Дмитрий А. Мельников[1], Юрий Ф. Релеев[2], Леонид Д. Кварацхелия[3]
[1]Федеральный исследовательский центр «Информатика и управление» РАН,
ул. Вавилова, 44, корп. 2, Москва, 119333, Россия
[2,3]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: mda-17@yandex.ru, https://orcid.org/0000-0003-4515-9712
[2]e-mail: r3le@yandex.ru, https://orcid.org/0000-0001-9352-541X
[3] e-mail: kvarleon1997@gmail.ru, https://orcid.org/0000-0002-9199-3903

МОДЕЛЬ ДОВЕРИЯ ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

DOI: http://dx.doi.org/10.26583/bit.2020.1.04

Аннотация. В статье представлено исследование современных моделей доверия на основе инфраструктуры открытых криптографических ключей (*Public Key Infrastructure* – PKI), целью которого является разработка российской национальной модели доверия. Для достижения поставленной цели была обоснована необходимость создания национальной инфраструктуры доверия в условиях перехода к цифровой экономике. Вместе с тем, в работе проведён анализ текущего состояния российской PKI, которое характеризуется отсутствием единой структуры удостоверяющих центров (УЦ) и единого федерального органа регулирования в области обеспечения криптографическими ключами (сертификатами открытых ключей). Анализ зарубежных PKI-моделей доверия позволил сделать вывод о том, что ни одна из таких моделей не может быть эталонной, и не может быть реализована в Российской Федерации. Основу предлагаемой модели составляет концепция распределённой системы центров подтверждения подлинности, которая имеет иерархическую структуру и позволит объединить все государственные и частные УЦ в единую динамическую систему, способную удовлетворить самые разнообразные потребности цифровой экономики и граждан Российской Федерации по обеспечению информационной безопасности. Реализация разработанной авторами модели доверия позволит, в первую очередь, предотвратить многие киберпреступления и попытки нанесения финансово-экономического ущерба субъектам информационного взаимодействия.
Ключевые слова: инфраструктура открытых ключей, доверие, целостность, неотказуемость, удостоверяющий центр, центр подтверждения подлинности, сертификат открытого ключа, электронная подпись.
Для цитирования: МЕЛЬНИКОВ, Дмитрий А.; РЕЛЕЕВ, Юрий Ф.; КВАРАЦХЕЛИЯ, Леонид Д. МОДЕЛЬ ДОВЕРИЯ ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ. Безопасность информационных технологий, [S.l.], v. 27, n. 2, p. 47-64, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1270>. Дата доступа: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.04.

Dmitry A. Melnikov[1], Yury F. Releev[2], Leonid D. Kvaratskheliya[3]
[1]Federal Research Center "Computer Science and Control" of Russian Academy of Sciences,
Vavilov Str., 44/2, Moscow, 119333, Russia
[2,3]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115409, Russia
[1] e-mail: mda-17@yandex.ru, https://orcid.org/0000-0003-4515-9712
[2] e-mail: r3le@yandex.ru, https://orcid.org/0000-0001-9352-541X
[3] e-mail: kvarleon1997@gmail.ru, https://orcid.org/0000-0002-9199-3903

Trust Model for the Russian Federation Digital Economy

DOI: http://dx.doi.org/10.26583/bit.2020.1.04

Abstract. The paper presents a study of modern trust models based on the Public Key Infrastructure (PKI) infrastructure, the purpose of which is to develop a Russian national trust model. To meet this goal, the necessity of creating a national infrastructure of trust in the transition to a digital economy was

substantiated. At the same time, the analysis of the current state of the Russian PKI, which is characterized by the absence of a unified structure of the certification authorities (CA) and a unified federal regulatory authority in the field of cryptographic key management (public key certificates), is carried out. An analysis of foreign PKI models of trust allowed us to conclude that none of these models can be used as reference and implemented in the Russian Federation. The basis of the proposed model is the concept of a distributed system of the validation authorities, which has a hierarchical structure and will allow combining all public and private CAs into a single dynamic system that can meet the most diverse needs of the digital economy and citizens of the Russian Federation to manage information security. The implementation of the trust model developed by the authors will allow, first of all, preventing many cybercrimes and attempts to cause financial and economic damage on the subjects of information interaction.

Keywords: public key infrastructure, trust, integrity, nonrepudiation, certificate authority, validation authority, public key certificate, digital signature.

For citation: MELNIKOV, Dmitry A.; RELEEV, Yury F.; KVARATSKHELIYA, Leonid D. Trust Model for the Russian Federation Digital Economy. IT Security (Russia), [S.l.], v. 27, n. 2, p. 47-64, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1270>. Date accessed: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.04.

Введение

В современных информационно-технологических системах (ИТС) самого широкого спектра назначения для обеспечения конфиденциальности, целостности, неотказуемости и установления авторства используются методы, способы и средства криптографической защиты информации. Наиболее характерным примером такого использования является электронная (цифровая) подпись (ЭП/ЭЦП) [1]. Применение ЭП позволяет проверить отсутствие искажения информации (целостность) принадлежность подписи владельцу сертификата ключа подписи (авторство), и в случае успешной проверки проверить факт подписания электронного документа (неотказуемость). При этом, в отличие от обычных рукописных подписей, её невозможно подделать, не получив закрытый ключ автора подписи.

Задача распределения и обмена ключами между участниками защищённого взаимодействия в рамках ИТС решается на основе асимметричных криптографических систем. Однако, при использовании таких криптосистем существует проблема, которая заключается в доверии к тому или иному открытому ключу. Что «мешает» злоумышленнику сформировать собственную пару ключей и выдавать себя за другого владельца? Решение этой проблемы выходит за рамки теоретической криптографии и относится к сфере организации системы обеспечения криптоключами, в частности, созданию инфраструктуры PKI [1–3]. Идея состоит в том, что есть третья сторона, которой доверяют взаимодействующие стороны. Доверенная третья сторона (ДТС) осуществляет привязку (*binding*) открытых ключей к уникальным идентификаторам (или параметрам подлинности (ПРП), *identity*) физических и юридических лиц (организаций). Привязка осуществляется путём регистрации клиентов (формирование их цифрового образа, т.е. ПРП) и выдачи им сертификатов ($СЕРТ_{ОК}$) удостоверяющим центром (УЦ, *certification authority* – CA), в которых параметр подлинности криптографически связан (с помощью ЭП УЦ) с открытым ключом. В дальнейшем при взаимодействии принадлежность открытого ключа конкретному клиенту может быть проверена в УЦ ДТС. В Российской Федерации УЦ выполняют все перечисленные задачи – регистрацию, выдачу $СЕРТ_{ОК}$ и их проверку [3].

Тем не менее, даже после внедрения PKI, проблема доверия остается нерешённой [4]. В общем случае неизвестно, насколько доверенными можно считать УЦ и субъекты, имеющие их $СЕРТ_{ОК}$. Каждый УЦ должен иметь политику сертификации, в которой

отражается порядок выдачи $СЕРТ_{ОК}$ и процедуры проверки физических и юридических лиц, получающих $СЕРТ_{ОК}$. Однако, с точки зрения неквалифицированного в соответствующей предметной области пользователя, проверка политики сертификации на её полноту и корректность является проблематичной. Ещё сложнее проверка того, что УЦ действительно реализует свою политику и является надёжным. В работе описывается способ решения данных проблем – формирование структуры доверия на основе PKI. В первом разделе обосновывается необходимость такой структуры. Во втором разделе приводятся обзор зарубежного опыта и анализ существующих моделей доверия на основе PKI. В третьем разделе обосновывается выбор и приводится описание предлагаемой национальной структуры модели доверия для цифровой экономики Российской Федерации.

1. Обоснование необходимости национальной инфраструктуры доверия

1.2 Определение доверия

Ключевым фактором обеспечения ИБ при взаимодействии субъектов (людей, организаций, ИТС) является доверие – взаимосвязь между двумя сторонами, называемыми доверяющей стороной (доверитель) и доверенной стороной (доверяемый). Доверитель проводит оценку и принимает решение о доверии, основываясь на личном опыте и полученной информации, то есть он является в некотором смысле «мыслящим» субъектом. Доверяемая же сторона может быть физическим лицом и организацией, а также, например, информацией, криптографическим ключом.

