D.A. Melnikov, V.G. Ivanenko, T.A. Kondratyeva, A.D. Melnikov

Practical Implementation of Various Public Key Infrastructure Models

Keywords: electronic (digital) signature; public key infrastructure; authentication; confidentiality; integrity; non-repudiation; validation authority; certification authority; public key certificate.

Abstract: The paper proposes a short comparative analysis of the contemporary models of public key infrastructure (PKI) and the issues of the PKI models real implementation. The Russian model of PKI is presented. Differences between the North American and West Europe models of PKI and Russian model of PKI are described. The problems of creation and main directions of further development and improvement of the Russian PKI and its integration into the global trust environment are defined.

Д.А. Мельников, В.Г. Иваненко, Т.А. Кондратьева, А.Д. Мельников

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ РАЗЛИЧНЫХ МОДЕЛЕЙ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ

Введение

Одной из значимых услуг (служб, сервисов), предоставляемых современными информационно-технологическими сетями и (или) системами (ИТС), является возможность проведения юридически значимого электронного документооборота (ЭДО) в рамках обеспечения целостности и конфиденциальности данных на основе использования механизмов идентификации и аутентификации пользователей, а также средств обеспечения неотказуемости от авторства сообщения [1].

В технических средствах, реализующих указанные механизмы, часто используются несколько классов криптографических способов обеспечения информационной безопасности (ИБ) одновременно. Например, если для обеспечения конфиденциальности ЭДО применяют симметричные алгоритмы шифрования, то распределение ключей может быть осуществлено тремя способами:

1) напрямую между взаимодействующими сторонами с использованием алгоритмов и процедур симметричного шифрования;

2) используя процедуры симметричное шифрование с привлечением доверенной третьей стороны (ДТС);

3) применяя обеспечение ключами на основе алгоритмов и процедур открытой криптографии с привлечением ДТС.

Первый способ вполне приемлем для небольших автономных (локальных) систем. Если пользователь устанавливает соединения только с малым количеством контрагентов, то он может провести предварительную процедуру инициализации с каждым из них без особых затруднений.

Второй способ приемлем для крупных систем с прямым административным подчинением, для которых достаточно обеспечение ограниченной поддержки аутентификации без решения задачи обеспечения неотказуемости.

Третий способ, наиболее целесообразный для распределённых ИТС общего пользования, обеспечивает комплексное и всестороннее технологическое решение. Если ДТС «связывает» открытый ключ с конкретным пользователем или системой путем удостоверения параметра подлинности взаимодействующей стороны, обладающей соответствующей парой ключей открытого шифрования, то можно реализовать весь спектр услуг по обеспечению ИБ. В частности, с использованием технологии электрон-

ной цифровой подписи (ЭЦП) могут подтверждаться целостность, аутентификация пользователей и неотказуемость.

Для распределённых ИТС общего пользования необходимо наличие большого количества ДТС, технологически связанных между собой. Такая совокупность взаимосвязанных ДТС образует инфраструктуру обеспечения ИБ, на которую могут полагаться участники юридически значимого ЭДО. На практике наибольшее распространение получила так называемая инфраструктура открытых ключей (*publickeyinfrastructure* – PKI [2]), позволяющая «связывать» открытые ключи с конкретными пользователями и предоставляющая необходимые услуги, востребованные при проведении процедур полноценного юридически значимого ЭДО.

В данной работе рассмотрен зарубежный опыт использования различных моделей формирования PKI, а также итоги более чем 20-летнего развития отечественной инфраструктуры открытых ключей, не имеющей пока своего логического завершения.

Основные элементы PKI

С целью единообразного описания различного, в том числе отечественного, опыта формирования PKI, рассмотрим ее основные организационно-технологические элементы, позволяющие вести юридически значимый ЭДО, гарантирующий, что:

- пользователь или процесс, который был идентифицирован в качестве передающей стороны в процедуре информационного обмена, действительно является источником сообщения;
- пользователь или процесс, выступающий в роли принимающей стороны в процедуре информационного обмена, действительно является получателем;
- целостность данных не скомпрометирована.

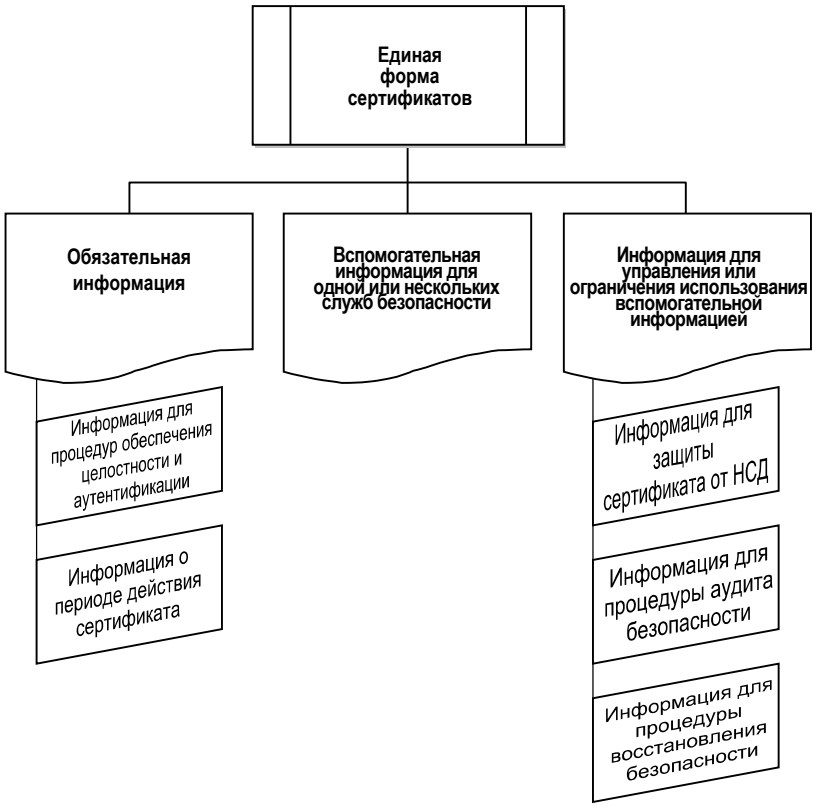

Рис. 1. Структура сертификата

PKI представляет собой совокупность организационных структур и аппаратно-программных средств обеспечения технологий шифрования и служб, способных в интересах пользователей обеспечить безопасность электронных коммерческих сделок с использованием ИТС общего пользования. Основу деятельности PKI составляют выпуск и обеспечение юридически значимого оборота так называемых цифровых сертификатов (рис. 1, [3–7]), удостоверяющих принадлежность ЭЦП конкретной организации и (или) физическому лицу.

Типовая PKI должна обеспечивать:

- выпуск цифровых сертификатов для индивидуальных пользователей и (или) серверов технологических процессов документооборота;
- регистрацию ПО оконечного пользователя;
- собственную интеграцию с каталогами сертификатов;
- средства обслуживания, восстановления и аннулирования сертификатов.

