*V.I. Korolev*

**Architectural Building A Public Key Infrastructure Integrated Information Space**

*Keywords: information security, public key infrastructure, cryptographic protection, trust model, system architecture, corporation.*

The article keeps under consideration the mattersto apply the cryptographic system having a public key to provide information security and to implya digital signature. It performs the analysis of trust models at the formation of certificates and their use. The article describes the relationships between the trust model and the architecture public key infrastructure. It contains conclusions in respect of the options for building the public key infrastructure for integrated informationspace.

*В.И. Королёв*

# АРХИТЕКТУРНОЕ ПОСТРОЕНИЕ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ ИНТЕГРИРОВАННОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

## Обзор проблемы и постановка задачи

Современные информационные системы характеризуются двумя фундаментальными качествами:

- во-первых, они создаются как *автоматизированные системы* с широким использованием для обеспечения информационной деятельности компьютерных и телекоммуникационных технологий;
- во-вторых, они интегрируют большие объёмы информационных ресурсов для внутренней обработки и хранения данных, обеспечивают интенсивное электронное информационное взаимодействие с другими внешними по отношению к ним информационными системами.

При этом они обрабатывают разнородную информацию ограниченного доступа (государственная, коммерческая, банковская тайны, служебная информация, персональные данные) [2]. Это требует использования средств гарантированной защиты информации в программно-технической и телекоммуникационной среде, обеспечения надёжной аутентификации и авторизации информации при информационном обмене. Для реализации этих требований используются криптографические средства. Внедрение криптографии в информационные технологии позволило в целом повысить защищённость информации при её передаче по каналам связи и автоматизированной обработке, квалифицированно оценивать определённый уровень гарантии защиты информации при реализации базовых функций защиты – аутентификации и управления доступом к ресурсам [11]. Кроме того, криптографические средства обеспечили реализацию важнейших функций электронной обработки информации: авторизацию электронных документов, подтверждение их правового статуса в виде *электронной подписи* (ЭП) [1].

В данной работе не рассматриваются вопросы применения *простой* электронной подписи[1] с использованием логинов, паролей, кодов подтверждения и прочих средств, имеющих ограниченные возможности признания юридически значимого электронного документооборота и не обеспечивающих достаточного уровня подтверждения штатного выполнения функций защиты. Предметом рассмотрения являются техноло-

гии на основе криптографических преобразований. Если область приложения этих технологий является электронная подпись, то предметом рассмотрения в соответствии с законом РФ [1] является *усиленная* электронная подпись.

Возможности и преимущества использования криптографии в информационных технологиях в наиболее полной мере представляет криптографическая система с открытым ключом (КСОК), которая для шифрования и расшифрования использует *ключевую пару*: секретный ключ (private key) и открытый ключ (public key). Ключевая пара обладает свойством комплементарности, в том смысле, что оба ключа являются атрибутами одного и того же алгоритма реализации (неотъемлемая общность), но каждый из них является противоположной зависимой друг от друга функциональной сущностью. Зашифрованные данные с помощью открытого ключа можно расшифровать, только имея секретный ключ, а подпись, сделанную с помощью секретного ключа, можно подтвердить, используя соответствующий ему открытый ключ. Свойство комплементарности приобретает ещё более широкий смысл при использовании электронной подписи и построении инфраструктуры открытых ключей для поддержки юридически значимого электронного документооборота в межгосударственных информационных системах, в которых государства-участники используют свои национальные криптографические алгоритмы [13].

Ключевая пара создаётся специальными криптографическими средствами, и по сущности и назначению функционирования КСОК эта процедура не должна быть отчуждаема (свойство иммонентности) от субъекта авторизации (пользователя). При этом *ключ электронной подписи* является секретным во владении пользователя, а открытый *ключ проверки электронной подписи* по схеме «доказательство обладания секретным ключом» подтверждается *удостоверяющим центром* (УЦ) в том, что субъект авторизации владеет секретным ключом, который соответствует предъявляемому открытому ключу для издания сертификата.

*Сертификат ключа проверки электронной подписи* – электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи [1].

Технологии и процессы создания пары ключей, их использования, мониторинга жизненного цикла, исключения из употребления в системах и интегрированных информационных пространствах взаимодействия обеспечиваются созданной *инфраструктурой открытых ключей* (ИОК). Сама ИОК зависит от ряда правовых и технологических факторов и в каждом конкретном случае на уровне практического функционирования определяется её архитектурой. При этом свойство иммонентности в соответствии с законодательными нормами РФ имеет ряд особенностей при практической реализации.

Так, в *корпоративных информационных системах* (КИС) ключевые пары могут создаваться с помощью специальных средств операторами этих систем (криптоменеджерами) в соответствии с порядком использования электронной подписи пользователями в КИС или самими пользователями по соглашениям между участниками электронного взаимодействия. В этих случаях созданная ключевая пара, как правило, используется только для реализации *неквалифицированной электронной подписи*, которая не отвечает в полной мере требованиям ответственного правового регулирования информационного взаимодействия в телекоммуникационных сетях, строгого выполнения функций аутентификации и контроля доступа.