У доверительной связи есть своя «область действия», обозначающая цель её применения. Например, «быть доверенным» относительно предоставляемых услуг и товаров, или же «быть подлинным» пользователем ИТС. Так как существует множество различных определений термина «доверие», не всегда понятно, что подразумевается под ним в том или ином контексте. В силу этого, всегда необходимо уточнять и определять значение термина в конкретной ИТС.

1.3 Доверие в PKI

Как доверие к оценке, так и доверие к принятому решению означают положительную убеждённость в чём-либо, от чего (в перспективе или на текущий момент) зависит благосостояние доверителя. Доверие к оценке наиболее естественно измеряется как дискретный или непрерывный уровень надёжности (убеждённости), тогда как доверие к принятому решению лучше представить в виде выбора между двумя вариантами. Одним из возможных решений проблемы доверия в PKI является отражение рассчитанного каким-либо образом уровня доверия в $СЕРТ_{ОК}$ [3]. Однако, реализация такого подхода на практике весьма проблематична – пользователи неохотно будут приобретать $СЕРТ_{ОК}$ с низким уровнем доверия.

УЦ выдают $СЕРТ_{ОК}$ в соответствии с политикой сертификации, описывающей требования к получателям, и детальное описание процедур проверки получателей. Доверяющая сторона должна оценивать достаточность этих требований и проверок. Также, доверяющая сторона должна быть убеждена в том, что УЦ действительно следует этой политике. Даже подлинный $СЕРТ_{ОК}$ не может дать полную гарантию того, что открытый ключ является подлинным – злоумышленник может каким-либо образом заставить УЦ выпустить $СЕРТ_{ОК}$ с поддельным именем. С этой угрозой связано множество компьютерных инцидентов и атак [5].

В масштабах Российской Федерации проблема доверия в инфраструктуре PKI существенно усложняется. Так, согласно перечню аккредитованных УЦ Министерства

связи и массовых телекоммуникаций, по состоянию на 19.12.2019 аккредитованы 502 УЦ[1]. На сегодняшний день злоумышленники активно пользуются несовершенством (а точнее, отсутствием) национальной структуры доверия к PKI. Возникло несколько прецедентов неправомерного использования УЦ электронных подписей застрахованных лиц и оформления документов без участия гражданина[2]. Например, таким образом была осуществлена незаконная продажа квартиры без участия собственника[3]. Ряд УЦ предлагают услугу дистанционного выпуска СЕРТ$_{ОК}$ без личного контакта заявителя и центра регистрации (ЦР). Фактически, это облегчает задачу злоумышленников по получению поддельного СЕРТ$_{ОК}$, что может трактоваться как нарушение действующего законодательства[4]. Для предотвращения возникновения подобных проблем и развития цифровой экономики в России необходимо формирование структуры национальной структуры доверия PKI.

2. Анализ существующих моделей доверия на основе PKI

2.1 Издание сертификатов и подтверждении подлинности

СЕРТ$_{ОК}$ показывает степень доверия между УЦ и владельцем открытого ключа. Зачастую, эта степень отражает лишь то, что владелец открытого ключа правомочно владеет уникальным именем, указанным в СЕРТ$_{ОК}$. Помимо этого, в СЕРТ$_{ОК}$ может быть указана и другая информация.

Доверие к параметрам, указанным в СЕРТ$_{ОК}$, формируется доверяющей стороной из доверия к УЦ. Связанная таким образом последовательность СЕРТ$_{ОК}$ называется *цепочкой доверия*. А совокупность взаимосвязанных СЕРТ$_{ОК}$ называется *сетью доверия*. Формально, любую сеть доверия, основанную на СЕРТ$_{ОК}$ можно назвать PKI, однако на практике используются лишь определённые модели.

Структура доверия при создании СЕРТ$_{ОК}$ представлена на рис. 1. При этом подразумевается, что ЦР является составной частью УЦ.

В нижней части рисунка отражены процедуры формирования доверия. Доверительная связь, отмеченная индексом 1, показывает, что корневой УЦ безусловно и полностью доверяет подлинности своей собственной пары открытого и закрытого ключей. Необходимо отметить, что подлинность корневого открытого ключа невозможно подтвердить соответствующим СЕРТ$_{ОК}$, так как эта проверка выполняется тем же самым ключом (если бы ключ сам мог подтверждать свою подлинность, то в инфраструктуре не было бы смысла). Таким образом, доверие к корневой ключевой паре следует из внешних по отношению к PKI-инфраструктуре источников. Индекс 2 указывает на формирование самоподписанного СЕРТ$_{ОК}$. Индексы 3–6 отражают формирование прямого доверия привязке ключей путём выпуска СЕРТ$_{ОК}$ промежуточного УЦ и пользователя. При этом

[1]Перечень аккредитованных удостоверяющих центров (по состоянию на 19.12.2019) сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, URL: https://digital.gov.ru/ru/activity/govservices/certification_authority/ (дата обращения: 22.12.2019).

[2]Счётная палата Российской Федерации Бюллетень Счетной палаты №12 (декабрь) 2017 г. Пресс-центр счетной палаты Российской Федерации, URL: http://audit.gov.ru/activities/bulleten/bulletin-of-the-accounting-chamber-12-2017.php (дата обращения: 15.12.2019).

[3]Аракелян Е., Хожателова Ю. Новый вид мошенничества: Оставили без квартиры, подделав электронную подпись. 2019 // Комсомольская правда, URL: https://www.kp.ru/daily/26979/4038526/ (дата обращения: 15.12.2019).

[4]Письмо Министерства связи и массовых коммуникаций РФ от 9 октября 2017 г. № П15-1-200-24056 «О разъяснении некоторых положений Федерального закона «Об электронной подписи».

УЦ выпускают СЕРТ$_{ОК}$ согласно своим политикам сертификации, и этим подтверждают подлинность соответствующих привязок.

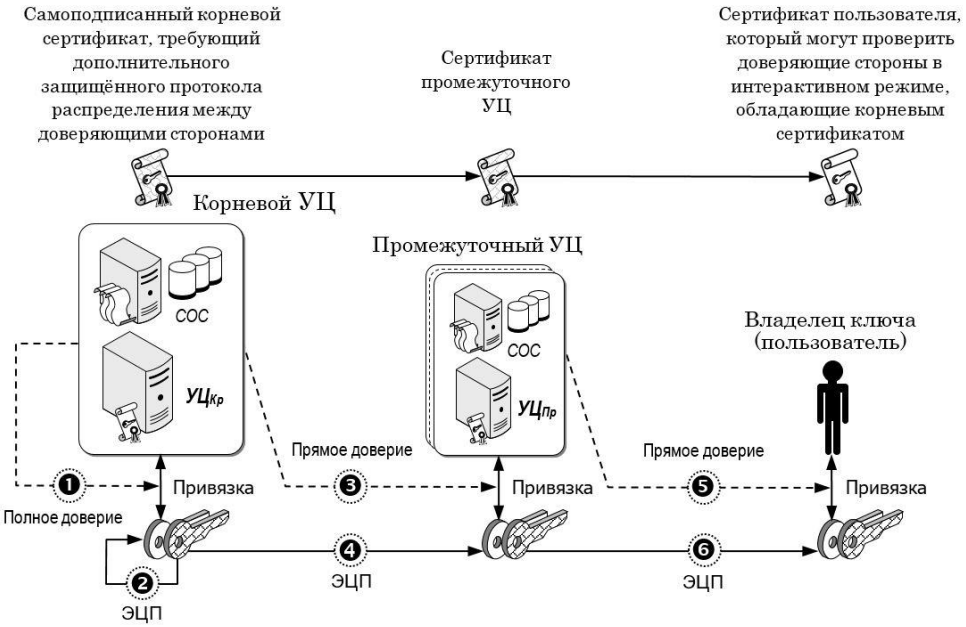

Рис. 1. Структура доверия при создании СЕРТ$_{ОК}$ (СОС[5] – список отозванных СЕРТ$_{ОК}$)
(Fig. 1. The trust structure for a issuing certificates (CRL – certificate revocation list))

На рис. 2 приведена структура доверия при подтверждении подлинности (ПП) СЕРТ$_{ОК}$. Если доверяющая сторона имеет прямое доверие (индекс 1) к корневому УЦ, то с помощью его СЕРТ$_{ОК}$ она может сформировать косвенное доверие (индекс 4) к открытому ключу контрагента. Способы формирования доверительных взаимосвязей определяются соответствующими политиками сертификации УЦ. Процедура проверки подлинности, как правило, осуществляется путём проверки электронной подписи: СЕРТ$_{ОК}$ пользователя подписан ключом промежуточного УЦ, а его СЕРТ$_{ОК}$, в свою очередь, подписан ключом корневого УЦ, к которому доверяющая сторона имеет прямое доверие.