Функциональными элементами PKI являются ***центры сертификации*, *центры* (*пункты*) *регистрации*, *репозитарии* и *архивы*** [2, 7, 8], дополнительными – ***центры атрибутных сертификатов***.

Центры сертификации, получившие в отечественной практике название УЦ – удостоверяющий центр, обеспечивают подтверждение параметров подлинности взаимодействующих сторон в процессе ЭДО, включая электронную коммерцию, путем издания *сертификата открытого ключа* (СЕРТ|ОК) для каждого параметра подлинности на основе соответствия зарегистрированным (учётным) данным пользователей.

Центр (пункт) регистрации (РЦ) – доверенный субъект УЦ для регистрации или подтверждения параметров подлинности клиентов, пользующихся услугами этого УЦ.

Репозитарий представляет собой базу данных (БД), в которой хранятся действующие цифровые сертификаты, выданные центром сертификации, а также списки отозванных сертификатов (СОС). *Главная задача* репозитария – предоставлять данные, которые помогают его пользователям, именуемым как взаимодействующие стороны и получившим сообщения, подписанные ЭЦП, согласовать (установить) состояние (статус) цифровых сертификатов физических лиц и (или) организаций. СЕРТ|ОК могут быть аннулированы в случае компрометации закрытого ключа владельца сертификата, увольнения владельца, изменения его регистрационных данных. Кроме того, СОС задокументируют исторический статус аннулированных сертификатов.

Архив (archive) представляет собой БД, содержащую информацию, которая будет использоваться в урегулировании возможных будущих споров (конфликтных ситуаций). *Задача* архива – хранить и защищать необходимую и достаточную информацию для определения того, является ли ЭЦП на «устаревшем» документе заслуживающей доверия.

Пользователи PKI (PKI-пользователи) представляют собой юридические (организации) или физические лица, которые пользуются услугами инфраструктуры. Среди них выделяют:

– *взаимодействующую сторону*, которая полностью доверяет сертификату, содержащему открытый ключ противоположной стороны;

– *держатель (владелец) сертификата*, который получил СЕРТ|ОК и может подписывать электронные документы.

Следует заметить, что физическое лицо и (или) организация могут одновременно выступать и в роли взаимодействующей стороны, и в роли владельца сертификата.

PKI связывает различные УЦ между собой надёжными технологическими маршрутами так, что проверяющая сторона может быть уверена в подлинности используемого СЕРТ|ОК. Получатели подписанного сообщения, не взаимодействующие с УЦ, который выпустил СЕРТ|ОК для отправителя сообщения, могут также проверить подлинность СЕРТ|ОК отправителя путём поиска маршрута между УЦ, обслуживающим получателя подписанного сообщения, и УЦ, выдавший сертификат отправителю.

Структура таких связей может быть *сетевой* или *иерархической* (рис. 2) [2, 8]:

- *в иерархическая структуре* УЦ «выстраиваются» под корневым («главным») УЦ, который выпускает СЕРТ|ОК для «подчинённых» УЦ;
- *в сетевой структуре* независимые УЦ сертифицируются каждый с каждым, т.е. кросс-сертифицируются – выпускают и доставляют СЕРТ|ОК друг другу и объединяют их в пары кросс-сертификации (*crossCertificatePair*), в результате чего формируется сеть доверенных связей между «равноправными» (*peer*) УЦ.

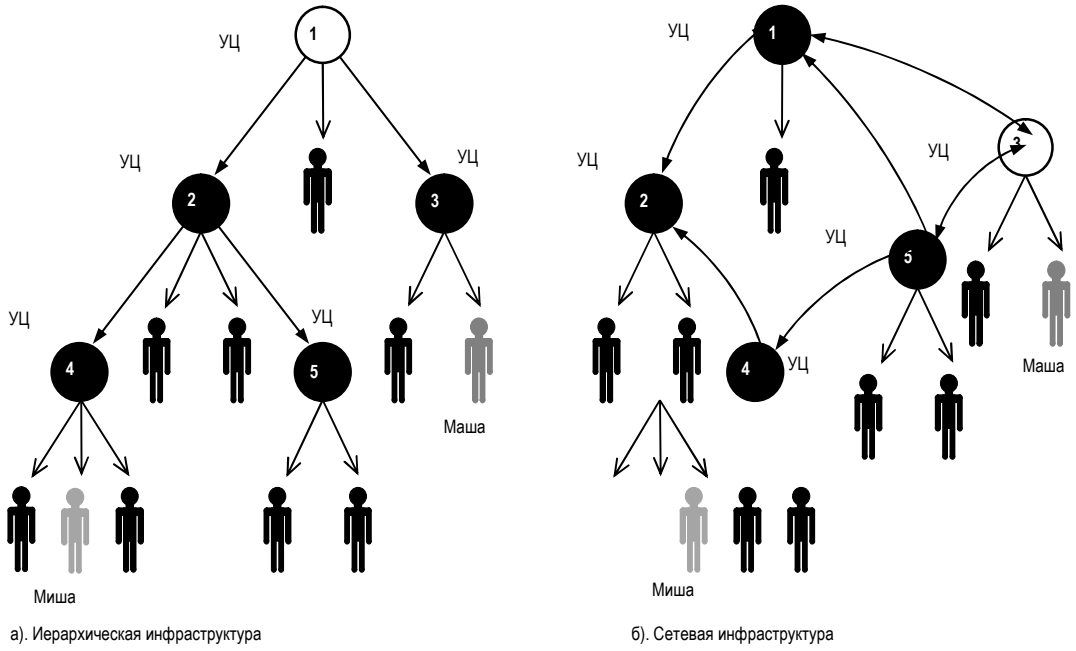

Рис. 2. Основные типы PKI-архитектур

Прикладные системы PKI базируются на глобальной Службе единого каталога (СЕК), предназначенной для распределения СЕРТ|ОК и информации об их состоянии. СЕК предоставляет средства для хранения и распределения сертификатов и их обновления. Типовые услуги СЕК определяются Рекомендациями ITU-TX.500 [9].

Указанный Стандарт включает серию рекомендаций и технические требования и, кроме того, содержит ряд ссылок на несколько других стандартов ISO. Он был разработан с целью описания услуг (служб) СЕК, которые могли бы функционировать, невзирая на системные, корпоративные и международные различия. Совокупность разработанных протоколов определяет функциональные процедуры информационного взаимодействия серверов, например формирования маршрутов («цепочек») доверия, дублирования и перенаправления, а также вводит протокол доступа к СЕК (*DirectoryAccess-*

Protocol – DAP) для связи между клиентом и сервером. Немного позже, в качестве альтернативы DAP-протоколу, в рамках интернет-сообщества был разработан протокол упрощённого доступа к СЕК (*LightweightDirectoryAccessProtocol* – LDAP). Большинство СЕК-серверов и их клиентов используют LDAP-протокол, и не все из них поддерживают DAP-протокол [10].