Также допускается (Ст.13 п. 7, Закон РФ №63-ФЗ от 06.04.2011) создание ключей электронных подписей и ключей проверки электронных подписей непосредственно УЦ пообращениям заявителей и оформлении соглашений, при этом УЦ несёт ответственность за обеспечение секретности ключей электронных подписей.

Если УЦ прошёл государственную *аккредитацию*, ключевая пара (ключ электронной подписи и ключ проверки электронной подписи) приобретает абсолютное право формирования *квалифицированной электронной подписи*, «собственноручно авторизованной и заверенной печатью». В этом случае сертификаты, выдаваемые УЦ, приобретают статус *квалифицированного сертификата.*

Отсюда следуют, по крайней мере, две модели организации производства и использования ключевых пар и сертификатов:

- децентрализованная модель *сетей доверия*, создаваемых на основе соглашений или доменов доверия УЦ, не прошедших аккредитацию;
- модель *квалифицированного единого пространства доверия*, в основу которой положена система аккредитованных УЦ и развёрнутая на их базе ИОК.

Понятие *единого пространства доверия* (ЕПД) до настоящего времени не определено каким-либо нормативным документом, поэтому будем считать приемлемым следующее: «ЕПД – это совокупность взаимосвязанных доверенных сервисов, развёрнутых на базе инфраструктуры открытых ключей» [11].

Под доверенными сервисами будем понимать электронные сервисы, участвующие в создании, валидации, обработке, хранении электронных сертификатов и подписей, штампов времени, электронных документов, а также обеспечивающие доставку электронных сообщений, аутентификацию и т.д. При этом средства доверенных сервисов подлежат подтверждению соответствия обязательным требованиям законодательства РФ по защите секретной информации или информации ограниченного доступа.

Использование аккредитованных УЦ обеспечивает контролируемое правовое пространство сообщества пользователей, которое технически и технологически отождествляется с системой, являющейся ИОК.

Далее будем рассматривать только модель квалифицированного пространства доверия, термин «сертификат» использовать в качестве квалифицированного сертификата.

Таким образом, инфраструктура открытых ключей (*Public Key Infrastructure PKI*) – система средств (технических, материальных, нормативно-правовых документов и т. д.), организационно-технологических решений, служб и других компонентов, в совокупности используемых для поддержки решения задач по обеспечению информационной безопасности на основе криптографической системы с открытым ключом.

Удостоверяющий центр является базовым объектом ИОК, формирующим сертификаты подчиненных центров и конечных пользователей, главным *управляющим* компонентом ИОК, который:

- является доверенной третьей стороной;
- осуществляет управление сертификатами как операционный сервер и хранилище.

Архитектура построения ИОК является атрибутом создания ИОК как системы для конкретного *интегрированного информационного пространства*.

Под интегрированным информационным пространством (ИИП) [7] будем понимать множество ИТ-систем различного назначения, их пользователей, которые владеют, накапливают и обрабатывают информационные ресурсы, представляющие взаимный интерес для решения своих задач, либо являются средой информационного взаимодействия пользователей, либо реализуют часть функционала в исполнении заданной

транзакции какой-либо сложной распределённой задачи. Очевидно, что эти системы и пользователи обеспечены в электронной среде средствами информационного взаимодействия, которые и позволяют создать ИИП.

В то же время, архитектура ИОК является неотъемлемой частью, приложением архитектурного построения ИИП. Последнее положение объясняет следственную зависимость архитектуры ИОК от архитектуры ИИП.

Архитектура ИИП, его реализация зависит от решений по всей совокупности ИТ-систем, которые, как правило, существенно распределены по территориальному признаку и авторизованы по назначению и принадлежности. Проблема наследования и решение сохранить и интегрировать разрозненные и разноплановые ИТ-системы неизбежно приводит к гетерогенности интегрированного информационного пространства и созданию дополнительных интерфейсов транссистемного взаимодействия. Создание интегрированной информационно-технологической инфраструктуры (ИИТИ) наоборот приводит к консолидации ресурсов (информационных и вычислительных) на базе создания мощных высокопроизводительных пулов технических и программных средств – центров обработки данных (ЦОД), взаимодействующих через телекоммуникационную сеть. Кроме таких крайних вариантов используется и развивается множество других архитектурных решений построения ИИП (облачные технологии [11] и сервис-ориентированная архитектура [8], создание общесистемного ПО «middleware»[7] и т.д.).

Единое пространство доверия как некоторая правовая, технологическая и техническая система, погружаемая в ИИП, зависит не только от архитектурных и технических решений построения ИИП, но, прежде всего, от модели и требований информационного взаимодействия самих субъектов, для которых ИТ-системы являются инструментом реализации бизнес-процессов.

Очевидным представляется предположение: для ИИП, в котором используется юридически значимый электронный документооборот, и при этом удалённый транссистемный доступ требует строгую аутентификацию и гарантированный контроль доступа, необходимо создавать квалифицированное ЕПД на базе ИОК.

Примерами обоснованности создания ИИП такого характера могут быть следующие объекты информатизации.

