ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ
«ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
«ИНФОРМАТИКА И УПРАВЛЕНИЕ» РОССИЙСКОЙ АКАДЕМИИ НАУК»
(ФИЦ ИУ РАН)

На правах рукописи

МЕЛЬНИКОВ Дмитрий Анатольевич

МЕТОДЫ И СРЕДСТВА ПОСТРОЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТОЙ НА ОСНОВЕ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ ДЛЯ ШИРОКОМАСШТАБНЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

ДИССЕРТАЦИЯ

на соискание учёной степени доктора технических наук

по специальности

05.13.19 «Методы и системы защиты информации, информационная безопасность»

Научный консультант:
доктор технических наук,
академик Академии криптографии
Российской Федерации
Будзко В.И.

Москва – 2022

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность работы

Современное развитие российского общества сопровождается стремительной *цифровизацией* (*цифровой трансформацией*) всех его сфер, включая экономику, науку, здравоохранение, образование, культуру и т.д. Это отражено в Указе Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года». Вместе с этим, с целью решения задачи по обеспечению ускоренного внедрения цифровых технологий в экономике и социальной сфере, Правительством Российской Федерации сформирована национальная программа «Цифровая экономика Российской Федерации», утверждённая протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7.

Вызовами и угрозами для реализации целей развития цифровой экономики в сфере информационной безопасности (ИБ) являются рост масштабов компьютерной преступности, в том числе международной, современное состояние национальной инфраструктуры обеспечения ИБ в Российской Федерации, которая пока ещё не способна эффективно парировать многочисленные угрозы, исходящие из глобальной Интернет-сети, нехватка высококвалифицированных специалистов в области информационной безопасности и др.

Переход Российской Федерации на «цифровые рельсы» требует, в первоочередном порядке, создание *информационно-телекоммуникационной инфраструктуры цифровой экономики* (ИТИЦЭ), включающей широкомасштабные информационно-телекоммуникационные системы (далее – ИТС), которые решают различные социально-экономические и задачи информационного и иного обеспечения. Неотъемлемым компонентом любой ИТС является система обеспечения информационной безопасности (СОИБ), которая включает, в том числе, и систему управления криптографической защитой информации (КЗСУ). Очевидно, что ИТС, образующие ИТИЦЭ, должны обладать очень высоким уровнем защищённости, а СОИБ каждой ИТС должна противостоять реальным нарушениям. Следует отметить, что СОИБ всех ИТС, входящих в ИТИЦЭ, образуют информационно-технологическую структуру обеспечения безопасности (ИТИБ).

Кроме того, ИТИЦЭ (вместе с ИТИБ) должна быть надёжной и обеспечивать *доверие*[1] граждан и бизнеса при проведении ими различных финансово-экономических транзакций и

[1] Убеждённость в том, что ИТИЦЭ (ИТИБ) функционирует штатно.

получении электронных услуг. Другими словами, основу доверия между взаимодействующими экономическими субъектами (провайдерами электронных услуг (ПЭУ) и их пользователями) составляет высокий уровень защищённости ИТИЦЭ и входящих в неё ИТС.

Одним из системообразующих компонентов СОИБ ИТС является КЗСУ, одной из задач которой является обеспечение средств криптографической защиты информации (СКЗИ) криптографическими ключами. В настоящее время, ввиду широкомасштабности ИТС КЗСУ базируются на инфраструктурах открытых ключей (ИОК), также входящих в ИТС [8]. В рамках КЗСУ именно ИОК реализует *функцию обеспечения криптоключами* на основе доставки, согласования и распределения криптографических ключей между объектами/субъектами ИТС (СКЗИ). Очевидно, что КЗСУ должна быть надёжной и эффективной, а также способствовать формированию доверия пользователей СКЗИ (граждан, организаций и т.п.), т.е. последние должны быть уверены в том, что СКЗИ работают штатно. Следовательно, ИОК в рамках выполнения функции обеспечения криптографическими ключами должна формировать доверие между субъектами ИТС (владельцами СКЗИ), т.е. выступать в роли системы формирования доверия (или просто *системы доверия*).

Таким образом, необходимая российской цифровой экономике надёжная КЗСУ (система доверия) может быть построена на основе ИОК ИТС. Вместе с тем, анализ ИОК ИТС в РФ показал, что они требуют своей глубокой модернизации и обновления, после чего они будут способны защитить права и законные интересы личности, бизнеса и государства от угроз ИБ, т.е. значительно повысить уровень защищённости цифровой экономики РФ.

Однако, современное состояние ИОК ИТС в РФ не позволяет эффективно решать проблемы обеспечения безопасности и формирования доверия между взаимодействующими экономическими субъектами. Так, согласно перечню аккредитованных удостоверяющих центров (УЦ) Министерства цифрового развития, связи и массовых коммуникаций (Минцифры), по состоянию на 23.09.2021, аккредитовано более 100 УЦ [2]. Проведённый анализ показал, что все УЦ (входящие в ИОК ИТС) в РФ обладают уязвимостями, которыми пользуются киберпреступники. Сущность одной из таких уязвимостей заключается в том, что в состав УЦ одновременно входят центры сертификации (ЦС) и регистрации (ЦР), а это позволяет злонамеренным сотрудникам УЦ (или в условиях давления криминальных структур) выпускать фальшивые (незаконные) сертификаты открытых ключей ($СЕРТ_{ОК}$), которые в последствие могут использоваться (без участия их истинных владельцев) с криминальными целями. Другая уязвимость состоит в том, что ряд УЦ предлагают услугу дистанционного выпуска $СЕРТ_{ОК}$ без личного контакта заявителя и центра регистрации (ЦР). Такая уязвимость УЦ облегчает задачу злоумышленников по получению поддельных $СЕРТ_{ОК}$, что может трактоваться как нарушение действующего законодательства [3].