Чтобы СЕК-серверы были «привлекательны» для прикладныхPKI-систем, они должны быть функционально совместимыми. Без такой совместимости проверяющая сторона информационного взаимодействия не сможет получить необходимые СЕРТ|ОК и СОС от удалённых источников с целью проверки подписей и подлинности СЕРТ|ОК.

Северо-американский опыт формирования PKI

Одной из основных причин создания и развития национальной PKI в США стал повсеместный переход к ЭДО, обусловленный принятием двух законов, которые обязывают федеральные ведомства предоставлять услуги в электронной форме, а именно:

• закон о мобильности и ответственности за медицинское страхование (*Health Insurance Portability and Accountability Act* [11]). Данный закон был принят в 1996 году. Нормы этого закона были направлены, в частности, на повышение эффективности здравоохранения за счёт использования способов электронного обмена структурированными данными о состоянии здоровья граждан. Для решения проблемы обработки персональных данных указанный закон дал право на применение стандартов по обеспечению конфиденциальности и целостности с целью защиты такой информации;

• закон о ликвидации бумажного делопроизводства в правительстве (*Government Paper work Elimination Act* [12]), принятый в 1998 году:

1) требует от федеральных ведомств предоставлять услуги в электронном виде;

2) требует, чтобы федеральные ведомства реализовали с 21 октября 2003 года дополнительную функцию предоставления информации или проведение процедур информационного обмена в электронной форме;

3) устанавливает правовой статус электронных записей и связанных с ними ЭЦП;

4) требует от ведомств использования методов электронной аутентификации (ЭА) с целью проверки параметра подлинности отправителя электронного сообщения и целостности последнего;

5) определяет ЭЦП как один из способов подписи электронных сообщений, которая идентифицирует и аутентифицирует персону (являющуюся источником сообщения), а также указывает на заверение содержания самой ЭП.

В рамках Президентского плана создания электронного государства, нацеленного на построение и расширение электронного государства (*e-Government*) была принята *Программа ЭА* (ПЭА) [13] для поддержки владельцев промежуточных систем в процессе создания ими доверенных связей со своими клиентскими сообществами на основе применения электронных средств подтверждения подлинности. Для развития этого направления ПЭА предлагает использовать службы по подтверждению подлинности при реализации федеральных электронных бизнес-процессов, которые, в свою очередь, позволяют обеспечить надёжность и конфиденциальность транзакций *E*-правительства на основе формирования единой стратегии и технической инфраструктуры подтверждения подлинности.

Совокупность государственных структур по реализации ПЭА включает Административно-бюджетное управление при Президенте США, Федеральный совет руководителей информационных служб, Федеральное управление по реализации программы формирования архитектуры предприятия и Центры службы электронной аутентификации (ЦСЭА). В частности, ЦСЭА несёт ответственность за предоставление услуг еди-

нообразной поточной аутентификации через государственные структуры. Этот процесс сопровождается непосредственной работой с ведомствами и учреждениями по оказанию им содействия при определении ими своих нужд в сфере ЭА (приемлемая политика и технические стандарты с гарантией требуемого уровня безопасности) и при решении проблем технической и функциональной совместимости.

Архитектура северо-американской модели федеральной PKI (FPKI) включает федеральный УЦ кросс-сертификации (ФУЦ), который представляет собой информационную систему, предназначенную для формирования взаимосвязей между отдельными PKI, невзирая на их архитектуры [13]. В рамках FPKI-архитектуры ФУЦ решает сложную техническую проблему функциональной совместимости, связанную со «встраиванием» PKI бизнеса в федеральную PKI-инфраструктуру. Такое «встраивание» заключается в предоставлении PKI-услуг частному бизнесу различными коммерческими провайдерами.

ФУЦ не выпускает сертификаты и не предназначен для использования в качестве «точки доверия». Все PKI-пользователи полагают, что ФУЦ является промежуточной точкой. ФУЦ устанавливает равноправные взаимоотношения между PKI-инфраструктурами различных организаций. Такие взаимосвязи могут быть объединены с целью формирования «моста доверия», соединяющего пользователей отдельных PKI различных организаций.

Общие принципы функционирования УЦ системы кросс-сертификации (УЦКС) представлены на рис. 4.

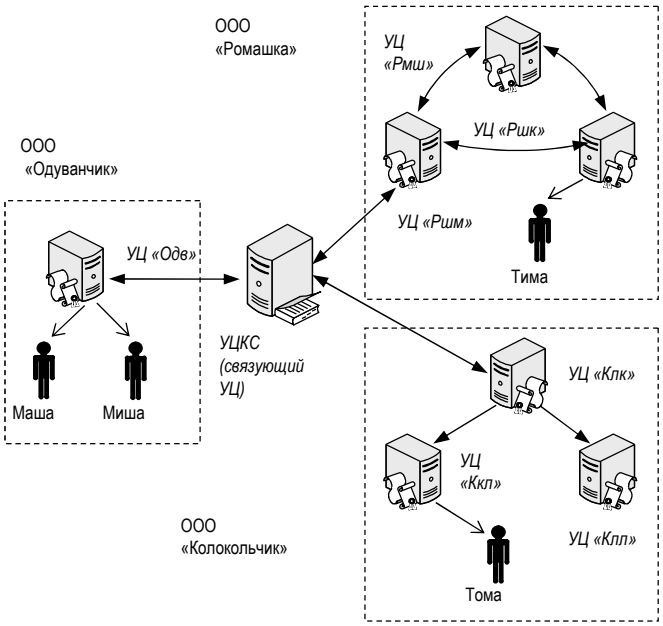

Рис. 4. УЦКС и PKI-инфраструктуры организаций

FPKI-архитектура (рис. 5) включает несколько кросс-сертифицированных УЦ, которые обладают полной функциональной совместимостью друг с другом. Эта группа УЦ является автономной (*off-line*) (т.е. не связанной с Интернет-сетью). Иерархическая структура информационно-издательской службы, входящей в FPKI-архитектуру, отвечает за предоставление автономных (*off-line*) и интерактивных (*on-line*) СЕК-услуг, которые разделены внутренним однонаправленным сетевым экраном [13].