**Информатизация органов исполнительной власти.** Интегрированное информационное пространство органов исполнительной власти должно, прежде всего, обеспечить юридически значимый межведомственный документооборот через СМЭВ. В соответствии с постановлением Правительства РФ от 9 февраля 2012 г. N 111«при организации межведомственного взаимодействия, осуществляемого в электронном виде органами исполнительной власти и органами местного самоуправления при предоставлении государственных или муниципальных услуг и исполнении государственных или муниципальных функций, применяется усиленная квалифицированная электронная подпись» [3]. Следовательно, ЕПД при информатизации органов исполнительной власти – это совокупность взаимосвязанных доверенных сервисов, в которой обеспечивается признание подлинности электронной подписи при электронном взаимодействии федеральных, региональных, муниципальных органов исполнительной власти, иных государственных органов, внебюджетных фондов, организаций и физических лиц. Соответственно могут быть выделены компоненты ИИП муниципального, регионального, федерального уровня со своими доменами доверия.

**Информатизация Корпорации.** Понятие Корпорации[1] как объединения компаний и их бизнеса связано с сущностью корпоративного управления, которое регулирует деловые, имущественные, информационные взаимоотношения между входящими в корпорацию компаниями, их владельцами, а также обеспечивает согласование целей заинтересованных сторон, обеспечивая эффективное функционирование компаний.

Головная структура управления Корпорации (Администрация), являясь объединяющим юридическим лицом и обеспечивая общесистемный менеджмент, может функционировать независимо от входящих компаний (самоуправляемо) при любых выбранных моделях объединения.

Компании Корпорации, при автоматизации бизнес-процессов и информатизации-управления, как правило, имеют свои информационно-технологические ресурсы (информационные ресурсы, ИТ-инфраструктуры и функциональные ИТ-приложения – автоматизированные системы и комплексы, в том числе наследуемые при вхождении в Корпорацию).

Они могут формировать свои сообщества (домены) пользователей, которые для информационного взаимодействия между собой и использования криптографии в целях обеспечения информационной безопасности требуют защищённого механизма. Но управление Корпорацией, менеджмент всей её деятельности требует консолидации определённых информационных ресурсов, их операционной интеграции в единой *корпоративной информационной системе*, которая является в ведении Администрации, со своим доменом доверия.

Кроме того, ИИП Корпорации не изолированно по отношению к внешним информационным системам, относящимся к объектам, которые не входят в Корпорацию. В том числе и в части межгосударственных информационных отношений.

Широкое использование электронного документооборота в управлении, в договорных отношениях, в инновационном и инвестиционном развитии, межкорпоративные и международные связи документированного характера, безусловно, требует юридически значимой электронной подписи. Не исключается строгая аутентификация при удалённом транссистемном информационном взаимодействии.

Так как ИИП является территориально распределённым образованием, архитектура ИОК, как правило, базируется на *системе удостоверяющих центров* (СУЦ).

Возможные пути построения архитектуры ИОК для интегрированного информационного пространства рассматриваются в данной работе как ***задача анализа***.

## Анализ вариантов архитектурного построения ИОК

Архитектура ИОК определяет структуру отношений доверия между удостоверяющими центрами и другими субъектами инфраструктуры. По архитектуре ИОК делятся на разные типы в зависимости от следующих характеристик [14]:

- количества удостоверяющих центров, которые непосредственно доверяют друг другу;
- структуры отношений доверия между удостоверяющими центрами;
- способа добавления в инфраструктуру нового УЦ;

[1]Корпорация – объединение производственных, проектных, торгово-сбытовых, финансовых предприятий и организаций для совместной хозяйственной деятельности, уменьшения возможного риска при осуществлении капиталоемких направлений промышленной и коммерческой деятельности за счет концентрации капитала, централизации функций обеспечения ресурсами, сбыта продукции, овладения новыми рынками, реализации более экономически целесообразной стратегии развития входящих в корпорацию хозяйственных единиц (http://forexom.com. Главная. Термины. Экономические термины и понятия. Бизнес. Корпорация)

– сложности построения и проверки пути сертификации;
– серьезности последствий компрометации удостоверяющих центров.

Эти характеристики являются качественными критериями выбора архитектуры ИОК при проектировании.

Любая архитектура имеет свой формализованный, разработанный на текущий срез действительности, метод, который связан с аппаратом реализации. По существу аппаратной платформой для реализации архитектуры ИОК являются два метода: иерархическая и сетевая структуры.

Но далее архитектура ИОК определяется выбранной моделью доверия удостоверяющих центров, поддерживающих функционирование ИТ-систем и информационное взаимодействие пользователей через системы, и следующей из модели организационно-системной структурой СУЦ [10].

В системе удостоверяющих центров могут быть выделены УЦ по признаку доверия:

– *корневые центры сертификации* – удостоверяющие центры, которым доверяет изначально всё сообщество пользователей, руководствуясь совместной политикой доверия, реализуемой предустановленными настройками хранилища сертификатов;
– *доверенные центры сертификации* – центры сертификации, которым доверяют владельцы сертификатов, образуя свои домены доверия.