На сегодняшний день злоумышленники активно пользуются несовершенством ИОК ИТС. Например, было выявлено несколько прецедентов неправомерного использования УЦ электронных подписей (ЭП) застрахованных лиц и оформления документов без участия гражданина [4]. Также было осуществлено несколько незаконных продаж квартир без участия их собственников [5]. Поддельные сертификаты используются злоумышленниками при создании ими *Web*-сайтов (гипертекстовых автоматизированных информационно-технологических систем, ГАИС), замаскированных под *Web*-сайты законных ПЭУ (например, *Web*-порталы по продаже билетов и турпутёвок). Это позволяет преступникам обманывать пользователей и переводить их деньги за фиктивные услуги на свои счета в банках.

Для предотвращения возникновения подобных проблем необходимо преобразование инфраструктуры обеспечения ИБ в части применения криптографических средств защиты информации, и, в частности, разработать КЗСУ (т.е. систему доверия) на основе ИОК ИТС, что обеспечит развитие цифровой экономики РФ. Однако, современное состояние ИОК ИТС не отвечает требованиям по противодействию киберпреступности. Вместе с тем, УЦ различных ИТС никак не взаимодействуют между собой, т.е. между ними нет никаких функциональных связей и они не образуют общегосударственную инфраструктуру открытых ключей, а каждый УЦ функционирует автономно. Очевидно, что назрела проблема глубокой модернизации ИОК ИТС, образующих ИТИЦЭ.

Таким образом, актуальной научно-технической проблемой является построение КЗСУ (системы доверия) на основе ИОК ИТС с целью парирования угроз ИБ, связанных с созданием цифровой экономики Российской Федерации, и защиты прав и законных интересов личности, бизнеса и государства.

Разработанная с использованием математического аппарата субъективной логики КЗСУ на основе ИОК ИТС позволит создать единое поле (пространство) доверия ЭП (ЕПД) и СЕРТ$_{ОК}$, а именно:

- объединить все существующие УЦ ИОК ИТС в единую национальную ИОК;
- сформировать единый распределённый российский сегмент Службы единого каталога (СЕК; с использованием протоколов доступа к СЕК), состоящий из СЕК отдельных ИОК ИТС;
- обеспечить трансграничное взаимодействие с другими странами, то есть вхождение ИОК ИТС в мировую инфраструктуру открытых ключей;
- сформировать технологическую основу доверия для различных прикладных автоматизированных информационно-технологических систем (АИС), входящих в ИТС, которые образуют ИТИЦЭ (например, системы предоставления государственных услуг в электронной форме, дистанционного образования, электронного нотариата, электронные финансовые и

платёжные системы, электронные торговые площадки (электронные биржи) и аукционы и т.д.);

– привлечь бизнес к дальнейшему совершенствованию и наращиванию ИОК ИТС, которые образуют ИТИЦЭ, что обеспечит ему гарантированную и стабильную прибыль;

– обеспечить «прорыв» в технологиях и социально-экономическом развитии России.

Работа выполнена при поддержке Федерального исследовательского центра «Информатика и управления» Российской академии наук.

Степень разработанности темы

Формирование ИОК ИТС в РФ началось в середине 90-х годов прошлого века. При этом формирование носило скорее «стихийный» и слабо контролируемый процесс [6], и, вместе с тем, не было «подкреплено» какими-либо научно-техническими исследованиями. Первая попытка формирования единой системы доверия на основе ИОК ИТС связана с образованием в 2004 году Федерального агентства по информационным технологиям (ФАИТ) [7], на которое были возложены функции государственного регулятора и координатора работ, включая научно-исследовательские, по созданию в России информационного общества (электронного правительства). ФАИТ стал федеральным органом исполнительной власти в области использования ЭП. В частности, ФАИТ курировало реализацию Федеральной целевой программы (ФЦП) «Электронная Россия (2002… 2010 годы)».

В рамках выполнения этой Программы был образован Общероссийский государственный информационный центр (ОГИЦ, Постановление Правительства РФ от 25.12.2007 г. №931). Цель создания ОГИЦ – 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 (ИТС).

Однако, в 2010 году с упразднением ФАИТ все работы, включая научные исследования, по созданию и совершенствованию системы управления криптографической защитой (системы доверия) на основе ИОК ИТС были практически свёрнуты. Минцифры акцентировало своё внимание на разработке и внедрению федеральной гипертекстовой АИС (ГАИС) «Портал государственных и муниципальных услуг Российской Федерации», которая представляет собой справочно-информационный *Web*-портал. А параллельно с этим в стране начали активно создаваться многофункциональные центры «Мои документы» (МФЦ), которые на практике дублировали предоставление государственных услуг, но только в бумажном виде. Другими словами, создание МФЦ фактически дискредитировало саму идею перехода

экономики на «цифровые рельсы» (переход от бумажного документооборота к электронному).

Вместе с тем, в предшествующий период (2011-2020 гг.) были предприняты единичные попытки научных исследований по теме создание ЕПД. В одном из первых таких исследований [8], относящемся к 2016 году, были проанализированы угрозы УЦ и проблемы обеспечения их безопасности, а также были представлены практические рекомендации по созданию ЕПД. Однако, в этой работе не учитывался человеческий фактор, а само понятие «доверия» интерпретировалось как надёжность, т.е. не исследовалась фундаментальная проблема точного понимания доверия в реальном мире, и в частности в ИТС.

В работах [1,9,10], также относящихся к 2016 году, была предложена модель единой (национальной) ИОК, состоящей из ИОК ИТС, а также инфраструктура подтверждения подлинности $СЕРТ_{ОК}$ и проверки ЭП. Указанная модель является компромиссным решением между североамериканской и западноевропейской моделями доверия на основе ИОК. С одной стороны, в российской модели присутствует федеральный УЦ, что характерно для североамериканской модели, а с другой, используется реестр состояния доверенных служб (список аккредитованных УЦ, РСДС), характерный для западноевропейской модели. Однако, в этих работах понятие «доверия» также не исследовалось, а авторы ограничились лишь разработкой функционально-структурной модели.