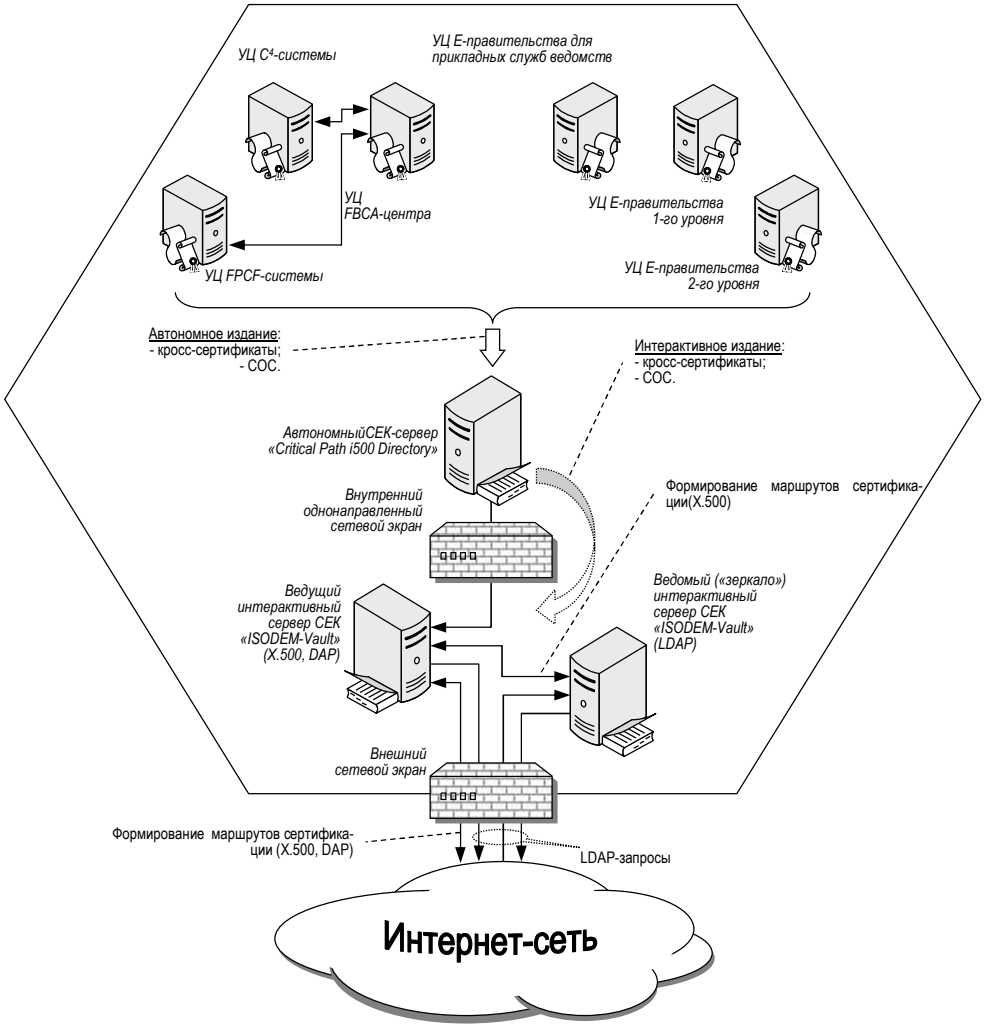

Рис. 5. Архитектура СЕК-системы в рамках федеральной PKI-инфраструктуры (интерактивный и автономный СЕК-сегменты)

В рамках FPKI-архитектуры определены уполномоченные УЦ, отвечающие за формирование и реализацию политики FPKI:

1) ФУЦ;

2) корневой УЦ системы формирования и реализация политики федеральной PKI-инфраструктуры (Federal PKI CommonPolicyFramework – FCPF);

3) корневой УЦ объединённой системы гражданских и коммерческих УЦ общего назначения (CitizenandCommerceClassCommon – C4);

4) УЦ *E*-правительства.

Все УЦ FPKI-архитектуры автономны (то есть изолированы от Интернет-сети), а их информация автоматически публикуется во внутреннем автономном СЕК-сегменте. Вся информация, накапливаемая и хранящаяся в автономном режиме, периодически в ежедневном режиме публикуется в интерактивном СЕК-сегменте ФУЦ (то есть соединённым с Интернет-сетью), что обеспечивает её всеобщую (глобальную) доступность на основе стандарта X.500 (DAP-протокол) и LDAP-протокола.

Западно-европейский опыт

Основополагающим нормативным актом в Европейском союзе (ЕС) является Директива Европейского парламента и Европейского совета от 13 декабря 1999 года «Основы объединения электронных подписей» (*DIRECTIVE 1999/93/ECOF THE-EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community frame work for electronic signatures*), который дал импульс к формированию Западно-Европейской PKI технологической основы создания *E*-государства, *E*-бизнеса, *E*-торговли и т.п.

Необходимость регламентации общего подхода была вызвана тем, что национальные PKI стран Европы создавались и совершенствовались по образцу северо-американской модели. Однако наличие в ЕС множества языков государственного уровня потребовало от Еврокомиссии использования новых подходов при создании и развитии единой (федеративной) модели PKI. Такими подходами стало использование таких структурных элементов, как *Центр подтверждения подлинности* (ЦПП) и *Реестр состояния доверенных служб* (РСДС) [14,15,16]. Функционально-структурная модель ЦПП представлена на рис. 6.

Одной из основных услуг ЦПП, которая предоставляется его пользователям, является проверка подлинности СЕРТ|ОК в режиме «одного окна». Сложность прикладной автоматизированной системы обслуживания ЭЦП (ПАСО), с точки зрения установления взаимосвязей с каждым УЦ на территории ЕС, связана с трудно реализуемым процессом управления составом и содержанием квалифицированных СЕРТ|ОК, выдаваемых европейским гражданам техническими УЦ, которых в Европе насчитывается несколько сотен [14, 17].

В этой связи любая ПАСО[1] должна обеспечивать:

1) проверку подлинности сертификата напрямую с выдавшим его УЦ, если последний известен, но в том случае, когда ЦПП не нужен;

2) нахождение адреса ЦПП, который способен и доступен для обработки СЕРТ|ОК, выданных указанным в сертификате УЦ;

3) отправку запроса о проверке подлинности СЕРТ|ОК на уже известный прикладной информационной системе ЦПП, выступающий в роли уполномоченного центра, который найдёт адрес целевого ЦПП и перенаправит ему поступивший запрос. Таким ЦПП может быть коммерческая или государственная ЦПП национального или европейского уровня.

[1] В данном случае под ПАСО понимается любая прикладная информационно-технологическая система (например, ЭДО, платёжная, финансовая, система электронной коммерции (бизнеса) и т.п.), которая обрабатывает, хранит и транслирует или использует электронные сообщения (документы), содержащие ЭП.