Система доверия в СУЦ определяется путём доверия. *Путь доверия* – цепочка документов, которая позволяет удостовериться, что предъявленный сертификат был выдан доверенным центром [9]. Последним звеном в этой цепочке является предъявленный сертификат, начальным звеном – сертификат корневого доверенного центра сертификации, а промежуточными звеном – сертификаты, выданные промежуточными центрами сертификации. При потере доверия к начальному звену цепочки (корневому центру сертификации) теряется доверие ко всей цепочке, т.е. ко всем выданным данным центром сертификатам и к предъявленному в том числе.

Сама модель доверия СУЦ должна ориентироваться на архитектуру ИИП, определяемую способами интеграции ИТ-систем и ИТ-инфраструктур входящих субъектов информационного взаимодействия. ИОК ИИП может включать в себя составляющие её ИОК, между которыми созданы интерфейсы доверия.

Для определения наиболее эффективной модели доверия с позиций ранее предложенных критериев выбора архитектуры ИОК для ИИП рассмотрим и проанализируем основные модели доверия и соответствующие им возможные архитектуры построения ИОК.

**Простая модель доверия.** Суть данной модели заключается в том, что все пользователи доверяют одному УЦ и используют при защищённом информационном взаимодействии и в технологиях с криптографическими средствами сертификаты только этого УЦ, образуя единый домен доверия. По существу модельной платформой реализации простой модели доверия является вырожденная иерархическая структура, в которой УЦ – корень дерева отношений, все пользователи образуют простые ветви связей.

Простой модели доверия соответствует простая архитектура ИОК, в которой образуются прямые отношения через единое УЦ и простые пути проверки сертификации. Если злоумышленник выдаст себя за УЦ, это потребует перевыпуска всех выписанных сертификатов и далее возвращения в режим штатной работы.

**Иерархическая модель доверия**. Структурная схема иерархической модели доверия ИОК представлена на рис. 1.

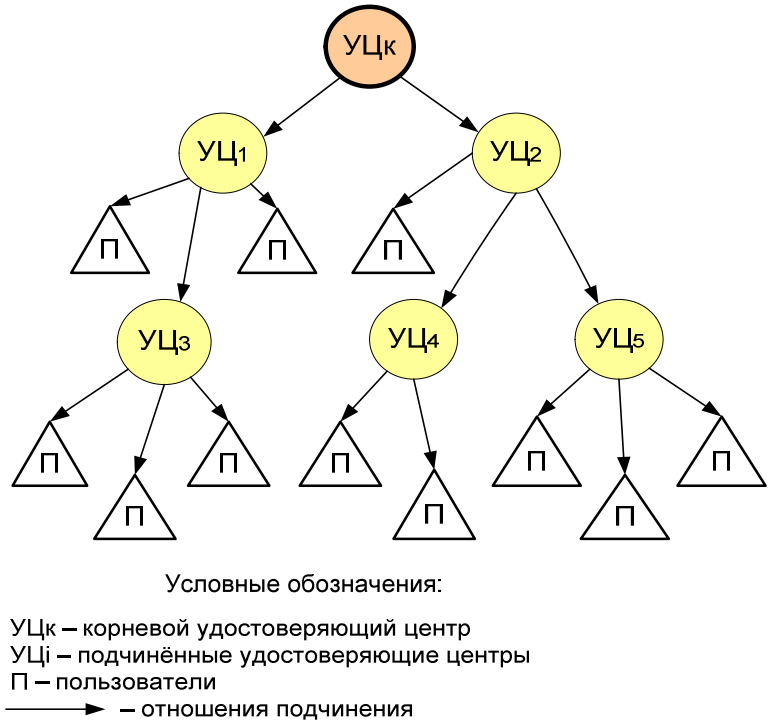


*Рис. 1. Иерархическая модель доверия*

Иерархическая модель доверия определяет организационно-системное построение СУЦ в виде иерархической структуры. Иерархическая структура СУЦ – платформа для построения архитектуры ИОК. Во главе всей структуры СУЦ стоит один УЦк (корневой центр сертификации), которому доверяет всё сообщество пользователей. Кроме головного УЦ в структуре присутствуют другие УЦ, которые подчиняются вышестоящему, и каждому из них, в свою очередь, приписаны определённое подмножество пользователей или нижестоящие УЦ.

Цепочки сертификатов С пользователей (пути доверия) определяются структурной схемой модели. Например, цепочки сертификатов для пользователей, которые поддерживаются УЦ3 (П3), следующие:

П3 →Ск > С2 > С4 > П4;П3 →Ск > С2 > С5 > П5

Достоинствами иерархической модели доверия являются:

– соответствие модели иерархической природе управления объектами, которые участвуют в информационном взаимодействии;
– простота и однозначность построения цепочек доверия.

Среди недостатков следует выделить сложность реконфигурирования, внесения изменений в структуру такой системы, что не относится, тем не менее, к созданию новых ветвей.