В 2020 году появилась первая работа [11], в которой на основе эвристического анализа была предложена модель КЗСУ (системы доверия), базирующейся на ИОК ИТС и включающей подсистему центров подтверждения подлинности (ЦПП), которая будет её ядром. Однако, несмотря на то, что предложенная модель доверия является уникальной, в указанной работе отсутствовал синтез этой модели и её системный анализ. Таким образом, приходится констатировать, что в Российской Федерации целенаправленные научные исследования по проблеме построения системы доверия на основе единой ИОК практически не ведутся.

За рубежом тема построения систем доверия на основе ИОК получила широкое развитие [12…18]. В частности, несколько предложенных вариантов таких систем были реализованы в государственных и частных АИС с использованием Интернет-сети, которые были проанализированы в [11]. Важнейшим шагом в зарубежных научных исследованиях явилось издание монографии [19] по субъективной логике (СЛ), которая стала продолжением работ [13,20…25] по исследованию доверия в ИТС и, в частности, в инфраструктурах открытых ключей.

Предлагаемые зарубежные варианты моделей КЗСУ (системы доверия) на основе ИОК не приемлемы для Российской Федерации вследствие различных причин, основными из которых являются функционирование всех УЦ в РФ на основе модели «ЦС+ЦР», обладающей

значительными уязвимостями, и отсутствие хоть сколько-нибудь понятной политики создания и дальнейшего развития единой ИОК на базе ИТС. Другими словами, в нашей стране государственные институты, в качестве регуляторов, практически не участвуют в создании и развитии ИОК ИТС, как основы управления криптографической защитой (системы доверия), в то время как в зарубежных экономически развитых странах ситуация полностью противоположная – государственные органы исполнительной власти отвечают за функционирование и дальнейшее развитие национальных ИОК, которые являются технологической основой цифровизации экономик и электронных правительств иностранных государств.

Таким образом, разработка и реализация модели КЗСУ (системы доверия) на основе ИОК для ИТС, и создание единой системы доверия (путём объединения ИОК ИТС) в интересах ИТИЦЭ РФ и её пользователей (организаций, ведомств и граждан) становится стратегической задачей, решение которой носит безотлагательный характер. Вместе с тем, необходимо определить методы и средства построения КЗСУ.

Теперь можно сформулировать **цель работы**: *разработка с использованием математического аппарата субъективной логики системы управления криптографической защитой (системы доверия) на основе инфраструктуры открытых ключей с целью повышения уровня защищённости ИТС, образующих ИТИЦЭ РФ.*

Для достижения цели работы были поставлены следующие задачи:

1. Анализ взаимосвязи концепций доверия и безопасности в ИТС, а также выбор и обоснование выбора методов и средств (математического аппарата субъективной логики) для построения и анализа КЗСУ (системы доверия) на основе ИОК с целью повышения уровня защищённости ИТС.

2. Анализ организации и компонентов ИОК, а также решаемые ею задачи по обеспечению безопасности. Проведение сравнительного анализа основных архитектур и современных моделей организации ИОК, реализованных за рубежом, а также анализа проблем безопасности и рисков пользователей ИОК. Исследование уязвимостей, характерных для российских УЦ, и которые снижают доверие к ним.

3. Сравнительный анализ архитектур обеспечения параметрами подлинности пользователей и провайдеров электронных услуг, и определение необходимых условий, обеспечивающих доверие пользователей к провайдерам электронных услуг, и провайдеров к пользователям. Анализ параметров подлинности, содержащихся в $СЕРТ_{ОК}$ и атрибутных сертификатах ИОК, а также систем (структур) доверия на основе ИОК.

4. Синтез модели КЗСУ (системы доверия) на основе ИОК с использованием математического аппарата субъективной логики, и анализ полученной модели системы доверия с

точки зрения решения задач обеспечения безопасности. Разработка методов защиты граждан и бизнеса при предоставлении электронных услуг и проведении коммерческих электронных процедур (включая финансовые транзакции) на основе синтезированной модели КЗСУ (системы доверия), а также построение модели единой системы идентификации Интернет-пользователей и провайдеров электронных услуг, которая позволит снизить уровень киберпреступности в мировом информационном пространстве.

5. Внедрение полученных в пунктах 2…4 результатов в научно-исследовательскую и практическую деятельность организаций и компаний.

Научная новизна диссертационной работы:

1. На основе анализа понятия «доверия» и «взаимосвязей/взаимоотношений» представлены новые модели (структурные блок-схемы) ложно-доверительных взаимосвязей: первая – модель взаимодействия Интернет-пользователя с поддельным (мошенническим) *Web*-сайтом, но воспринимаемым им, как подлинный; вторая – модель взаимодействия субъекта с управляемым им логическим объектом в условиях компьютерного шпионажа, когда этот логический объект узурпирован злонамеренным субъектом (нарушителем).

2. Впервые была разработана модель КЗСУ (системы доверия) на основе ИОК для ИТС, формирующих ИТИЦЭ РФ.

3. Впервые с целью синтеза и анализа КЗСУ (системы доверия) на основе ИОК для ИТС, формирующих ИТИЦЭ РФ, был использован математический аппарат субъективной логики.

4. В результате анализа КЗСУ (системы доверия) на основе ИОК для ИТС, формирующих ИТИЦЭ РФ, было впервые установлено, что все российские УЦ построены на основе модели «ЦС+ЦР», которая обладает серьёзными уязвимостями, позволяющими совершать киберпреступления против ИОК-пользователей с целью обмана граждан и организаций, т.е. является источником многочисленных угроз и рисков.

5. На основе анализа синтезированной КЗСУ (системы доверия) на основе ИОК для ИТС, формирующих ИТИЦЭ РФ, был впервые разработан метод (алгоритм) определения обоснованности (законности) выпуска $СЕРТ_{ОК}$, что представляет собой новую для ИОК задачу, которая не была решена ни одной из известных на сегодняшних день систем доверия на основе различных архитектур ИОК.