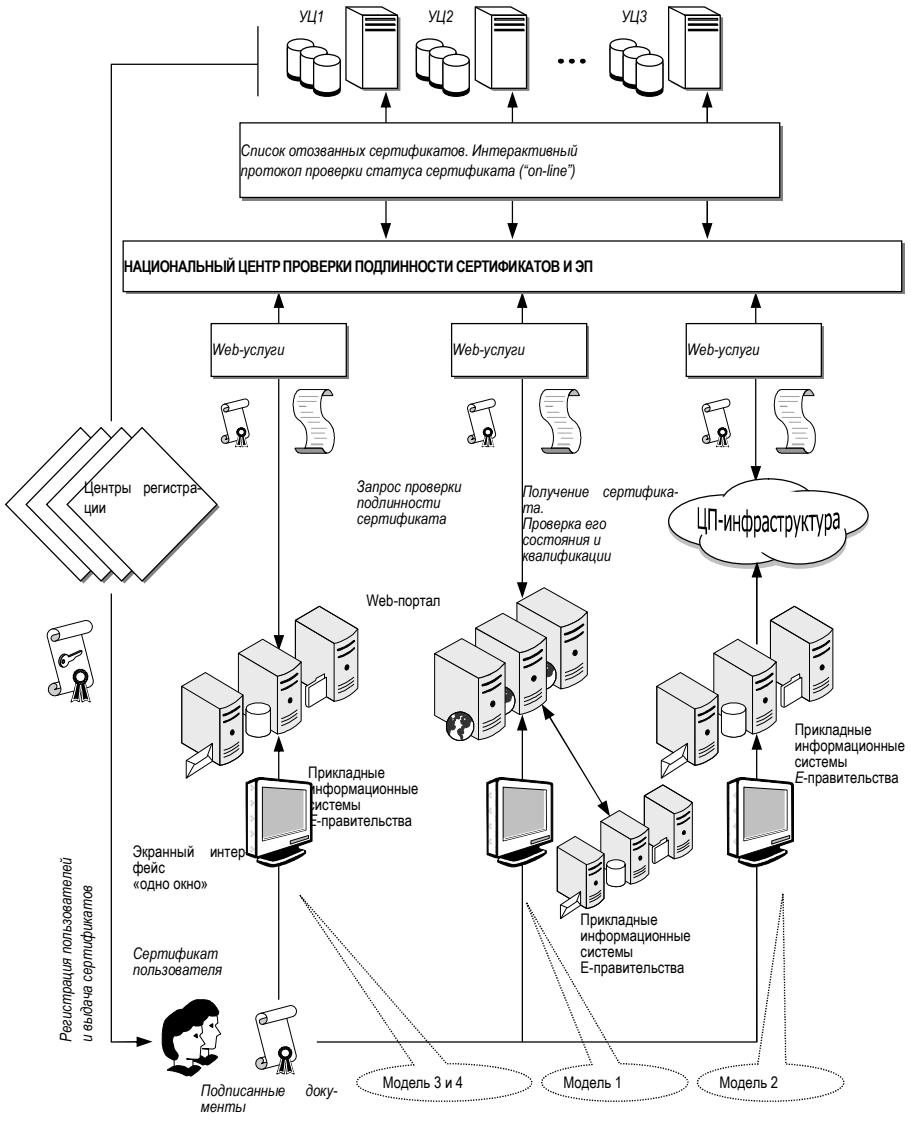

Рис. 6. Функционально-структурная модель ЦПП

Представленная на рис. 6 иерархическая структура распределения функций по обслуживанию ЭЦП основывается на концепции использования национальных ЦПП. В зависимости от соответствующей модели самой ПАСО, последняя может:

– напрямую передавать свои запросы на ЦПП (модели 3 и 4);

– передавать свои запросы на Web-портал, который устанавливает соединения с ЦПП (модель 1);

– использовать инфраструктуру ЭЦП для соединения с ЦПП (модель 2).

Для формирования федеративной (интегральной) системы ЦПП ЕС предусмотрено проведение следующих первостепенных мероприятий:

- построение доверенных связей (включая ответственность сторон) между участниками федеративной (интегральной) системы;
- обязательная разработка и стандартизация протоколов информационного обмена между ЦПП и между ЦПП и ПАСО;
- построение жизнеспособной модели управления на европейском уровне.

Второй важнейшей услугой, предоставляемой ЦПП, является проверка подлинности ЭЦП. ЦПП могут быть делегированы проверка грамматики и синтаксиса ЭЦП и математическая проверка ЭЦП.

В общем, делегирование этой процедуры ЦПП требует доставки всего документа в ЦПП (включая ЭЦП и возможно существующую электронную метку времени). Это может вызвать противоречие с точки зрения безопасности документооборота при обработке конфиденциальных данных. Данная проблема может быть легко преодолима с помощью локального вычисления значений хэш-функции подписанного документа и последующей доставки только значения хэш-функции вместо всего документа. При таком подходе процедуру проверки подлинности сертификата можно рассматривать как частный процесс процедуры проверки подлинности ЭЦП. Если в ЭЦП присутствует электронная метка времени, то последняя должна быть подтверждена в обязательном порядке.

На ЦПП могут возлагаться и дополнительные функции (предоставление услуг), среди которых:

- извлечение информации о владельцах CERT|OK третьей версии Рекомендации ITU-T X.509 и проведение их семантической обработки с целью обеспечения трансграничной функциональной совместимости ЭЦП [6];
- проведение проверки на предмет исторической подлинности CERT|OK и ЭП. Эта процедура позволит ПАСО проверить подлинность сертификата или ЭЦП в указанный в прошлом момент времени.