В ИОК иерархической архитектуры, являющейся производной иерархической модели доверия, если злоумышленник выдал себя за какое-то УЦ, система продолжает работать без этого УЦ. После восстановления его штатной работоспособности, он снова включается в структуру СУЦ.

Обобщая отличительные свойства этой модели доверия, можно сделать вывод, что она привлекательна для использования в качестве базовой в интегрированном информационном пространстве с централизованным управлением ИИП, территориально распределёнными объектами информационного взаимодействия и трансситемным доступом.

**Браузерная модель доверия**. Модельной платформой *браузерной модели* доверия также является иерархическая структура. Однако её отличие от классической иерархической модели доверия определяется двумя факторами. В-первых, эта модель может включать несколько корневых УЦ со своими деревьями подчинённых УЦ и прикреплённых к ним подмножеств пользователей, образующих сложный домен. Во-вторых, вводится технологическая надстройка в целях упрощения определения путей доверия при взаимодействии между пользователями из различных доменов, при которой в цепочку сертификации на некоторых уровнях могут быть включены не сертификаты, а списки доверенных сертификатов, подписанные уполномоченным удостоверяющим центром (CTL–*Certificate Trust List*). Данная возможность добавляет универсальность и гибкость масштабирования для объектов информационного взаимодействия и их систем, построенных на основе иерархической модели доверия.

Структурная схема браузерной модели доверия ИОК представлена на рис. 2.

Примеры цепочек сертификатов С для пользователей:

- цепочка П1 при проверке сертификата П2: П1 → $С_{к1}$>$CTL_1$> $С_{к2}$> $С_{21}$>П2;
- цепочка П3 при проверке сертификата П4: П3 → $С_{к2}$> $С_{22}$>$CTL_{22}$>$С_{к3}$>П4;
- цепочка П4 при проверке сертификата П3: П4 → $С_{к3}$>$CTL_3$>$CTL_{22}$> $С_{22}$> П3.

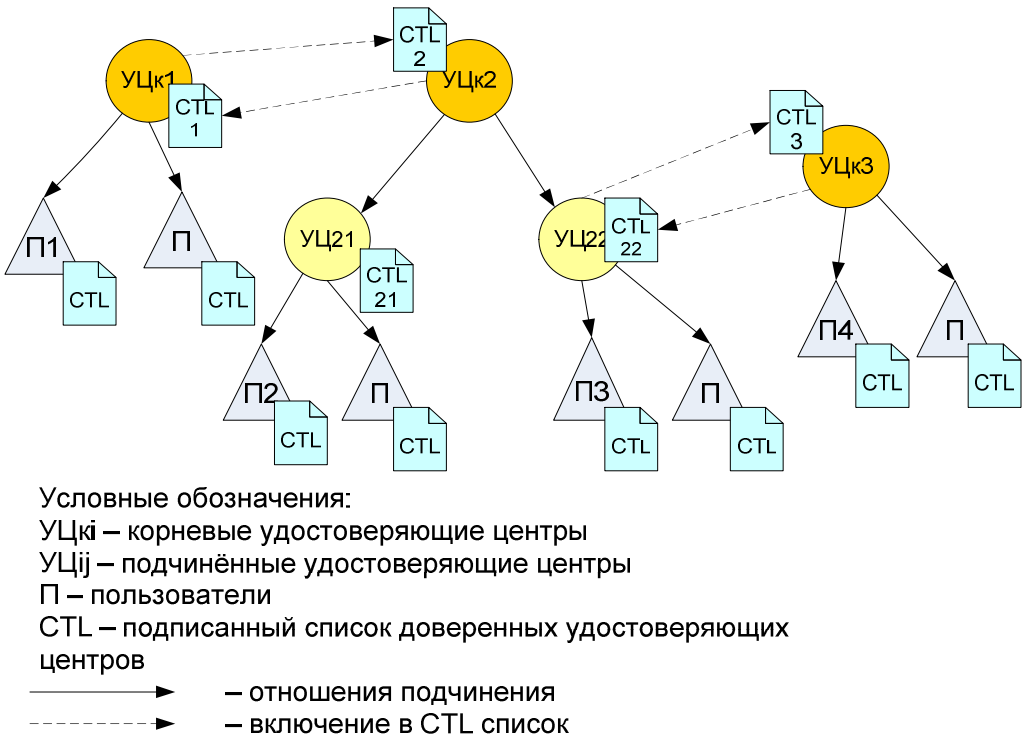


*Рис. 2. Браузерная модель доверия*

Достоинствами браузерной модели доверия являются:

– простота включения новых элементов, не входящих в иерархические отношения подчиненности;

– возможность установления отношений доверия между удостоверяющими центрами разного уровня;

- возможность реализации на основе некоторых платформ УЦ подписанных CTL-списков, которые таким образом становятся юридически значимыми электронными документами;
- возможность организации гибких взаимосвязей, которые могут быть изменены (разорваны) без ущерба для поддерживаемых ИОК.

Данная модель практически не имеет ограничений для её использования в интегрированном информационном пространстве любой архитектуры. Она может быть использована также для установления отношений доверия с удостоверяющими центрами, не входящими в ИОК ИИП.