2.2 Одиночная иерархическая PKI

Это – наиболее часто встречающийся вид PKI. В данном случае все пользователи доверяют одному корневому УЦ, которому подчиняются остальные нижестоящие УЦ (рис. 3). Преимущество такой структуры заключается в том, что необходимо распространить между доверяющими сторонами лишь один открытый ключ корневого УЦ по стороннему защищенному каналу связи. Имея этот открытый ключ, и СЕРТ$_{ОК}$ всех промежуточных УЦ, доверяющая сторона может проверить конкретную цепочку доверия от СЕРТ$_{ОК}$ пользователя к СЕРТ$_{ОК}$ УЦ, и сформировать косвенное доверие к открытому ключу пользователя.

Корневой УЦ должен быть доверенным в представлении общепризнанной организации, компетентность которой в вопросах регистрации пользователей и проверке открытых ключей подтверждается, например, аккредитацией.

[5]RFC 5280. IETF, May 2008; RFC 6818. IETF, January 2013.

Рис. 2. Структура доверия при подтверждении подлинности СЕРТ$_{ОК}$
(Fig. 2. The trust structure for a validating the certificates)

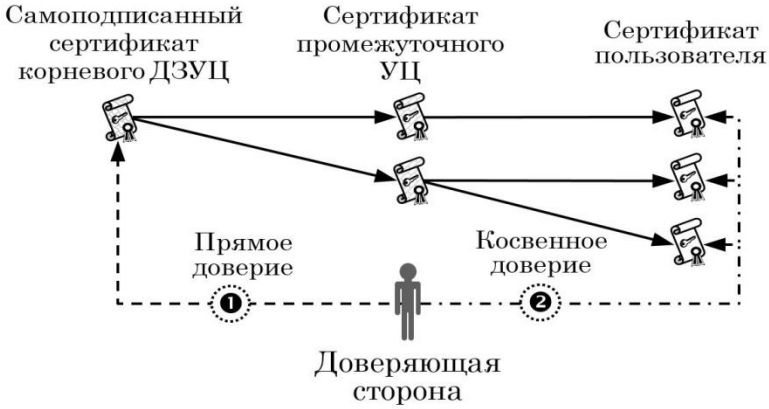

Рис. 3. Структура доверия в одиночной иерархической PKI
(Fig. 3. The trust structure in a single hierarchic PKI)

2.3 Многоиерархическая PKI

Отличием многоиерархической инфраструктуры является то, что СЕРТ$_{ОК}$ пользователей могут принадлежать к различным PKI-иерархиям. Для того чтобы доверяющая сторона могла сформировать доверие к СЕРТ$_{ОК}$ пользователя из любой иерархии, все корневые УЦ должны быть доверенными «замыкающими» (*anchor*) УЦ (ДЗУЦ), как показано на рисунке 4. У доверяющей стороны должно быть прямое доверие к ним.

При такой структуре доверия пропорционально возрастает нагрузка на проверяющую сторону, которая должна получить все СЕРТ$_{ОК}$ корневых УЦ по дополнительным защищённым каналом связи. Это – следствие того, что данная структура плохо масштабируется. Проблема усугубляется ещё и тем, что множество СЕРТ$_{ОК}$ корневых УЦ постоянно изменяется.

Одной из реализаций такой модели можно считать инфраструктуру, реализованную в современных Web-обозревателях. В ней СЕРТ$_{ОК}$ корневых УЦ встраиваются в комплекс программного обеспечения (КПО) Web-клиента и регулярно обновляются. Такое

встраивание СЕРТ$_{ОК}$ позволяет осуществлять автоматическое подтверждение подлинности открытых ключей, используемых для информационного взаимодействия с помощью TLS-протокола (*Transport Layer Security* [7]), и проверки ЭП прикладных КПО.

У такой модели есть и серьёзные уязвимости. Защищённость PKI Web-обозревателей определяется защищённостью наиболее уязвимой отдельной PKI, входящей в её состав. Защищённость последней определяется наиболее уязвимым УЦ такой инфраструктуры. Следовательно, чем больше корневых СЕРТ$_{ОК}$ и промежуточных УЦ, тем менее защищённой становится вся инфраструктура Web-обозревателей. Существует множество способов злонамеренного выпуска фальшивых СЕРТ$_{ОК}$ [8,9]:

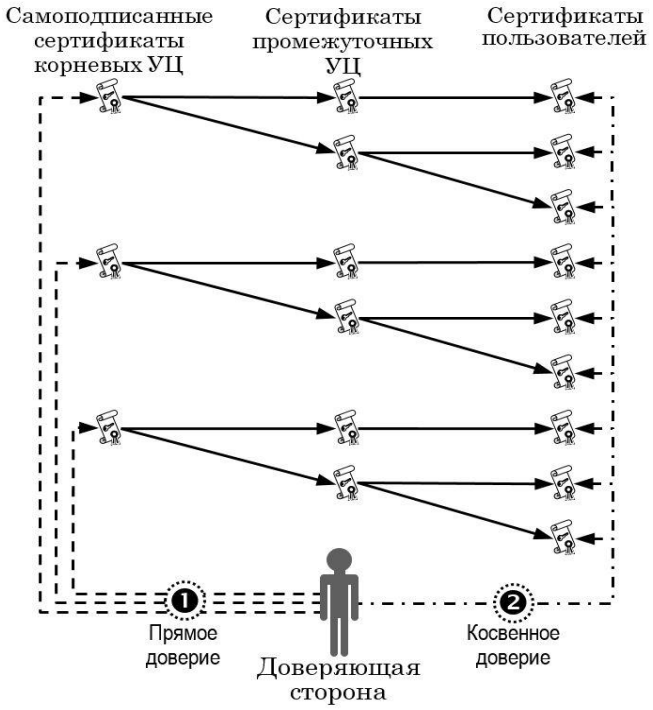

Рис. 4. Структура доверия в многоиерархической PKI
(Fig. 4. The trust structure in a multiple hierarchic PKI)

1. **Атака на УЦ**. В результате таких атак злоумышленники создают ложные СЕРТ$_{ОК}$ известных компаний и используют их для обмана пользователей, перехвата и анализа трафика. Реализации таких атак различны: от внедрения и работы вредоносного КПО в ИТС самих УЦ, до обмана с помощью фальшивых документов в ходе проверки ПРП при регистрации транзакций.

2. **Давление, шантаж УЦ**. Существует высокая вероятность того, что некоторые тайваньские компании-разработчики КПО (Realtek и JMicron) под давлением использовали свои подлинные СЕРТ$_{ОК}$ для подписи вредоносного КПО Win32/Stuxnet [10]. Эти подписи позволили внедрить вредоносный КПО в промышленных ИТС ряда предприятий атомной отрасли Ирана.

3. **Нелегальные УЦ**. С технической точки зрения, любой УЦ в рамках Web-PKI способен сформировать фиктивные СЕРТ$_{ОК}$ и ЭП. Нелегальные УЦ или недобросовестные сотрудники легальных УЦ могут получить большую выгоду, выпуская фальшивые СЕРТ$_{ОК}$, так как подобные СЕРТ$_{ОК}$ будут автоматически признаваться всеми известными операционными системами.

Многие люди произвольно запрашивают выпуск для них различных СЕРТ$_{ОК}$, причём на основе самостоятельных случайных решений, то есть имеет место быть избираемое прямое доверие (рис. 5).