6. Впервые разработан метод обнаружения злонамеренных ПЭУ, который включает два алгоритма проверки собственника $СЕРТ_{ОК}$.

7. Впервые предложена модель единой системы идентификации Интернет-пользователей и провайдеров электронных услуг на основе логической характеристики IPv6-протокола.

Теоретическая значимость работы:

1. На основе аппарата СЛ и эвристического метода поиска сети доверия была синтезирована новая (ранее не известная) модель КЗСУ (системы доверия) на основе ИОК и сформулировано основное требование к ней – она должна представлять собой сеть субъективного доверия (ССД), отображаемую в форму последовательно-параллельного орграфа (ППОГ). Синтезированная модель КЗСУ (системы доверия) на основе ИОК полностью удовлетворяет указанному требованию, позволяет сформировать маршруты доверия с минимальным числом рёбер в ППОГ, и, таким образом, напрямую соединить УЦ, ПЭУ и ИОК-пользователей с ЦПП (все входят в состав ИТС), т.е. обеспечить прямую транзитивность доверия. Кроме того, указанная модель не требует группирования УЦ в иерархическую структуру с корневым УЦ или сетевую структуру с главным УЦ, но включает распределённую подсистему ЦПП, выстроенную по иерархической схеме с корневым ЦПП.

2. Определена новая функция (задача), реализуемая (решаемая) разработанной КЗСУ (системой доверия) на основе ИОК – определение обоснованности (законности) выпуска $СЕРТ_{ОК}$, которая дополнила перечень известных функций (задач) обеспечения безопасности, реализуемых (решаемых) ИОК. Таким образом, расширены научные представления о возможностях различных архитектур ИОК, выполняющих функции инфраструктуры обеспечения безопасности.

3. Впервые, с теоретической точки зрения, была обнаружена и проанализирована глобальная уязвимость КЗСУ (системы доверия) на основе ИОК для ИТС, формирующих ИТИЦЭ РФ – чрезвычайно уязвимая модель построения всех без исключения российских УЦ («ЦС+ЦР»). Следствием этого является невозможность КЗСУ (системы доверия) на основе ИОК предотвратить выпуск фальсифицированных $СЕРТ_{ОК}$, которые, в свою очередь являются источниками многочисленных рисков и угроз.

Практическая значимость работы:

1. На основе синтезированной модели КЗСУ (системы доверия) на основе ИОК для ИТС, формирующих ИТИЦЭ РФ, была предложена усовершенствованная модель, в которой концепция единого (единственного) центра подтверждения подлинности заменена на концепцию распределённого центра. Усовершенствованная модель включает подсистему ЦПП, состоящую из центров, которые принадлежат ИТС федерального, федеральных окружных, региональных и муниципальных уровней. В совокупности такие центры образуют единую иерархическую систему центров подтверждения подлинности, которая является ядром системы доверия на основе ИОК.

2. Разработана функционально-структурная модель КЗСУ (системы доверия) на основе ИОК для ИТС, формирующих ИТИЦЭ РФ, которая включает единую иерархическую систему ЦПП. Кроме этого, были определены требования к ЦПП, входящих в такую единую иерархическую систему. Также была разработана географически-распределённая модель единой иерархической системы ЦПП, которая определяет возможные географические места размещения ЦПП на каждом уровне архитектуры.

3. Было сформулировано главное требование к КЗСУ (системы доверия) на основе ИОК для ИТС, формирующих ИТИЦЭ РФ, заключающееся в реализации следующих основных функций: предоставление (по запросу) услуг по проверке ЭП и целостности подписанного электронного документа; подтверждение подлинности (по запросу) предоставленного $СЕРТ_{ОК}$; проверка обоснованности (законности) выпуска сертификата открытого ключа с целью защиты прав и свобод гражданина, на имя которого (без его согласия) мог быть издан фальсифицированный сертификат.

4. Впервые разработан метод парирования угроз безопасности, связанных с выпуском фальсифицированных сертификатов удостоверяющим центром, который основан на подтверждении подлинности и проверке законности выпуска $СЕРТ_{ОК}$. Предложен алгоритм и вариант реализации указанного метода, предусматривающий участие специализированного государственного органа (например, многофункционального центра «Мои документы»), который регистрирует заявку пользователя ИОК на получение сертификата открытого ключа и подтверждает наличие такой заявки.

5. Предложен метод распознавания поддельных (мошеннических) *Web*-сайтов, который включает проверку и подтверждение подлинности сертификата провайдера электронных услуг со стороны пользователя с целью предотвращения (блокирования) мошеннических транзакций. Указанный метод предусматривает разработку и применение пользователем специализированного программного модуля (КПО), установленного в его компьютер или смартфон, т.е. КПО по команде пользователя осуществляет процедуры проверки и подтверждения подлинности сертификата ПЭУ. Предложенный метод предусматривает два варианта обнаружения мошеннических *Web*-сайтов, которые определяются тем, какой сертификат провайдера электронных услуг использует злоумышленник, либо украденный сертификат, принадлежащий законному провайдеру электронных услуг, *Web*-портал которого имитирует злоумышленник, либо свой собственный сертификат, полученный электронным способом в зарубежном центре сертификации.

6. Предложен комплекс международных и национальных мероприятий по созданию и реализации глобальной системы идентификации Интернет-пользователей и провайдеров электронных услуг на основе логической характеристики IPv6-протокола.

Методология и методы диссертационного исследования:

Основными методами диссертационного исследования являются анализ, синтез и структурное (системное) моделирование с последующим анализом синтезированных моделей. Исследование основано на функционально-ориентированном и предметно-ориентированном подходах. При первом подходе применялась последовательная декомпозиция проблемы на отдельные, достаточно простые составляющие, обладающие функциональной определённостью. При втором подходе формировались абстрактные модели реальных объектов, которые позволили создать оптимальные (субоптимальные) системы, устанавливающие взаимосвязи между функциональными объектами (субъектами).