**Сетевая модель доверия** ИОК строится как сеть доверительных отношений. Сеть образуется множеством УЦ, которые, предоставляя сервисы ИОК, связаны одноранговыми (равноправными) отношениями и образуют свой домен доверия. Головной УЦ (корневой центр сертификации) не выделяется. СУЦ представляет собой сетевую структуру объектов (УЦ) с равноправными отношениями.

Соответственно ИОК имеет сетевую архитектуру построения. В этой архитектуре все УЦ доверяют всем УЦ, с которыми установлены двусторонние отношения доверия, а каждый пользователь доверяет только тому УЦ, который выдал ему сертификат. Для установления и подтверждения двусторонних отношений доверия УЦ выпускают сертификаты друг для друга.

В данную архитектуру ИОК легко добавляется новый УЦ. Для этого ему нужно обменяться сертификатами, по крайней мере, с одним из входящих в сеть УЦ. Сетевая модель доверия обуславливает наиболее сложное построение цепочек сертификации (путей доверия), но придаёт ИОК большую гибкость, так как пользователи могут иметь многочисленные пункты доверия.

**Компрометация** одного УЦ не отражается на сетевой ИОК в целом: удостоверяющие центры, которые выпустили сертификаты для скомпрометированного УЦ, просто аннулируются, тем самым удаляя из инфраструктуры ненадежный УЦ. В результате не нарушается работа пользователей, связанных с другими удостоверяющими центрами. Компрометация ИОК приводит к двум возможным последствиям – сворачивается работа одного УЦ вместе с его сообществом пользователей или ИОК распадается на несколько инфраструктур, если становятся ненадежными несколькоУЦ. Восстановление штатного режима функционирования в ИОК с сетевой архитектурой происходит проще, чем в ИОК с иерархической архитектурой, так как компрометация, как правило, затрагивает меньшее количество пользователей.

Построить путь доверия в сети достаточно сложно, поскольку этот процесс не детерминирован, имеются многочисленные варианты формирования цепи сертификатов. Это может привести к построению правильного пути либо завести в тупик. По этой причине валидация пути доверия часто выполняется одновременно с его построением, частью этого процесса является удаление неверных ветвей. Для построения правильного пути используется несколько дополнительных полей сертификатов.

Достоинством сетевой модели доверия является простота включения новых элементов, не входящих в иерархические отношения подчиненности.

Основным недостатком является сложность и неоднозначность цепочек доверия сертификатов (путей доверия).

Обобщая отличительные черты этой модели доверия можно заключить, что она достаточно сложна для использования в качестве базовой при построенииархитектуры ИОК, обеспечивающей квалифицированную электронную подпись, так как её недостатки существенно усложняют процесс валидации и контролируемого управления си-

стемой. Однако она может быть эффективно использована для реализации неквалифицированной электронной подписи, особенно в корпоративных информационных системах (КИС), когда круг пользователей однозначно определён и информационное взаимодействие осуществляется на основании договорных отношений или через криптоменеджеров систем. В этом случае часто не выпускаются даже сертификаты ключа проверки электронной подписи, и сеть может строиться практически без УЦ.

**Кросс-сертифицированная модель доверия**. Структурная схема кросс-сертифицированной модели доверия ИОК представлена на рис. 3.

Данная модель может рассматриваться как смешанный вид иерархической и сетевой моделей. Соответственно архитектура ИОК может рассматриваться как смешанный вид иерархической и сетевой архитектур. Модель включает в себя локальные иерархические системы ИОК, поддерживающие предприятие или куст предприятий (например, региональный). Между предприятиями имеет место информационное взаимодействие, что требует организации соответствующего интерфейсного сервиса ИОК. Образуется связующая межкустовая система ИОК на основе кросс-сертифицированных связей между корневыми центрами локальных систем ИОК. В ИОК кросс-сертифицированной архитектуры самая сложная система цепочек сертификации (путей доверия).