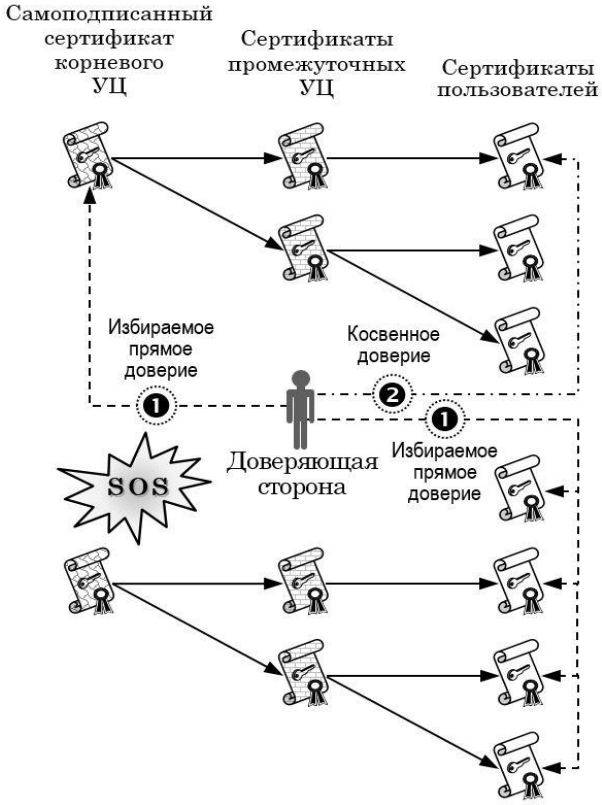

Рис. 5. Структура избираемого прямого доверия
(Fig. 5. The discretionary direct trust structure)

В таком случае игнорируется не только требование наличия защищенных дополнительных каналов получения СЕРТ$_{ОК}$ корневых УЦ, но и надёжность корневого УЦ как ДЗУЦ [11]. Данная модель применима в ситуациях с небольшими рисками в некритичных прикладных ИТС. Например, возникают случаи, когда подлинность СЕРТ$_{ОК}$ не может быть подтверждена в силу того, что отсутствует корневой СЕРТ$_{ОК}$, или же, когда невозможно соблюсти политику ПП в силу того, что срок действия с СЕРТ$_{ОК}$ корневого УЦ истёк. Однако, таким же образом принимаются решения, когда возможен реальный ущерб, например, при установке прикладных КПО. В таких случаях нельзя исходить из одного лишь удобства и низкой стоимости.

Необходимо отметить, что подобная проблема может быть присуща всем моделям доверия PKI, ведь доверяющая сторона из соображений удобства зачастую просто игнорирует факт существования корневых СЕРТ$_{ОК}$. И даже если доверяющая сторона знает о них, она далеко не всегда обладает достаточными компетенциями и информацией необходимой для принятия решения о доверии таким СЕРТ$_{ОК}$.

2.4 Взаимная сертификация нескольких корневых УЦ

Для того чтобы снизить нагрузку на доверяющие стороны можно позволить корневым УЦ осуществлять взаимную (обоюдную) сертификацию (*cross certification*). В такой структуре доверия для подтверждения подлинности доверяющей стороне

необходим всего лишь один СЕРТ$_{ОК}$ любого из корневых УЦ. На рис.6 показано, как доверяющая сторона формирует доверие к открытым ключам пользователей множества PKI-иерархий с взаимно сертифицированными корневыми УЦ.

Недостатком такой модели является увеличение нагрузки на сами корневые УЦ, так как каждый из них должен провести процедуру сертификации со всеми другими корневыми УЦ такой иерархии. В соответствии с теоремой Эйлера (лемма «о рукопожатиях») [12], необходимое число всех таких процедур составляет:

$$\frac{n*(n-1)}{2}, \tag{1}$$

где n – число отдельных корневых УЦ.

Для каждой такой процедуры необходимо согласие корневых УЦ и изменения и дополнение их политики, поэтому данная модель плохо масштабируется и применяется лишь в очень ограниченных случаях.

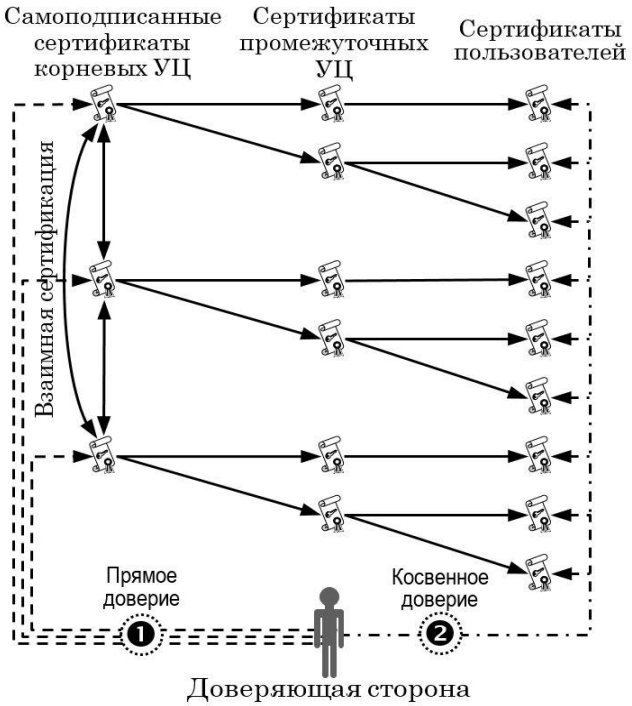

Рис. 6. Структура доверия при взаимной сертификации
(Fig. 6. The cross-certification trust structure)

2.5 Использование связующего УЦ

В качестве улучшения предыдущей модели можно использовать связующий (*bridge*) УЦ между множеством корневых УЦ (рис. 7). Преимущества такого решения в том, что доверяющим сторонам необходимо получить лишь один корневой СЕРТ$_{ОК}$ по дополнительному защищённому каналу, и что каждому корневому УЦ необходима взаимная сертификация лишь с одним связующим УЦ.

Как и в предыдущем случае, недостатком является необходимость согласия всех сторон на взаимную сертификацию со связующим УЦ, и наоборот, согласие связующего УЦ на сертификацию со всеми корневыми УЦ.

2.6 PKI-инфраструктура с центром подтверждения подлинности

С точки зрения доверяющей стороны наиболее проблематичными задачами являются безопасное получение СЕРТ$_{ОК}$ корневого УЦ по дополнительным каналам и ПП СЕРТ$_{ОК}$ пользователей. Возможно выделение этих функций и включение в модель нового участника, берущего на себя такие обязательства, ещё одного «якоря» доверия (ДЗУЦ) – центра ПП (ЦПП, *validation authority* – VA). Такая модель доверия приведена на рис. 8.

При этом ЦПП не обязательно должен выполнять функции УЦ – одна организация может представлять либо функции УЦ, либо ЦПП, либо выполнять обе функции одновременно. Для такой ПП необходимо защищённое соединение между доверяющей стороной и ЦПП, а для этого, в свою очередь, необходим безопасный обмен криптографическими ключами по дополнительному каналу. Процедуры сертификации и ПП отдельны друг от друга, поэтому защищённый канал необязательно должен основываться на асимметричной криптографии.