При исследовании понятия «доверия» был проведён анализ известных теоретических работ по данной тематике и на основе результатов этого анализа были предложены новые структурные модели доверительных взаимосвязей/взаимоотношений между «мыслящими» субъектами и логическими объектами. Первая модель отражает ситуацию, при которой злонамеренный субъект управляет мошенническим логическим объектом (например, поддельным *Web*-сайтом), мыслящий доверяющий субъект доверяет такому объекту. Вторая модель отражает ситуацию, при которой мыслящий доверяющий субъект управляет доверенным логическим объектом, а одновременно с этим злонамеренный субъект узурпировал (захватил) управление и манипулирует логическим объектом (модель компьютерного шпионажа).

Основные результаты исследований были получены на основе применения математического аппарата субъективный логики, которая включает ряд новых операторов, позволяющих проанализировать различные субъективные сети доверия. При разработке модели системы доверия в условиях сложных сетей субъективного доверия использовались алгоритмы синтеза последовательно-параллельных графов (элементы теории графов) с учётом соответствующих критериев синтеза и требований к надёжности при вычислении рекомендуемых мнений.

Положения, выносимые на защиту:

1. Разработанная с помощью математического аппарата субъективной логики модель КЗСУ (системы доверия) на основе инфраструктуры открытых ключей для ИТС и её усовершенствованная версия, в которой предложена концепция распределённого ЦПП, представляющего собой единую иерархическую систему ЦПП, которая является ядром системы (формирования) доверия в ИТС, входящих в ИТИЦЭ РФ.

2. Функционально-структурная модель КЗСУ (системы доверия) на основе инфраструктуры открытых ключей для ИТС, в рамках которой были определены требования к ЦПП,

входящих в единую иерархическую систему ЦПП ИТС. Географически-распределённая модель единой иерархической системы ЦПП, которая определяет географические места размещения ЦПП ИТС на каждом уровне иерархии.

3. Главное требование к КЗСУ (системы доверия) на основе инфраструктуры открытых ключей для ИТС, заключающееся в реализации следующих основных функций: предоставление (по запросу) услуг по проверке ЭП и целостности подписанного электронного документа; подтверждение подлинности (по запросу) предоставленного $СЕРТ_{ОК}$; проверка обоснованности (законности) выпуска $СЕРТ_{ОК}$ с целью защиты прав и свобод гражданина, на имя которого (без его согласия) мог быть издан фальсифицированный сертификат.

4. Реализуемый КЗСУ (системы доверия) на основе инфраструктуры открытых ключей для ИТС метод парирования угроз безопасности, связанных с выпуском фальсифицированных $СЕРТ_{ОК}$ УЦ, который основан на подтверждении подлинности и проверке законности выпуска $СЕРТ_{ОК}$, и предусматривает участие специализированного государственного органа, предназначенного для регистрации заявки пользователя ИОК на получение $СЕРТ_{ОК}$ и подтверждения наличие такой заявки.

5. Реализуемый КЗСУ (системы доверия) на основе (инфраструктуры) открытых ключей для ИТС метод распознавания поддельных (мошеннических) *Web*-сайтов, который включает проверку и подтверждение подлинности $СЕРТ_{ОК}$ ПЭУ со стороны пользователя с целью предотвращения (блокирования) мошеннических транзакций.

6. Модель единой (глобальной) системы идентификации Интернет-пользователей и провайдеров электронных услуг на основе логической характеристики IPv6-протокола, реализация которой позволит существенно снизить киберпреступность в мировом информационном пространстве.

Достоверность результатов исследования, интерпретации результатов моделирования, выносимых на защиту научных положений, новизны и выводов подтверждается тем, что выявленные в работе уязвимости и закономерности, разработанные способы и выводы не противоречат основным целям, задачам и международным стандартам обеспечения информационной безопасности, а все аналитические результаты получены с использованием математического аппарата субъективной логики. Корректность синтезированных моделей систем доверия была подтверждена результатами последующего вероятностного анализа.

Личный вклад автора заключается в обсуждении и постановке цели, задач и программы исследования, разработке структурно-методологической схемы исследования, обработке и интерпретации результатов моделирования, обобщении установленных уязвимостей, формулировании положений и выводов, написании статей, учебников и учебного пособия,

выступлениях с докладами на международных конференциях. Все аналитические и практические результаты, представленные в диссертации, получены самим автором или при его непосредственном участии.

Апробация работы. Материалы диссертационной работы доложены и обсуждены на российских и международных конференциях: The 3rd European Conference on Information Warfare and Security (Royal Holloway University of London, Лондон, Великобритания, 28-29 июня 2004 года); 10-ая Научно-практическая конференция «Современные информационные технологии в управлении и образовании» (ФГУП НИИ «Восход», Москва, 24 марта 2011 года); Всероссийская Интернет-конференция «Информационные технологии и их применение» (ФГБОУ ВПО Иркутский государственный лингвистический университет, Иркутск, 13-17 мая 2013 года); The International Conference on e-Business, e-Commerce, e-Management, e-Learning and e-Governance (IC5E 2014, Лондон, Великобритания, 30-31 июля 2014 года); The IEEE 3rd International Conference on Future Internet of Things and Cloud (FiCloud 2015, Рим, Италия, 24-26 августа 2015 года); The 8th International Conference on Computer Supported Education (CSEDU 2016, Рим, Италия, 21-23 апреля 2016 года); The IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud 2016, Вена, Австрия, 22-24 августа 2016 года); The IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud 2017, Прага, Чехия, 21-23 августа 2017 года); The 6th International Conference Actual Problems of System and Software Engineering (APSSE 2019, Москва, Россия, 12-14 ноября 2019 года); 2020 Annual International Conference on Brain-Inspired Cognitive Architectures for Artificial Intelligence: Eleventh Annual Meeting of the BICA Society (BICA*AI 2020).