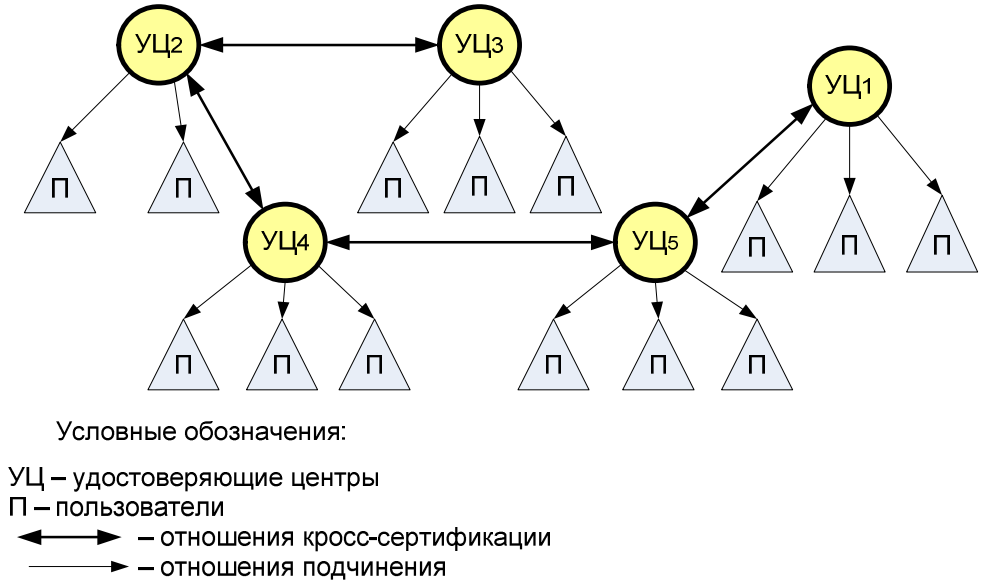


*Рис. 3. Кросс-сертифицированная модель доверия*

Цепочки сертификатов С для пользователей, которые поддерживаются УЦ2 (П2), следующие:

П2 →$C_2$> $C_3$> П3; П2 →$C_2$> $C_4$> $C_5$ >$C_1$>П1

**Мостовая модель доверия**. Структурная схема мостовой модели доверия ИОК представлена на рис. 4.

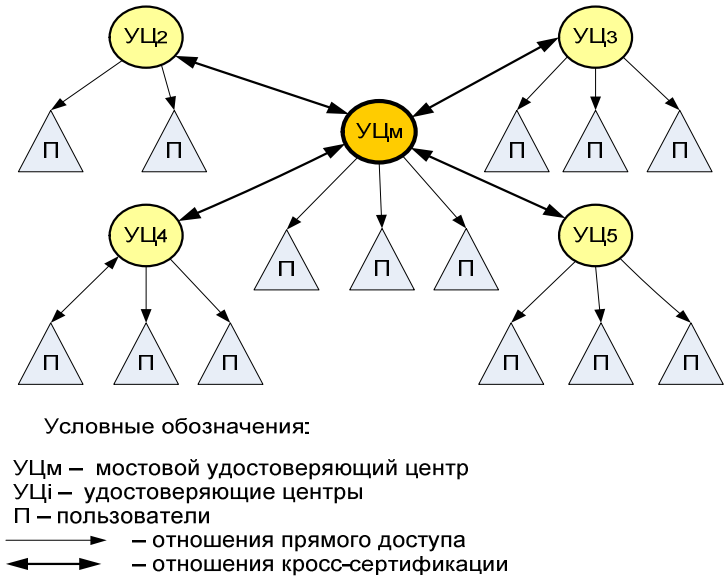


*Рис. 4. Мостовая модель доверия*

Архитектура ИОК, основанная на мостовой модели доверия, предназначена для того, чтобы убрать недостатки сложного процесса сертификации в кросс-сертифицированной ИОК. В данном случае все предприятия (или кусты предприятий) локальных систем ИОК доверяют не какому-то одному или нескольким корневым центрам локальных ИОК, а одному определённому мостовому корневому УЦ, который является практически их общим головным УЦ. Он может не быть основным пунктом доверия, однако, выступает в роли посредника между другими УЦ.

Достоинствами мостовой модели доверия являются:

– простота включения новых элементов, не входящих в иерархические отношения подчиненности;
– возможность организации гибких взаимосвязей, которые могут быть изменены (разорваны) без ущерба для поддерживаемых ИОК.

Недостатки:

– возможность организации связей только между корневыми УЦ;
– установление отношений доверия между УЦ разных уровней подчиненности невозможно.

Цепочки сертификатов С для пользователей, которые поддерживаются УЦ2 (П2), следующие:

П2 →$C_2$> См>$C_3$>П3;П2 →$C_2$> См> $C_5$ > П5; П2 →$C_2$> См> $C_4$> П5.

Следует отметить, что проведение процедуры кросс-сертификации должно обязательно сопровождаться приведением в соответствие политики сертификации объединяемых УЦ.

Обобщая отличительные черты мостовой модели доверия, можно заключить, что она может быть использована как дополняющая иерархическую модель для включения в домен доверия других УЦ, не входящих в систему ИОК ИИП.

## Обоснование применения

Предлагаемые модели доверия являются базой системного проектирования архитектуры ИОК.

Результаты рассмотрения и анализа моделей доверия и соответствующих им архитектур построения ИОК позволяют сделать вывод, что наиболее эффективной для создания внутренней архитектуры ИОК ИИП с обозначенными характеристиками является иерархическая модель доверия, которая отвечает требованиям для структур, интегрируемых в Корпорацию или взаимодействующих как региональный куст. Для обеспечения взаимодействия с внешними доменами доверия целесообразно использовать мостовую модель доверия, учитывая при этом, что кросс-сертификация (в том числе с мостовыми УЦ) возможна только на уровне корневых УЦ. При необходимости установления отношений доверия на уровне подчиненных УЦ, либо на разных уровнях, целесообразно использовать браузерную модель.