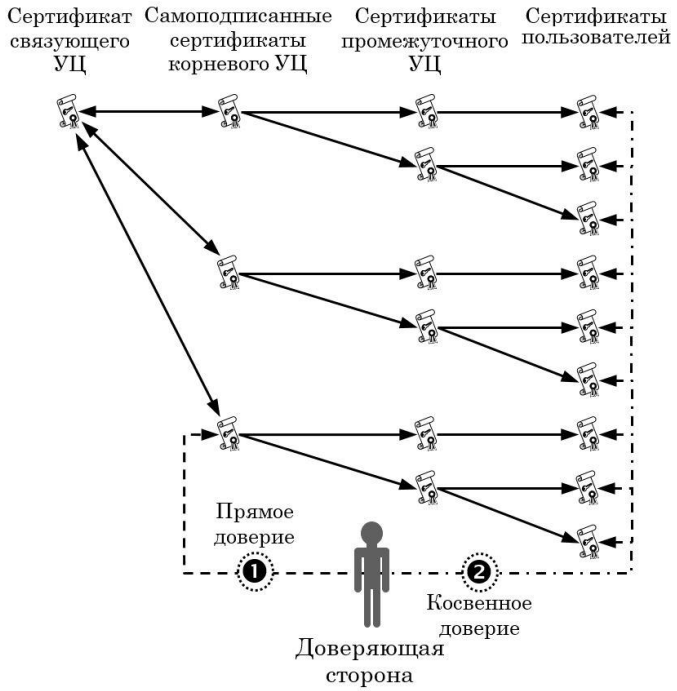

Рис. 7. Структура доверия на основе связующего УЦ
(Fig. 7. The bridge certification authority trust structure)

В такой модели существуют два важных аспекта ИБ: доверяющая сторона должна иметь возможность аутентифицировать ЦПП, чтобы доверять процедуре ПП СЕРТ$_{ОК}$. И напротив, ЦПП может аутентифицировать доверяющую сторону для предоставления ей доступа к процедуре ПП.

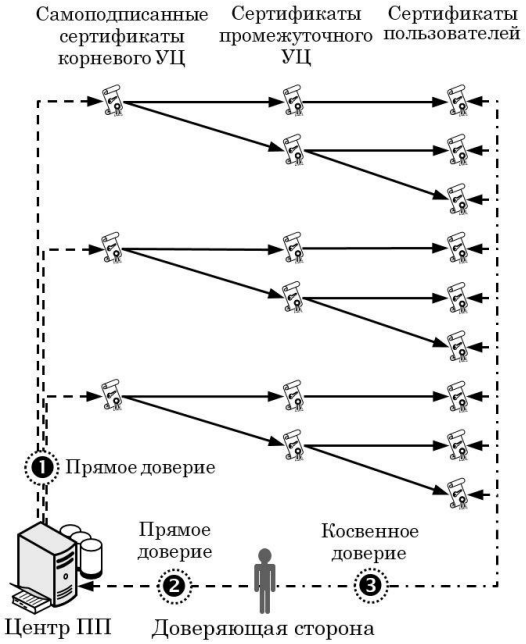

Рис. 8. Структура доверия на основе многоиерархической PKI с ЦПП
(Fig. 8. The validation authority trust structure)

Модель с ЦПП снимает нагрузку с доверяющих сторон и отражает одну из главных тенденций в PKI-технологии [13]. Так как ЦПП независимы от УЦ, то с помощью них возможно соединение множества независимых PKI-инфраструктур.

3. Обоснование выбора и разработка национальной структуры модели доверия

3.1 Зарубежный опыт формирования национальных структур моделей доверия

США

Развитие национальной PKI в США было обусловлено принятием двух важнейших законодательных актов:

1. HIPAA[6] – закон о мобильности и подотчётности в здравоохранении принятый в 1996 году, требовавший в том числе создания национальных стандартов для электронного документооборота в здравоохранении и общих идентификаторов для поставщиков, медицинского страхования, и работодателей;

2. GPEA[7] – закон о прекращении бумажного документооборота в правительстве, принятый в 1998 году. Закон требовал, чтобы за 5 лет система предоставления информации (услуг) гражданам федеральными органами и службами, а также все процедуры были переведены в электронный формат. Также закон устанавливал юридический статус ЭП, и обязывал ведомства внедрить процедуры электронной аутентификации.

[6]The Health Insurance Portability and Accountability Act of 1996. HIPAA; Pub. L. 104–191, 110 Stat. 1936, enacted August 21, 1996.
[7]The Government Paperwork Elimination Act. GPEA, Pub. L. 105-277, Approved October 21, 1998.

Структура модели доверия федеральной PKI (FPKI) включает в себя федеральный связующий УЦ (ФСУЦ). Основной его задачей является создание цепочки доверия как между федеральными ведомствами, объединяя их в одну государственную сеть доверия, так и создание связи с негосударственной сетью доверия [14, 15]. Очевидно, что как УЦ федеральных ведомств, так и частные УЦ должны удовлетворять определенным требованиям для того, чтобы провести взаимную сертификацию с ФСУЦ (рис. 9)[8].

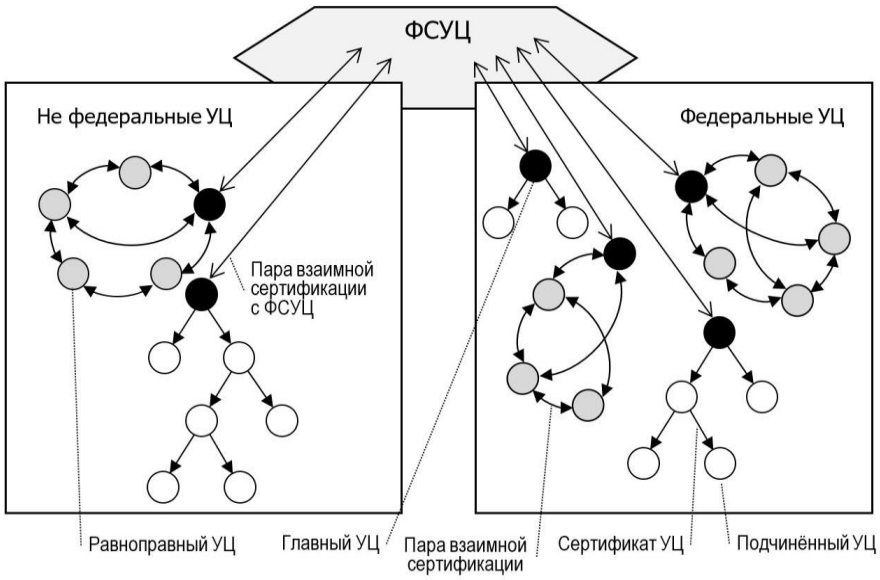

Рис. 9. Взаимодействие между федеральной и частной PKI в США
(Fig. 9. Interoperation between federal and non-federal PKIs)

Необходимо отметить, что ФСУЦ не является корневым для всех остальных, он не выпускает СЕРТ$_{ОК}$ и не является ДТС, а выступает лишь в качестве «моста доверия» между различными сетями доверия.

Европейский союз (ЕС)

В Европейском союзе развитие PKI связано с директивой 1999/93/ЕС «Об использовании электронных подписей в электронных контрактах в рамках Евросоюза»[9]. Важным отличием от модели США является то, что в ЕС существует множество языков государственного уровня. Это потребовало введения новых элементов в инфраструктуру – национальных ЦПП и реестра состояния доверенных служб (РСДС)[10].

Сложностью в создании такой инфраструктуры является то, что прикладные ИТС, которые обрабатывают ЭП, должны устанавливать взаимосвязь с каждым УЦ на территории ЕС, а их насчитывается несколько сотен. В связи с этим такие системы должны обеспечивать:

1. подтверждение подлинности СЕРТ$_{ОК}$ напрямую с выдавшим его УЦ (когда он известен);

[8] National Institute of Standards and Technology. Introduction to Public Key Technology and the Federal PKI Infrastructure. NIST Special Publication 800-32, 26 February 2001.
[9] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
[10] IDABC. Study on European Federated Validation Service (EFVS): Analysis and Assessment. Common Solution Model. Contract № 1, Framework contract ENTR/05/58-SECURITY, Specific contract № 14. September 2009.

2. поиск адреса ЦПП который может обработать СЕРТ$_{ОК}$, который выдан УЦ, обозначенном в СЕРТ$_{ОК}$;

3. отправка запроса в известный ЦПП, выполняющий функцию перенаправления. Этот ЦПП получит адрес целевого ЦПП и отправит запрос ему. Перенаправляющим ЦПП может быть, как коммерческий, так и государственный ЦПП на уровне отдельной страны или всего Евросоюза.

Эти требования привели к следующей модели системы обслуживания СЕРТ$_{ОК}$ (рис. 10). Данная структура основывается на использовании национальных ЦПП. В первом случае система передает запросы в ЦПП напрямую (модели 3 и 4), во втором случае (модель 1) запросы передаются на Web-сервер, который связывается с ЦПП. В последнем случае всё происходит через инфраструктуру ЭП для соединения с ЦПП (модель 2).