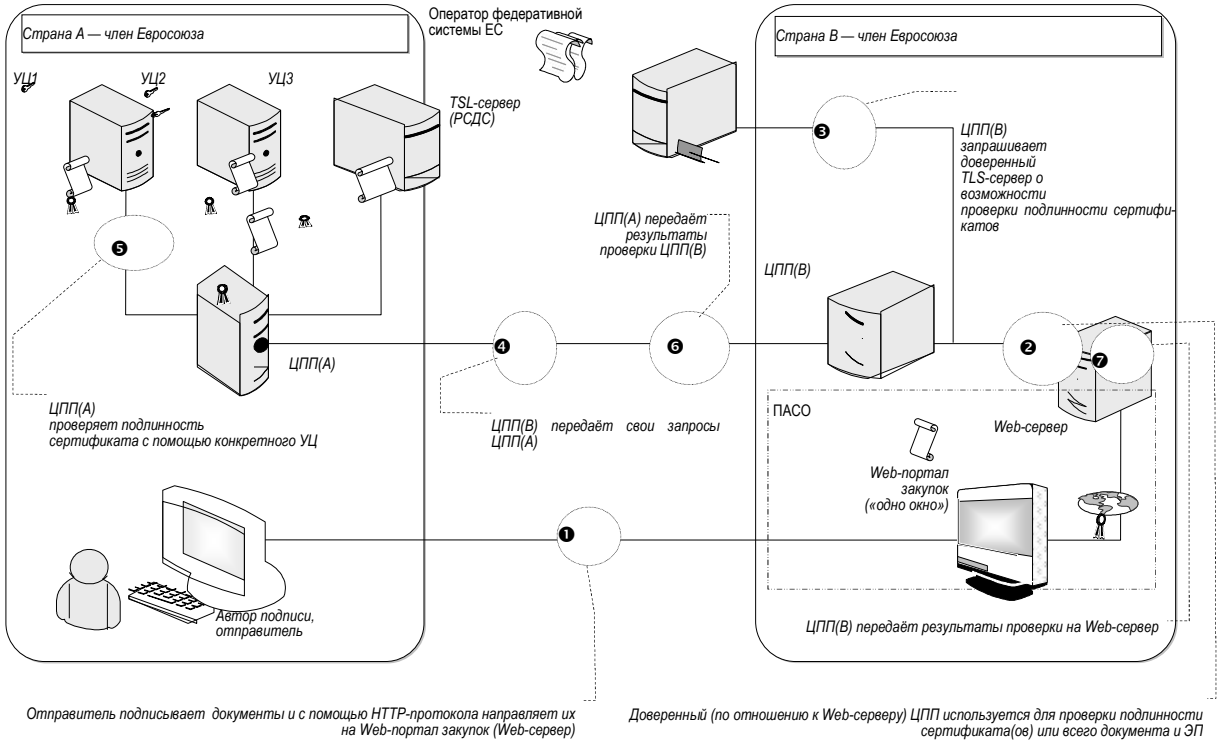

Рис. 7. Функционально-структурная схема федеративной модели PKI Евросоюза

На рис. 7 представлена функционально-структурная схема западно-европейской реализации PKI.

В широком смысле, федеративная модель PKI ЕС включает следующих участников [14]:

1. УЦ, которые выдают СЕРТ|ОК. Их основная роль заключается в:

- создании базовой инфраструктуры, предназначенной для формирования ЭЦП самими пользователями этой инфраструктуры;
- обеспечении базовых «строительных» компонентов для проверки подлинности СЕРТ|ОК, которые выдают эти УЦ;
- соблюдении стандартных общеевропейских правил в соответствие с требованиями Европейской директивы по ЭЦП.

2. УЦ, которые несут ответственность за проверку ЭЦП (и, следовательно, за проверку подлинности СЕРТ|ОК) по отношению к своим потребителям.

3. Оператор федерации (орган в рамках Еврокомиссии), который вводит единые правила, чтобы ЦПП, входящие в федерацию, были под контролем. Он предоставляет доступ к общим надёжным ресурсам, включая обзор ЦПП, способных установить соединение с определёнными УЦ (сопровождает РСДС). Не допускается, чтобы оператор действовал бы сам в качестве ЦПП, так как это может скомпрометировать его нейтралитет.

Отечественный опыт

Формирование отечественной национальной PKI началось в середине 90-х годов прошлого века в виде «стихийного» и слабо контролируемого на государственном уровне процесса [18]. В 2004 году было образовано Федеральное агентство по информационным технологиям (ФАИТ), на которое были возложены функции государственного регулятора и координатора работ по созданию в России информационного общества, в том числе PKI, так как ФАИТ стал уполномоченным федеральным органом исполнительной власти в области использования ЭЦП. Кроме этого, ФАИТ курировало реализацию Федеральной целевой программы (ФЦП) «Электронная Россия (2002… 2010 годы)».

В рамках выполнения последней ФЦП был образован Общероссийский государственный информационный центр (ОГИЦ [19]). Целью создания ОГИЦ (рис. 8) является обеспечение информационного взаимодействия федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ, других государственных органов и органов местного самоуправления при предоставлении гражданам и организациям государственных услуг с использованием телекоммуникационных технологий. Основными функциями ОГИЦ были определены:

1) предоставление государственных услуг в электронном виде в режиме «одного окна»;

2) выполнение функций федерального УЦ, являющегося корневым в системе УЦ национальной PKI России.

По своим стратегическим задачам ОГИЦ определялся как *информационно-технологическое ядро российского информационного общества*. Обобщёнными задачами, поставленными перед ОГИЦ, стали:

- обеспечение юридически значимого ЭДО и иного информационно-технологического взаимодействия органов власти страны между собой;
- предоставление технических средств и информационных технологий для государственных автоматизированных информационных систем (ГИС);

• официальное информирование о деятельности органов государственной власти и органов местного самоуправления и предоставление населению и организациям государственных услуг в электронном виде.

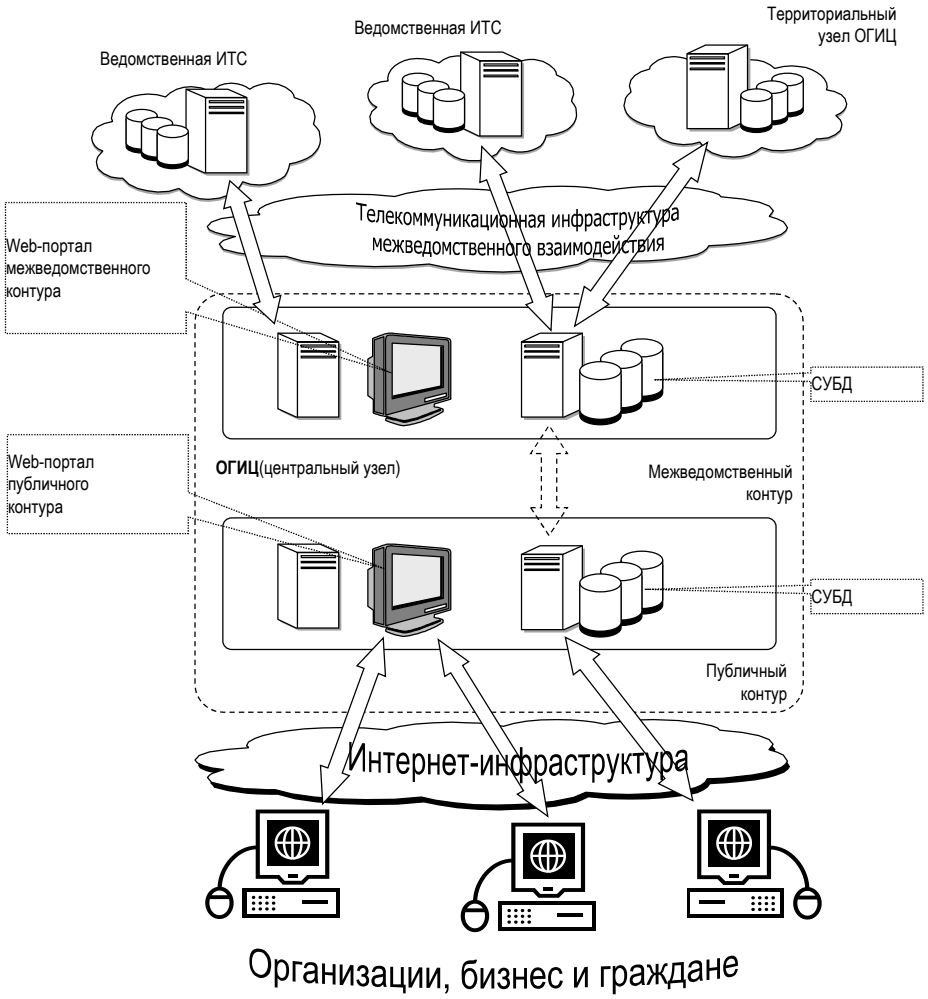

Рис. 8. Функциональная структура ОГИЦ

Информационное взаимодействие органов власти между собой и с гражданами предполагалось осуществлять в рамках отдельных сетевых сегментов (контуров, рис. 8) – межведомственного и публичного, каждый из которых следует рассматривать как совокупность взаимосвязанных информационно-технологических и телекоммуникационных объектов.