Реализация полученных результатов:

1. Полученные результаты диссертационного исследования были реализованы или использованы в научно-исследовательской и практической деятельности следующих организаций:

– Акционерном обществе «Газпромбанк»;

– Акционерном обществе «Научно-технический и сертификационный центр по комплексной защите информации» (АО Центр «Атомзащитаинформ»);

– Обществе с ограниченной ответственностью «Код безопасности»;

– Обществе с ограниченной ответственностью Фирма «АНКАД»;

– Группе компаний (ГК) «МАСКОМ».

2. В НИР «Ключи – 2018» (Договор № 569-27-и от 24.04.2018), выполненной в Федеральном исследовательском центре «Информатика управление» РАН для Центрального Банка Российской Федерации.

3. Материалы диссертационной работы используются в Национальном исследовательском ядерном университете «МИФИ» и Финансовом университете при Правительстве Российской Федерации при подготовке бакалавров, магистров и аспирантов по направлению «Информационная безопасность» (*учебники*: Мельников Д.А. Организация и обеспечение безопасности информационно-технологических сетей и систем: Учебник. – М.: IDO Press, Университетская книга, 2012. ISBN 978-5-4243-0004-2; Мельников Д.А. Информационная безопасность открытых систем: Учебник. – М.: Флинта, Наука, 2013. ISBN 978-5-9765-1613-7; *учебные пособия*: Орлов В.А., Мельников Д.А. Современная криптография и архитектура безопасности компьютерных сетей: Учебное пособие. – М.: МГУПИ, 2009; Фомичёв В.М., Мельников Д.А. Криптографические методы защиты информации (в 2-х частях): Учебное пособие. М.: Юрайт. 2016. ISBN 978-5-9916-7089-3.

Публикации. Материалы диссертации опубликованы в изданиях, рекомендованных ВАК, а также в изданиях, индексируемых в базах данных Scopus и Web of Science: 1 статья в журнале, индексируемом в Scopus и/или Web of Science, 7 статей в сборниках трудов международных научных конференций, индексируемых Scopus и/или Web of Science, 20 статей в рецензируемых российских журналах из списка ВАК, РИНЦ, а также 3 статьи в сборниках трудов международных конференций (на английском языке). По теме работы опубликованы 2 учебника и 2 учебных пособия.

Структура и объём диссертационной работы. Диссертационная работа состоит из введения, 6 глав, заключения, основных выводов, списка цитируемой литературы и двух приложений. Общий объём диссертации составляет 350 страниц, включая 100 рисунков, 13 таблиц, 201 библиографический источник.

Автор настоящей диссертационной работы выражает благодарность за помощь и содействие в проведении исследований и обсуждение полученных результатов д.т.н., академику Академии криптографии РФ В.И. Будзко, Заслуженному деятелю науки РФ, д.т.н., проф. И.Н. Синицыну, д.ф.-м.н., проф. В.М. Фомичёву, д.ф.-м.н. М.А. Пудовкиной, д.т.н., проф. В.Г. Иваненко, к.т.н., доценту В.С. Горбатову, а также коллективам 63 отдела ФИЦ ИУ РАН и кафедр №41 «Защита информации», и №43 «Стратегические информационные исследования» ИИКС НИЯУ МИФИ.

Глава 1 ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЦИФРОВОЙ ЭКОНОМИКИ. ПОСТАНОВКА ЗАДАЧ ДИССЕРТАЦИОННОЙ РАБОТЫ

Современное развитие российского общества сопровождается ускоренной *цифровизацией* (*цифровой трансформацией*) всех его сфер, включая экономику, науку, здравоохранение, образование, культуру и т.д. Президент России В.В. Путин в послании Федеральному собранию 2016 года заявил: «Предлагаю запустить масштабную системную программу развития экономики нового технологического поколения – *цифровой экономики*. В её реализации будем опираться на российские компании, научно-исследовательские и инжиниринговые центры страны. Это вопрос национальной безопасности, технологической независимости России, нашего общего будущего… Нужно также учитывать, что в цифровых технологиях кроются и риски. Необходимо укреплять защиту от киберугроз, должна быть значительно повышена устойчивость всех элементов инфраструктуры, финансовой системы, системы госуправления».

Это предложение нашло своё отражение в Указе Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года». Вместе с этим, с целью решения задачи по обеспечению ускоренного внедрения цифровых технологий в экономике и социальной сфере, Правительством Российской Федерации сформирована национальная программа «Цифровая экономика Российской Федерации», утверждённая протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7.

1.1 Истоки понятия «цифровая экономика»

Концепция «*цифровая экономика*» получила всемирное распространение и стала предметом многочисленных научных, экономических и общественных дискуссий, которые проводятся на государственном и экспертном уровне. Начало международному обсуждению цифровой экономики было положено на Давосском форуме в 2015 году, на котором выступил президент форума профессор К. Шваб и проинформировал участников форума о грядущем глобальном социальном кризисе [26]. По его мнению, развитие технологий в ближайшие годы оставит без работы десятки миллионов человек. *Четвертая промышленная революция* – это смешение технологий физического, цифрового и биологического мира, которое создаёт новые возможности и воздействует на политические, социальные и экономические системы [27].

По сути, «цифровая экономика» подразумевает изменение технологической базы экономики, которое позволит автоматизировать рутинные операции. Это значительно меняет скорость реализации многих процессов, предоставляет новые возможности, но не меняет базовых основ экономики. По мысли К. Шваба [27]: «*Мы стоим у истоков четвертой промышленной революции. Она началась на рубеже нового тысячелетия и опирается на цифровую революцию. Её основные черты – это «вездесущий» и мобильный Интернет, миниатюрные производственные устройства (которые постоянно дешевеют), искусственный интеллект и обучающиеся машины*».