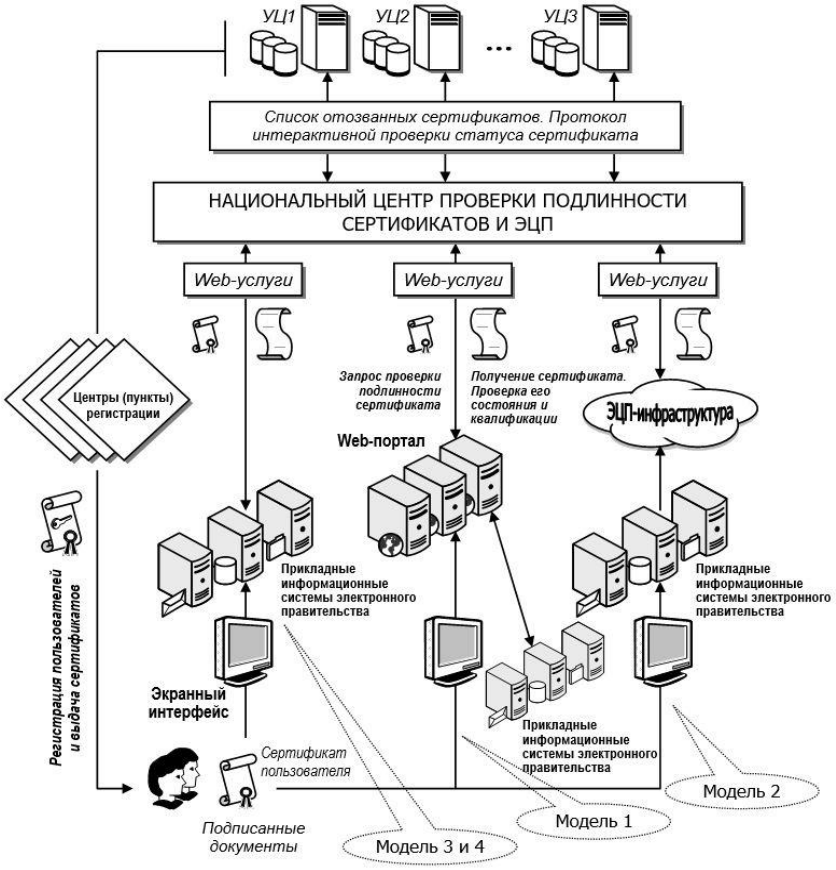

Рис. 10. Модель подтверждения подлинности СЕРТ$_{ОК}$ в режиме «одного окна»
(Fig. 10. The certificate validation by VA («one-stop-shop» mode))

В общем виде модель ПП в ЕС приведена на рис. 11. Отправитель, находящийся в стране $\mathcal{A}$, подписывает документа и отправляет его получателю в стране $\mathcal{B}$ (1). Получатель обращается в национальный ЦПП своей страны (2). ЦПП в стране $\mathcal{B}$ обращается в общеевропейский оператор РСДС (*PPRS*) и получает адрес целевого ЦПП в стране $\mathcal{A}$, который «отвечает» за УЦ, выпустивший СЕРТ$_{ОК}$ отправителя (3). После чего ЦПП в стране $\mathcal{B}$ отправляет запрос ЦПП в стране $\mathcal{A}$ на ПП СЕРТ$_{ОК}$ отправителя (4). ЦПП

в стране $\mathcal{A}$ осуществляет ПП с помощью соответствующего УЦ (5) и возвращает результат промежуточному ЦПП (6), который транслирует ответ получателю.

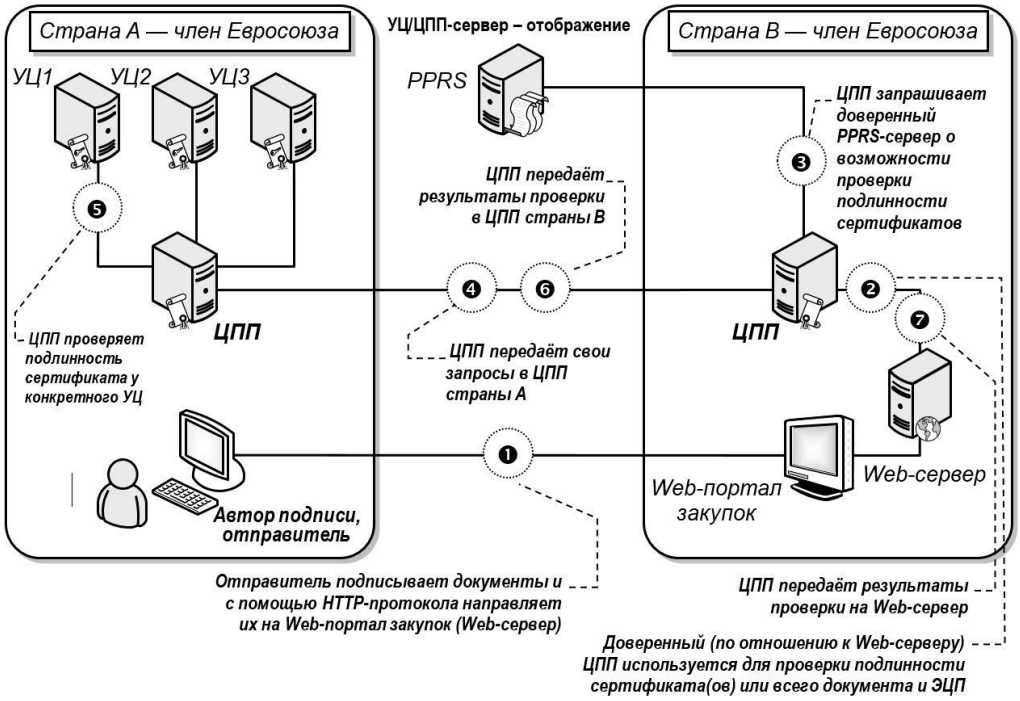

Рис. 11. Процедура ПП в модели ЕС
(Fig. 11. The certificate validation procedure in the EU model)

3.2 Современное состояние PKI в Российской Федерации

Согласно постановлению Правительства РФ №976 от 22.11.2011 федеральным органом исполнительной власти, уполномоченным в сфере использования ЭП является Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь). Правовой статус ЭП определен в Федеральном законе №63 ФЗ от 6 апреля 2011 г. «Об электронной подписи».

На сегодняшний день существует порядка 500 аккредитованных Минкомсвязью[11], и большое количество не аккредитованных УЦ, обслуживающих конкретные организации. В 2004 году была разработана Федеральная целевая программа «Электронная Россия» и созданы Общероссийский государственный информационный центр, головной УЦ РФ, текущая структура доверия включает в себя головной (корневой) Федеральный УЦ и несколько УЦ первого уровня, обслуживающих государственные организации. Все аккредитованные УЦ также включены в структуру доверия, а их первичные СЕРТ$_{ОК}$ должны издаваться головным УЦ. Однако, в настоящее время существующая в России структура доверия не способна удовлетворить потребности цифровой экономики и должна совершенствоваться и развиваться в рамках Национального проекта «Цифровая экономика Российской федерации»[12].

[11]Перечень аккредитованных удостоверяющих центров (по состоянию на 19.12.2019) // сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, URL: https://digital.gov.ru/ru/activity/govservices/certification_authority/ (дата обращения: 22.12.2019).
[12]Национальная проект «Цифровая экономика Российской Федерации». Паспорт проекта утверждён протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. N 7.

3.3 Предлагаемая модель

В [16] была впервые предложена национальная система ПП СЕРТ$_{ОК}$ и проверки ЭП на основе PKI. На рис. 12 представлена национальная структура доверия на основе PKI. В этой структуре выстраивание иерархий частных УЦ или их взаимная сертификация необязательны, что означает неприкосновенность частного бизнеса. Обязательным условием функционирования национальной структуры доверия – это согласие каждого частного УЦ на подключение к Национальной системе ЦПП (НСЦПП), а также их аккредитация.