Российская модель национальной инфраструктуры открытых ключей, подтверждения подлинности СЕРТ|ОК и проверки ЭП представлена на рис. 9. По сути, представленная модель является *компромиссным решением* между северо-американской и западно-европейской моделями [18]. С одной стороны, в российской модели присутствует ФУЦ, что характерно для северо-американской модели, и одновременно используется список аккредитованных УЦ (аналог РСДС).

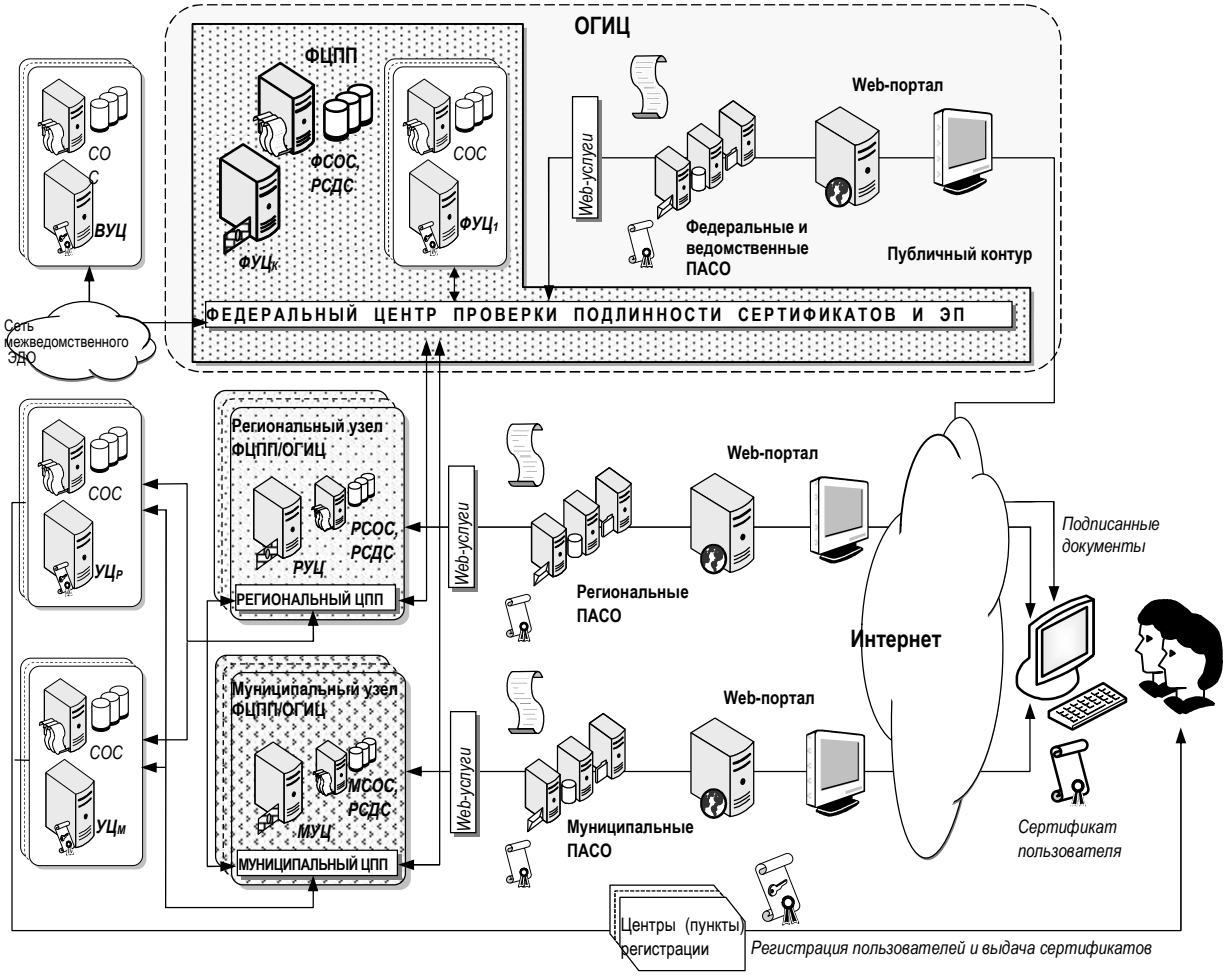

Рис. 9. Российская модель национальной инфраструктуры открытых ключей

Выбор такой модели был связан, в первую очередь, с тем, что во второй половине 90-х годов прошлого века в России началось лавинообразное появление УЦ, число которых перевалило за 400. Их неконтролируемый рост неизбежно привел бы к технологическому «зоопарку», т.е. взаимодействие созданных УЦ практически было невозможно в силу отсутствия функциональнаясовместимости. С созданием ФАИТ начался сложный процесс медленного становления отечественнойPKI.

В настоящее время структура ОГИЦ включает только корневой ФУЦ ($ФУЦ_К$, нулевой уровень иерархии) и несколько УЦ первого уровня ($ФУЦ_1$). Список аккредитованных УЦ ведётся в TSL-формате, установленном стандартом [15]. Дальнейшее развитие отечественной национальной PKI после упразднения в августе 2010 года ФАИТ практически отсутствует [20]. Это связано с тем, что:

- не определен орган государственной власти, обеспечивающий какой-либо контроль со стороны государства. Так в Минкомсвязи России ведётся только РСДС, а дальнейшее развитие системы отдано «на откуп» бизнес-структурам. В то же время приведенные выше примеры развитых стран говорят о необходимости прямого и активного участия органов государственной власти в развитии информационного общества, в том числе национальной PKI в качестве регуляторов;
- ФЦП «Электронная Россия (2002…2010 годы)» завершилась неудовлетворительно, индикаторы информационного общества не были достигнуты. Выделенные ресурсы были направлены, в основном, на программно-техническое перевооружение ве-

домственных ИТС, которые по-прежнему остаются во многом функционально несовместимыми и не могут стать технологической основой современного информационного общества;

- существует значительная нехватка квалифицированных профессиональных кадров в области информатизации, в том числе создания PKI;
- по нашим оценкам, в стране существует более 400 УЦ, из которых лишь часть включена в РСДС, т.е. аккредитована на государственном уровне. Другая часть – различные ведомственные и корпоративные УЦ, обслуживающие отдельные конкретные организации. Третья часть – это не аккредитованные частные УЦ, обслуживающие муниципальные органы государственной власти и региональный бизнес. И большинство из них заинтересовано в государственном регулировании этой отрасли на основе единых правил с использованием государственной и частно-государственной политики партнерства, которая объединит все существующие УЦ в едином правовом и технологическом поле – национальной PKI.