Подтверждением этих слов является мнение экспертов Давосского форума в 2015 году, которые выделили несколько кардинальных преобразований [27], которые ожидаются до 2025 года, среди которых:

- 10% людей будут носить подключённую к Интернет-сети одежду;
- 90% людей получат возможность хранения данных различных объёмов и на бесплатной основе (за счёт доходов от рекламы);
- к Интернет-сети будет подключён примерно 1 триллион измерительных приборов (датчиков, сенсоров и т.п.);
- в США появится первый робот-фармацевт;
- 10% очков для чтения будут подключены к Интернет-сети;
- одновременно до 80% жителей планеты будут «присутствовать» в Интернет-сети;
- будет произведён первый автомобиль при помощи трёхмерной печати;
- появится первое правительство, которое при переписи населения будет использовать технологию и источники «больших данных»;
- в продаже появится первый имплантируемый смартфон;
- примерно 5% потребительских товаров будет создано с помощью технологии трёхмерной печати;
- примерно 90% жителей планеты будут пользоваться смартфонами;
- примерно 90% жителей планеты будут иметь регулярный доступ к Интернет-сети;
- на дорогах США число беспилотных автомобилей будет составлять примерно 10% от общего количества автомобилей;
- будет проведена первая в мире хирургическая операция по пересадке печени, созданной с использованием трёхмерной печати;
- примерно 30% корпоративных аудиторских проверок будет проводиться с использованием технологии искусственного интеллекта (ИИ);
- впервые правительство будет собирать налоги с помощью прикладных АИС, использующих технологию «блокчейн» (БЧ, *blockchain*);

▪ более 50% домашнего Интернет-трафика приходится на долю прикладных АИС и программно-аппаратных комплексов (ПАК);

▪ число поездок/путешествий на автомобилях для совместного использования будет превышать число поездок на частных автомобилях;

▪ появится первый город (с населением более 50000 жителей) без светофоров;

▪ примерно 10% всемирного валового продукта хранится в системах, использующих технологию БЧ;

▪ в составе корпоративного совета директоров впервые появится ИИ-робот.

Однако, некоторые из представленных выше цифровых преобразований вряд ли будут реализованы даже в отдалённой перспективе, а некоторые – чреваты возникновением огромных рисков, которые будут сопровождаться значительными материально-финансовыми потерями в различных отраслях экономии и социальной сферы. В частности, это относится к технологии БЧ, которая несёт в себе серьёзные угрозы ИБ. В ряде работ [28,29,30,31] указывается, что непродуманное и повсеместное использование систем БЧ может привести к огромному экономическому урону. К главным уязвимостям систем БЧ относятся: игнорирование принципа неотказуемости и уязвимость систем обеспечения криптографическими ключами. Таким образом, без учёта информационно-технологических проблем, связанных с обеспечением кибербезопасности, нельзя «бездумно» следовать рекомендации по широкому применению систем БЧ.

Также вызывают сомнения перспективы создания и применения на существующей автодорожной сети (автомагистралях) безопасного беспилотного автомобиля. Данное утверждение можно обосновать следующим образом. Все автомагистрали, по которым будет двигаться беспилотный автомобиль должны иметь наукоёмкую технологичную инфраструктуру, которая будет обеспечивать беспилотный автомобиль данными о его местоположении и окружающей обстановке. Если первая задача, в принципе, может быть решена за счёт применения, либо глобальных систем навигации и местоопределения (однако, возникает проблема точности местоположения), либо специальной дорожной разметки, включая передатчики специальных синхросигналов, то вторая не может быть решена принципиально, так как просто невозможно спрогнозировать «поведение» других автомобилей, движущихся впереди, сзади или параллельно с беспилотным автомобилем, т.е. невозможно предугадать действия водителя (тем более пьяного или употребившего наркотики) автомобиля, движущегося рядом с беспилотным автомобилем. В такой ситуации возникает справедливый вопрос: «А не дешевле и проще построить для таких «беспилотников» выделенные пути (дороги, например, рельсы), надёжно отгороженные от остального автотранспорта?».

Очевидно, что рекомендации экспертов Давосского форума, с одной стороны, весьма иллюзорны, но, с другой стороны, обладают скрытым подтекстом, смысл которого в следующем. Вживляемые мобильные телефоны, Интернет-очки, одежда, подключённая к Интернету, тотальная «смартфонизация», *Интернет вещей* сделают мир «прозрачным», а *каждый человек будет непрерывно контролируемым*. Из теории управления следует, что контролируемость системы является важнейшим условием её управляемости. Тогда становится ясным, что реализация рекомендаций давосских экспертов позволит поднять на качественно новый уровень *технологии манипуляции общественного сознания и управления обществом*, живущим в основном в виртуальном пространстве [26].

1.2 Эволюция цифровизации

Идея глобальной цифровизации и перехода к цифровой экономике (цифровой трансформации экономики) возникла отнюдь не спонтанно. Эволюция цифровой трансформации имеет прочную теоретическую основу в виде цифрового языка математики, положившего начало точным наукам и прикладным разработкам в технике. Считается, что зарождение информационно-цифровой эпохи было инициировано появлением электронно-вычислительных машин (ЭВМ), обеспечивших выполнение цифровых преобразований, обработку и передачу информации без участия человека. В этом заключается принципиальное отличие ЭВМ от машин с автоматическим управлением. Возникновение ИИ ещё более усилило самостоятельность в решении и расширило класс решаемых ЭВМ задач [26].

В работе [32] совершенно справедливо отмечено, что «повсеместная компьютеризация и масштабное расширение сфер применения компьютерных систем инициировало возникновение актуальной сегодня темы цифровой революции».

Цифровая трансформация, с момента возникновения ЭВМ и до настоящего времени прошла значительный путь, на протяжении которого произошла смена нескольких технологических укладов, сегодня данное понятие ассоциируют с интенсивным развитием ИТС и началом периода второго поколения информатизации. Это, как полагают многие учёные и специалисты-практики, является основой формирующегося *VI технологического уклада*. На рисунке 1.1 представлены основные этапы информационно-технологического развития экономики и социальной сферы [33].