Аналогично западноевропейской модели, при ПП СЕРТ$_{ОК}$ и проверке ЭП в рамках одного муниципального образования (или региона) не будет необходимости перенаправления запроса на более высокий уровень, что снизит общую нагрузку на систему. Такая многоуровневая иерархия позволяет освободить корневые УЦ и ЦПП от необходимости вести постоянно изменяющийся перечень всех частных УЦ.

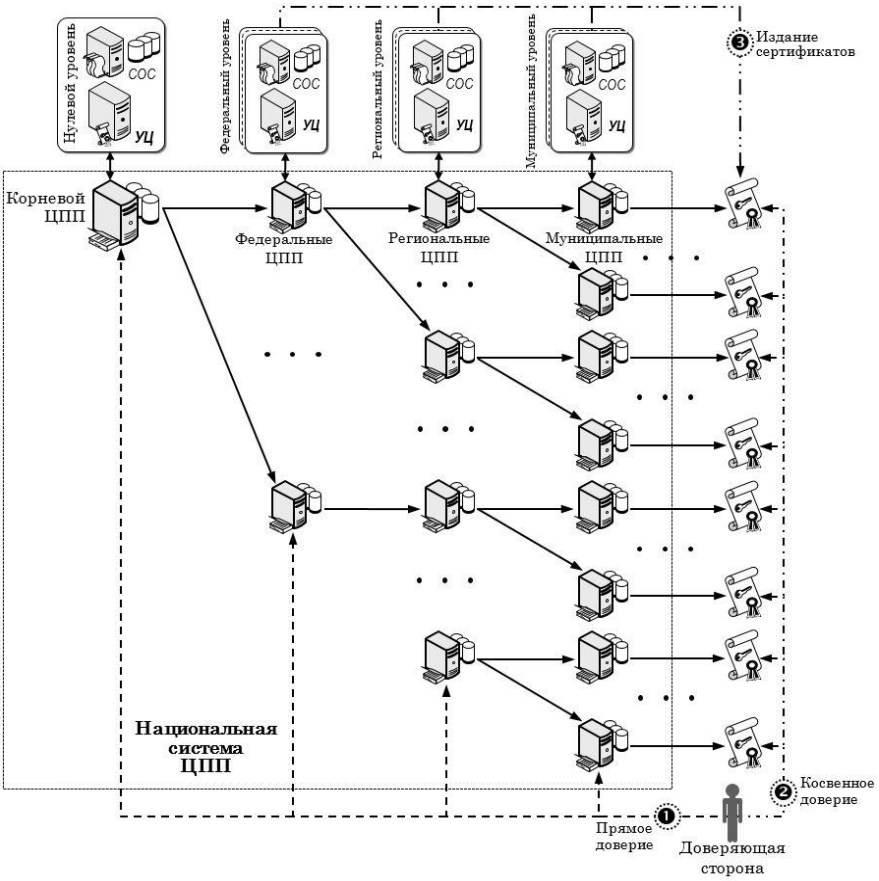

Рис. 12. Модель национальной структуры доверия
(Fig. 12. The national trust structure model)

НСЦПП – это ядро всей национальной структуры доверия, ПП СЕРТ$_{ОК}$ и проверки ЭП, которая представляет собой иерархическую и распределённую структуру ЦПП, включающую несколько уровней ЦПП (федеральный, региональный и муниципальный). С точки зрения государственного управления, НСЦПП представляет собой государственную «надстройку», которая осуществляет регулирование в области ЭП и обеспечивает доверие и функционирование соответствующих государственных и

коммерческих транзакций в различных отраслях цифровой экономики, включая частно-государственное партнёрство.

На федеральном уровне НСЦПП возможно создание отдельных ведомственных и отраслевых ЦПП иерархий и соответствующих сети доверия, которые могут быть организованы не только по географическому принципу, но и по ведомственному, экономическому или иному принципу. При этом частные УЦ разделяются по территориальному признаку. Каждый частный УЦ будет добровольно входить в реестр муниципального или регионального ЦПП. Таким образом, национальная структура доверия Российской Федерации будет самостоятельным сегментом критической информационной инфраструктуры, который потребует создания необходимых систем обеспечения безопасности.

Заключение

Несовершенство PKI в Российской Федерации, т.е. фактическое отсутствие национальной структуры доверия, является источником проблем использования ЭП пользователями, в частности, узковедомственное использование ЭП, и повышает вероятность возникновения различных инцидентов и противоправных действий со стороны злоумышленников в информационно-технологической сфере. При развитии таких инфраструктур основное внимание уделялось модернизации технологической базы и ИТС, а не семантическим аспектам доверия. А ведь именно из-за неправильной трактовки $СЕРТ_{ОК}$ и ПРП происходит большая часть преступлений в данной сфере, особенно когда дело касается глобальной Интернет-сети.

Существует множество теоретических моделей структур доверия на основе PKI, так или иначе нашедших применение на практике. Несмотря на то, что в последние годы предпринимается множество попыток по развитию и регулированию PKI, было введено предоставление многих государственных услуг в электронной форме и т.д., анализ зарубежных национальных структур доверия показал, что текущая ситуация в области PKI в Российской Федерации далека от совершенства.

Предлагаемая национальная модель доверия объединяет все существующие УЦ страны в единую национальную структуру доверия на основе PKI, иерархия которой позволит существенно снизить накладные расходы электронного документооборота, как на государственном, так и на коммерческом уровне, и создаст благоприятные условия для дальнейшего развития цифровой экономики Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ:

1. Горбатов В.С., Полянская О.Ю. Основы технологии PKI. М.: Горячая Линия – Телеком., 2004. – 248 с. ISBN 5-93517-154-6. URL: https://elibrary.ru/item.asp?id=19582746 (дата обращения: 15.01.2020).
2. Раджендран В., "Эволюция экосистемы PKI", 2017 Международная конференция по инфраструктуре открытых ключей и ее приложениям (PKIA), Бангалор, 2017. С. 9–10. DOI: 10.1109/PKIA.2017.8278951. URL: https://ieeexplore.ieee.org/abstract/document/8278951 (дата обращения: 20.01.2020).
3. Мельников Д.А. и др. Практическая реализация различных моделей инфраструктуры открытых ключей. Безопасность информационных технологий, V. 23, № 1. стр. 100-114, 2016. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/38 (дата обращения: 07.03.2020).
4. Kaimov A.T., Kaimov A.T. Public key infrastructure: a survey. – 2018. URL: https://repository.kbtu.kz/bitstream/handle/123456789/75/Вестник%201-2018%20для%20библиотеки-92-99.pdf?sequence=1&isAllowed=y (дата обращения: 09.03.2020).
5. Radif M. J. Vulnerability and Exploitation of Digital Certificates, 2018 Al-Mansour International Conference on New Trends in Computing, Communication, and Information Technology (NTCCIT). IEEE, 2018. P. 88–92. URL: https://ieeexplore.ieee.org/abstract/document/8681179 (дата обращения: 25.01.2020).
6. Kohlas R., Jonczy J., and Haenni R. A Trust Evaluation Method Based on Logic and Probability Theory. In The Proceedings of the Joint iTrust and PST Conferences on Privacy, Trust Management and SecURLty

