, основанные на XML. Согласно ДСТУ ETSI TS 101 903:2009 и ДСТУ ETSI TS 101 904:2009 проверяются форматы сообщений, используемые в обмене данными между компонентами PKI.

5. Функциональные протоколы необходимые PKI для доставки сертификатов, CRL или информации о статусе сертификата с помощью разнообразных приложений (почтовых клиентов или Интернет-браузеров). Задача стенда — выбрать «минимальные достаточные» по функциональности репозитарии и методы доступа, способные поддержать все интероперабельные репозитарии и клиентские приложения, достигая взаимодействия с автоматической верификацией подписи и цепочки сертификатов независимо от реализации клиента и репозитария ПТК. Этот блок тестов основан на наиболее распространенных стандартах репозитариев, каталогах X.500 и методах доступа, указанных в PKIX Интернет-стандартах: LDAP v3 и OCSP v1. Транспортные протоколы между репозитарием и клиентами ограничены TCP/IP (для LDAP) и HTTP (для OCSP).

6. Процедуры валидации подписей и цепочек сертификации. Верифицируются согласно ДСТУ CWA 14171, а также оценивается поддержка политик подписания согласно ETSI TR 102 272.

7. Криптоалгоритмы. Соответствие устанавливается согласно перечню утвержденных и рекомендованных криптоалгоритмов ЭЦП, в основном соответствующих рекомендациям ДСТУ ETSI TS 102 176:2009. Причем проверяется кроссмодульная (между шаблонным криптомодулем и реализованным) генерация подписи (один криптомодуль генерирует ЭЦП, второй верифицирует ЭЦП и наоборот).

8. API-подписи. Верифицируется соответствие реализованных API нормам ДСТУ EN 14890.

Пример работы тестового стенда — проверка подписи сертификата открытого ключа криптоалгоритмом ДСТУ 4145. Согласно ДСТУ ETSI TS 101 862 поле подписи имеет ASN.1 тип BIT STRING (листинг 1).

Листинг 1

```
Certificate  ::=  SEQUENCE  {
   tbsCertificate  TBSCertificate,  --  Контент  сертификата
-- Комплект  подписи  и  ее  параметры
      signatureAlgorithm  AlgorithmIdentifier,
   signature    BIT  STRING  --  Значение  подписи  }
```

На листинге 2 приведен фрагмент корневого сертификата ЦЗО, в котором в ASN.1 тип BIT STRING вложен ASN.1 тип OCTET STRING, содержащий строку подписи. При наличии криптомодуля ДСТУ 4145 любой не украинский комплекс не сможет верифицировать ЭЦП, поскольку в бинарной строке подписи имеются лишние байты, указывающие ASN.1 тип OCTET STRING и его длину в DER-кодировании нотации ASN.1.

Листинг 2

```
Offset|  Len   |LenByte|
======+=======+=======+=========================================
  1104|  111|   1| BIT  STRING  UnusedBits:0  :
  1107|  108|   1|   OCTET  STRING  :
      |     |    |     7C40D696732D1A766B01B7A881D158BE9006AB833B10BA873F0538
      |     |    |     6C91877118D7ED2EF6033D8C6410CD8D190FBD7F544980248D5518
      |     |    |     F73615A81E192A70BE51DE0C401E27BE6BECCCAAC5F4DB9F2119D4
      |     |    |     F7317926D12CA7FDC368B206B85F3CEF9D569AB3DBEC3CA32B6534
```

ЗАКЛЮЧЕНИЕ

Идентифицировать проблемы интероперабельности НСЭЦП целесообразно, сопоставив ее как открытую систему с эталонной моделью квалифицированной инфраструктуры открытых ключей QPKI. В связи с этим разработано стандартное представление политики подписания как базовой составляющей бизнес-модели ЭЦП согласно Директиве 1999/93/ЕС. Разработан профиль комплекта подписей ДСТУ 4145 + ГОСТ 34.311 для интероперабельных его реализаций в криптомодулях на основе библиотеки «UPGCryptoProviderBasic» (сертификат авторского права № 31086 от 24.11.2009) криптографических преобразований согласно спецификации Microsoft CryptoAP. Внедрена формальная методика аккредитации ЦСК, основанная на национальных стандартах Украины, гармонизированных с европейскими. Разработан действующий прототип тестового стенда для оценки степени интероперабельности реализаций эталонной модели QPKI на основе формальной методики аккредитации ЦСК.

СПИСОК ЛИТЕРАТУРЫ

1. Закон України від 22.05.2003 № 852 «Про електронний цифровий підпис».
2. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ та Держдепартаменту з питань зв'язку та інформатизації Мінтрансу від 11.09.2006 №99/166.
3. Мелащенко А.О., Перевозчикова О.Л. Організація кваліфікованої інфраструктури відкритих ключів. — Київ: Наук. думка, 2010. — 392 с.
4. Закон України від 01.12.2005 № 3164 «Про стандарти, технічні регламенти та процедури оцінки відповідності».
5. Сергієнко І.В. Інформатика та комп'ютерні технології. — Київ: Наук. думка. — 2004. — 432 с.

Поступила 11.03.2011