В то же время очевидно, что представленная на рис. 9 модель формирования PKI позволит решить основные задачи по формированию единого поля доверия ЭЦП [18], среди которых:

- объединение всех существующих УЦ в единую PKI;
- формирование единого распределённого российского сегмента Службы единого каталога (с использованием DAP- и LDAP-протоколов);
- обеспечение технологической основы трансграничного взаимодействия с другими странами, т.е. вхождение российского PKI-пространства в мировую PKI;
- формирование технологической основы доверия для различных электронных взаимодействий, включая предоставление государственных услуг в электронной форме, дистанционное образование, *E*-нотариат, *E*-бизнес и т.д.;
- участие бизнес-структур в дальнейшем совершенствовании и наращивании российскогоPKI-пространства, что обеспечит им гарантированную и стабильную прибыль;
- обеспечение технологического «прорыва» и ускоренного социально-экономического развития России.

Заключение

В настоящее время развитие национальной PKI-инфраструктуры Российской Федерации практически сведено к минимуму. В этой связи необходимо кардинальное изменение государственной политики в области создания и развития информационного общества: от политики «стороннего наблюдения» до политики активного правового регулирования и дальнейшего совершенствования всех элементов информационного общества.

СПИСОК ЛИТЕРАТУРЫ:

1. ITU-T, X.810, «Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview». 1995. (ISO/IEC 10181-1: 1996).
2. National Institute of Standards and Technology. «Introduction to Public Key Technology and the Federal PKI Infrastructure». NIST Special Publication 800-32, 26 February 2001.
3. RFC 5280, «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile», IETF, May 2008.
4. RFC 6818, «Updates Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile», IETF, January 2013.
5. ISO, «Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks». ISO/IEC 9594-8, 2014-03-01.
6. ITU-T, X.509, «Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks». 10/2012.

7. Мельников Д.А. Информационная безопасность открытых систем. М.: ФЛИНТА, Наука. 2013.
8. Горбатов В. С., Полянская О. Ю. Основы технологии PKI. М.: Горячая Линия – Телеком., 2004.
9. ITU-T, X.500, «Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services». 10/2012. (ISO/IEC 9594-1: 2014).
10. RFC 4510-4519, «Lightweight Directory Access Protocol (LDAP)», IETF, June 2006.
11. «The Health Insurance Portability and Accountability Act of 1996». HIPAA; Pub. L. 104–191, 110 Stat. 1936, enacted August 21, 1996.
12. «The Government Paperwork Elimination Act». GPEA, Pub. L. 105-277, Approved October 21, 1998.
13. Federal PKI Operational Authority. «Federal Public Key Infrastructure (FPKI) Architecture. Technical Overview». October 2005.
14. IDABC, «Study on European Federated Validation Service (EFVS): Analysis and Assessment. Common Solution Model». Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°14. September 2009.
15. ETSI, «Electronic Signatures and Infrastructures (ESI); Trusted Lists». Technical Specification. ETSI TS 119 612 V1.2.1 (2014-04).
16. ETSI, «Electronic Signatures and Infrastructures (ESI); Cryptographic Suites». Technical Specification. ETSI TS 119 312 V1.1.1 (2014-11).
17. ETSI, «Electronic Signatures and Infrastructures (ESI); Signature validation procedures and policies». Technical Specification. ETSI TS 102 853 V1.2.1 (2014-12).
18. Мельников Д.А., Хоменок А.В. «Современное состояние отечественной инфраструктуры электронной коммерции». // Экономика, статистика и информатика. 2012. №1. С. 169–173.
19. «О некоторых мерах по обеспечению информационного взаимодействия государственных органов и органов местного самоуправления при оказаниигосударственных услуг гражданам и организациям». Постановление Правительства РФ от 25.12.2007 № 931.
20. «Об утверждении государственной программы Российской Федерации «Информационное общество (2011 – 2020 годы)» Постановление Правительства РФ от 15.04.2014 № 313 (ред. от 17.06.2015).

REFERENCES:

1. ITU-T, X.810, «Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview». 1995 (ISO/IEC 10181-1: 1996).
2. National Institute of Standards and Technology. «Introduction to Public Key Technology and the Federal PKI Infrastructure». NIST Special Publication 800-32, 26 February 2001.
3. RFC 5280, «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile», IETF, May 2008.
4. RFC 6818, «Updates Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile», IETF, January 2013.
5. ISO, «Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks». ISO/IEC 9594-8, 2014-03-01.
6. ITU-T, X.509, «Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks». 10/2012.
7. Melnikov D.A., «Open systems information security»: Textbook. – M.: FLINTA, Nauka, 2013. – 448 p. ISBN 978-5-9765-1613-7. (rus)
8. Gorbatov V.S., Polianskaia O.U. «Bases of PKI technology». – M.: Hot Line-Telecom, 2004. – 248 p. ISBN 978-5-9912-0213-8. (rus)
9. ITU-T, X.500, «Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services». 10/2012. (ISO/IEC 9594-1: 2014).
10. RFC 4510-4519, «Lightweight Directory Access Protocol (LDAP)», IETF, June 2006.
11. «The Health Insurance Portability and Accountability Act of 1996». HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996.
12. «The Government Paperwork Elimination Act». GPEA, Pub. L. 105-277, Approved October 21, 1998.
13. Federal PKI Operational Authority. «Federal Public Key Infrastructure (FPKI) Architecture. Technical Overview». October 2005.
14. IDABC, «Study on European Federated Validation Service (EFVS): Analysis and Assessment. Common Solution Model». Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°14. September 2009.
15. ETSI, «Electronic Signatures and Infrastructures (ESI); Trusted Lists». Technical Specification. ETSI TS 119 612 V1.2.1 (2014-04).
16. ETSI, «Electronic Signatures and Infrastructures (ESI); Cryptographic Suites». Technical Specification. ETSI TS 119 312 V1.1.1 (2014-11).
17. ETSI, «Electronic Signatures and Infrastructures (ESI); Signature validation procedures and policies». Technical Specification. ETSI TS 102 853 V1.2.1 (2014-12).
18. Melnikov D.A., Homenok A.V. «Modern e-Commerce Infrastructure». // Economics, statistics and informatics. 2012, No.1. 169-173 pp. (rus)
19. The Decree of the Government of the Russian Federation dated 25.12.2007 No. 931.
20. The Decree of the Government of the Russian Federation dated 15.04.2014 No. 313.