(IFIPTM 2008), Trondheim, June 2008. DOI:10.1007/978-0-387-09428-1_2. URL: https://link.springer.com/chapter/10.1007/978-0-387-09428-1_2 (дата обращения: 07.03.2020).
7. Rescorla E. RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3. IETF, August 2018. DOI: RFC 8446. URL: https://www.hjp.at/doc/rfc/rfc8446.html (дата обращения: 05.03.2020).
8. Hayes J.M. The problem with multiple roots in web browsers – certificate masquerading. In 7th Workshop on Enabling Technologies, Infrastructure for Collaborative Enterprises (WETICE ’98). CAUSA Proceedings. P. 306–313. IEEE Computer Society, Palo Alto, 17–19 June 1998. DOI: 10.1109/ENABL.1998.725710. URL: https://ieeexplore.ieee.org/abstract/document/725710 (дата обращения: 01.03.2020).
9. Soghoian C. and Stamm S. Certified lies: Detecting and defeating government interception at-tacks against SSL (short paper). In Financial Cryptography. P. 250–259, 2011. DOI: 10.1007/978-3-642-27576-0_20. URL: https://link.springer.com/chapter/10.1007/978-3-642-27576-0_20 (дата обращения: 02.03.2020).
10. Shakarian P. Stuxnet: Cyberwar revolution in military affairs. – Military Academy West Point NY, 2011. URL: https://apps.dtic.mil/docs/citations/ADA546439 (дата обращения: 01.03.2020).
11. Jøsang A. PKI trust models. In Atilla Elçi *et al.* (editors), Theory and Practice of Cryptography Solutions for Secure Information Systems (CRYPSIS). – IGI Global, 2013. P. 279–301. ISBN13: 9781466640306. DOI: 10.4018/978-1-4666-4030-6.ch012. URL: https://www.igi-global.com/chapter/content/76520 (дата обращения: 10.02.2020).
12. Омельченко А.В. Теория графов. – М.: МЦНМО, ISBN 978-5-4439-1247-9. 2018. – 416 с.
13. Ølnes J. PKI Interoperability by an Independent, Trusted Validation Authority. In Proceedings of the 5th Annual PKI R&D Workshop, NIST, Gaithersburg MD, April 2006. URL: https://pdfs.semanticscholar.org/63ed/e2298104b2a71083406f04c4ba071e048499.pdf (дата обращения: 10.02.2020).
14. Freeburg M., McCaughan A. HIPAA for dummies: A practitioner’s guide // Compelling counseling interventions: Celebrating VISTAS’fifth anniversary. 2008. P. 305–312. URL:https://www.counseling.org/resources/library/VISTAS/2008-V-Print-complete-PDFs-for-ACA/Freeburg_Article_29.pdf (дата обращения: 10.02.2020).
15. Fletcher P.D. The government paperwork elimination act: Operating instructions for an electronic government // International Journal of Public Administration. 2002. Т. 25. №. 5. P. 723–736. URL:https://www.researchgate.net/publication/247530761_The_Government_PaperWork_Elimination_Act_Operating_Instructions_For_An_Electronic_Government (дата обращения: 15.02.2020).
16. Melnikov D.A., Durakovsky A.P., Gorbatov V.S., Modestov A.A. and Ivanenko V.G. Russian Model of Public Keys and Validation Infrastructure as Base of the Cloud Trust. In Proceedings of the 4rd International Conference on Future Internet of Things and Cloud (FiCloud 2016). 2016. P. 123–130. DOI:10.1109/FiCloud.2016.25.URL:https://www.researchgate.net/publication/322288892_Russian_Model_of_Public_Keys_and_Validation_Infrastructure_as_Base_of_the_Cloud_Trust (дата обращения: 16.02.2020).

REFERENCES:

[1] Gorbatov V.S., Poljanskaja O.Ju. Osnovy tehnologii PKI. M.: Gorjachaja Linija – Telekom., 2004.– 248 p. ISBN 5-93517-154-6. URL: https://elibrary.ru/item.asp?id=19582746 (accessed: 15.01.2020) (in Russian).
[2] Rajendran B. Evolution of PKI ecosystem, 2017 International Conference on Public Key Infrastructure and its Applications (PKIA). IEEE, 2017. P. 9–10. URL: https://ieeexplore.ieee.org/abstract/document/8278951 (accessed: 20.01.2020).
[3] Melnikov, D.A. et al. Practical Implementation of Various Public Key Infrastructure Models. IT Security (Russia), V. 23, № 1. P. 100-114, 2016. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/38 (accessed: 07.03.2020). (in Russian).
[4] Kaimov A.T., Kaimov A.T. Public key infrastructure: a survey. – 2018. URL: https://repository.kbtu.kz/bitstream/handle/123456789/75/Вестник%201-2018%20для%20библиотеки-92-99.pdf?sequence=1&isAllowed=y (accessed: 09.03.2020).
[5] Radif M. J. Vulnerability and Exploitation of Digital Certificates, 2018 Al-Mansour International Conference on New Trends in Computing, Communication, and Information Technology (NTCCIT). IEEE, 2018. P. 88–92. URL: https://ieeexplore.ieee.org/abstract/document/8681179 (accessed: 25.01.2020).
[6] Kohlas R., Jonczy J., and Haenni R. A Trust Evaluation Method Based on Logic and Probability Theory. In The Proceedings of the Joint iTrust and PST Conferences on Privacy, Trust Management and Security (IFIPTM 2008), Trondheim, June 2008. DOI:10.1007/978-0-387-09428-1_2. URL: https://link.springer.com/chapter/10.1007/978-0-387-09428-1_2 (accessed: 07.03.2020).
[7] Rescorla E. RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3. IETF, August 2018. DOI: RFC 8446. URL: https://www.hjp.at/doc/rfc/rfc8446.html (accessed: 05.03.2020).

[8] Hayes J.M. The problem with multiple roots in web browsers – certificate masquerading. In 7th Workshop on Enabling Technologies, Infrastructure for Collaborative Enterprises (WETICE '98). P. 306–313. DOI: 10.1109/ENABL.1998.725710. URL: https://ieeexplore.ieee.org/abstract/document/725710 (accessed: 01.03.2020)

[9] Soghoian C. and Stamm S. Certified lies: Detecting and defeating government interception at-tacks against SSL (short paper). In Financial Cryptography. P. 250–259, 2011. DOI:10.1007/978-3-642-27576-0_20. URL: https://link.springer.com/chapter/10.1007/978-3-642-27576-0_20 (accessed: 02.03.2020).

[10] Shakarian P. Stuxnet: Cyberwar revolution in military affairs. – Military Academy West Point NY, 2011. URL: https://apps.dtic.mil/docs/citations/ADA546439 (accessed: 01.03.2020).

[11] Jøsang A. PKI trust models. In Atilla Elçi *et al.* (editors), Theory and Practice of Cryptography Solutions for Secure Information Systems (CRYPSIS). – IGI Global, 2013. P. 279–301. ISBN13: 9781466640306. DOI: 10.4018/978-1-4666-4030-6.ch012. URL: https://www.igi-global.com/chapter/content/76520 (accessed: 10.02.2020).

[12] Omelchenko A.V. Teoriya grafov. – M.: MCNMO, ISBN 978-5-4439-1247-9. 2018. – 416 p. (in Russian).

[13] Ølnes J. PKI Interoperability by an Independent, Trusted Validation Authority. In Proceedings of the 5th Annual PKI R&D Workshop, NIST, Gaithersburg MD, April 2006. URL: https://pdfs.semanticscholar.org/63ed/e2298104b2a71083406f04c4ba071e048499.pdf (accessed: 10.02.2020).

[14] Freeburg M., McCaughan A. HIPAA for dummies: A practitioner's guide. Compelling counseling interventions: Celebrating VISTAS'fifth anniversary. 2008. P. 305–312. URL:https://www.counseling.org/resources/library/VISTAS/2008-V-Print-complete-PDFs-for-ACA/Freeburg_Article_29.pdf (accessed: 10.02.2020).

[15] Fletcher P.D. The government paperwork elimination act: Operating instructions for an electronic government. International Journal of Public Administration. 2002. T. 25. №. 5. P. 723–736. URL:https://www.researchgate.net/publication/247530761_The_Government_PaperWork_Elimination_Act_Operating_Instructions_For_An_Electronic_Government (accessed: 15.02.2020).

[16] Melnikov D.A., Durakovsky A.P., Gorbatov V.S., Modestov A.A. and Ivanenko V.G. Russian Model of Public Keys and Validation Infrastructure as Base of the Cloud Trust. In Proceedings of the 4rd International Conference on Future Internet of Things and Cloud (FiCloud 2016). 2016. P. 123–130. DOI:10.1109/FiCloud.2016.25.URL:https://www.researchgate.net/publication/322288892_Russian_Model_of_Public_Keys_and_Validation_Infrastructure_as_Base_of_the_Cloud_Trust (accessed: 16.02.2020).

Поступила в редакцию – 08 марта 2020 г. Окончательный вариант – 22 мая 2020 г.
Received – March 08, 2020. The final version – May 22, 2020.