В соответствии с этими выводами при проектировании ИОК для построения архитектуры ИОК ИИП должны быть выработаны организационно-технологические и технические решения, обеспечивающие реализацию в ИИП следующих основных целей:

- формирование правовой, организационной, технологической и технической основы реализации механизмов ЭП, обеспечивающих юридическую значимость электронных документов при информационном взаимодействии между автоматизированными информационными системами, входящими в ИИП, а также, при необходимости, с внешними информационными системами, в том числе и для организации международного информационного взаимодействия;
- повышение эффективности бизнес-процессов предприятий и структур субъектов, связанных с информационным обменом, за счёт использования механизмов ЭП;
- повышение безопасности информационных ресурсов и процессов их обработкипутём использования криптографических средств при поддержке ИОК.

## СПИСОК ЛИТЕРАТУРЫ:


1. Федеральный закон от 06. 04.2011 г. № 63-ФЗ «Об электронной подписи».
2. Федеральный закон от 20.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями на 21 июля 2014 года).
3. Постановление Правительства РФ от 9 февраля 2012 г. N 111 "Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи".
4. Приказ ФСБ России от 9 февраля 2005 года № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»,зарегистрирован в Минюсте РФ.
5. ГОСТ Р 51275-2006. НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Защита информации. ОБЪЕКТ ИНФОРМАТИЗАЦИИ. ФАКТОРЫ, ВОЗДЕЙСТВУЮЩИЕ НА ИНФОРМАЦИЮ. Общие положения
6. ГОСТ Р 51583. Порядок создания автоматизированных систем в защищенном исполнении.
7. Некрасова Е. Единство непохожих: интегрированное информационное пространство. 29 июня 2004 года, http://www.computtera.ru/
8. Назаренко А. Корпоративное информационное пространство: задачи и реализация. “Rational Enterprise Management”, 23.06.2008, http://www.intertrust.ru/press_center/articls/view/
9. Система оперативной проверки статуса сертификатов CoreStreetRTCValidationAuthority. Логическое и функциональное описание.
10. Полянская О. Ю., Горбатов В. С. Инфраструктуры открытых ключей. Учебное пособие. М, 2007. ISBN 978-5-94774-602-0
11. Сабанов А.Г. Аутентификация как составляющая единого пространства доверия // Электросвязь. № 8, 2012. ISBN 0013-5771.
12. Максимов Н.В., Алёшин Л.И. Информационные технологии. Учебное пособие. М.: Московский международный институт эконометрики, информатики, финансов и права, 2004.
13. Вышенский С.В., Григорьев П.В., Дубенская Ю.Ю. Инфраструктура открытых ключей с комплементарной криптографией. IT-ПАРК // Вестниксвязи. №9, 2007.

14. Полянская О.Ю. Основные понятия и типы архитектуры PKI. НОУ ИНТУИТ. Национальный исследовательский ядерный университет «МИФИ», http:www.intuit.ru/studies/courses/4647/110/info

## REFERENCES:

1. Federal law dated 06. 04.2011, No. 63-FZ"On electronic signature".
2. Federal law dated 20.07.2006, No. 149-FZ "On information, information technologies and information protection" (as amended on 21 July 2014).
3. Resolution of the Government of the Russian Federation dated February 9, 2012 N 111 "On electronic signature used by the bodies of Executive power and bodies of local self-government in the organization of electronic interaction between them, on the order of its use, and the establishment of requirements to ensure interoperability of electronic signatures"
4. Order of the Federal security service of Russia dated 9 February 2005 No. 66 "On approval of the Regulations on the development, production, implementation and maintenance of encryption (cryptographic) means of information protection (Regulation CCS-2005)", registered in Ministry of justice of the Russian Federation.
5. GOST R 51275-2006. NATIONAL STANDARD OF THE RUSSIAN FEDERATION. Protection of information. THE OBJECT INFORMATION. FACTORS AFFECTING INFORMATION. General provisions
6. GOST R 51583. The creation of automated systems in a secure execution.
7. Nekrasov E. The unity of the different: integrated information space. June 29, 2004, http://www.computtera.ru/
8. Nazarenko A. Corporate information space: challenges and implementation. “Rational Enterprise Management”, 23.06.2008, http://www.intertrust.ru/press_center/articls/view/
9. System operational verification of certificate status CoreStreet RTC Validation Authority. Logical and functional description.
10. Polyanskaya O. Y., Gorbatov V. S. Public key infrastructure. Textbook, Moscow, 2007. ISBN 978-5-94774-602-0
11. Sabans A. Authentication as part of the same space of trust //Telecommunications. № 8, 2012. ISBN 0013-5771.
12. Maksimov N. In., Aleshin, L. I. Information technology. Training manual. M.: Moscow international Institute of econometrics, Informatics, Finance and law, 2004.
13. Vyshenskii SV Grigoriev PV, Dubenskaya J.J. A public key infrastructure with a complementary cryptography. IT-park // Herald of communication. №9, 2007.
14. Polyanskaya O. Y. Basic concepts and types of PKI architecture. KNOW INTUITIVE. National research nuclear University "MEPhI", http:www.intuit.ru/studies/courses/4647/110/info 13. 2007.