По аналогии с промышленной революцией, которая превратила аграрную экономику в индустриальную, сегодня технологическая революция приводит к её цифровизации. В конце 1950-х годов появилось понятие «постиндустриальное общество» [34]. В [34] автор впервые усомнился в результативности предшествующих социально-экономических моделей в совре-

менных условиях. Его мысль относительно информационной эпохи получила развитие во второй половине 1990-х годов [35]. В [35] была сформулирована основная причина изменения привычной для того периода социально-экономической модели. Причина заключается в том, что формируется новое общество, а информация играет в нём новую роль.

Рисунок 1.1 – Основные этапы информационно-технологического развития экономики и социальной сферы [33]

Технологическая революция коснулась и Советского Союза. Ярким примером технологических преобразований стал радикальный проект академика В.М. Глушкова, который он предложил в 70-х годах прошлого века [26]. Учитывая успехи в автоматизации производственных процессов, он выдвинул идею создания *Общегосударственной автоматизированной системы* (ОГАС). Для того, чтобы такая система успешно работала, нужно, чтобы люди, с одной стороны, регулярно давали своевременную, точную и объективную информацию о запрашиваемых системой параметрах, а с другой – выполняли точно и в срок получаемые рекомендации. Так вот это и оказалась непреодолимым препятствием. Действительно, у человека есть личные, семейные, корпоративные и множество других интересов, да и своё понимание того «как нужно делать». Отвлечься от всего этого ради общегосударственных целей, полагая, что в моделях учтено всё необходимое, что и «ОГАС способна решить все задачи автоматизации», удалось немногим.

Кроме того, В.М. Глушков в те же годы предлагал отказаться от бумажного документооборота и перейти к «безбумажной информатике». Сделать это тоже не удалось в силу недостаточной культуры управления и неочевидности плюсов всего этого мероприятия. Бюрократия устойчива относительно перехода от гусиных перьев к авторучкам, улучшения качества бумаги, появления в кабинетах телефонов, компьютеров, смартфонов и широкополосного Интернета.

Идея академика В.М. Глушкова нашла своё продолжение в 2000-х годах с образованием ФАИТ и созданием ОГИЦ [6]. Цель создания ОГИЦ – 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 [36]. Но, как и ОГАС, ОГИЦ прекратил своё существование после упразднения ФАИТ в 2010 году. Причина – всё та же невежественная бюрократия.

1.3 Программа «Цифровая экономика Российской Федерации»

Правительство России проводит «широкую компьютеризацию» различных сфер жизнедеятельности, включая экономику и социальную сферу. Вместе с тем, Программа «Цифровая экономика Российской Федерации» (далее Программа) рассматривает не различные направления финансово-инвестиционной деятельности, а конкретные технологии, которые, по идее разработчиков Программы, должны изменить экономику России к лучшему.

К основным «*сквозным цифровым технологиям*», которые получат приоритетное развитие, относятся следующие:

- большие данные;
- нейротехнологии и искусственный интеллект;
- системы распределённого реестра (тоже, что и системы с БЧ, см. §1.1);
- квантовые технологии;
- новые производственные технологии;
- промышленный интернет;
- компоненты робототехники и сенсорики;
- технологии беспроводной связи;
- технологии виртуальной и дополненной реальности.

Концепция «сквозные цифровые технологии» была введена авторами Программы, причём они не дали описание этого понятия! В теории электросвязи термин «сквозное» относится к виртуальным соединениям (линиям/каналам связи) в информационно-технологических сетях и системах передачи данных [37]. В этой связи, словосочетание «сквозные … технологии» – некорректно.

В Программе определены три следующие *цели*.

1. «Создание экосистемы[2] цифровой экономики Российской Федерации, в которой данные в цифровой форме[3] являются ключевым фактором производства во всех сферах социально-экономической деятельности, и в которой обеспечено эффективное взаимодействие, включая трансграничное, бизнеса, научно-образовательного сообщества, государства и граждан».

Традиционно к основным факторам производства раньше относили труд, капитал, сырье. В условиях инновационной экономики к этому можно добавить технологии, знания, инновации. Почему вдруг таким фактором оказались «данные» и особенно в цифровой форме?

---

[2] «Экосистема» – термин, введённый разработчиками Программы – это экологическая или экономическая система? В Программе ответа на этот вопрос нет.

[3] Данные – информация, представленная в цифровом (дискретном) формате. Поэтому «данные в цифровой форме» – «масло масляное», т.е. это словосочетание некорректно.

Разработчики Программы поясняют, что «…в настоящее время данные становятся новым активом, причём главным образом, за счёт их альтернативной ценности, то есть применения данных в новых целях и их использования для реализации новых идей». Однако новые цели не конкретизируются, т.е. не определены. По-видимому, можно ожидать появления новых документов, где это будет разъяснено. Что же касается «эффективного взаимодействия» 1% населения, владеющего 80% национального богатства, и 99% оставшихся, то трудно надеяться, что Программа здесь поможет.

2. «Создание необходимых и достаточных условий институционального и инфраструктурного характера, устранение имеющихся препятствий и ограничений для создания и (или) развития высокотехнологичных бизнесов…» О достаточных условиях судить трудно, но к необходимым относится доступный кредит. Из курса экономики и мирового опыта известно, что условием выживания обрабатывающих производств является кредит в 10-12% годовых, а предприятий, использующих наукоёмкие технологии, – 3-4%. Если бы в результате выполнения этой программы удалось добиться таких кредитов в отечественных банках, то об остальном можно было бы «не беспокоиться». Однако, кроме объявленной цели далее в тексте Программы о «необходимых и достаточных условиях» никаких упоминаний нет.

3. «Повышение конкурентоспособности на глобальном рынке как отдельных отраслей Российской Федерации, так и экономики в целом». Поскольку об экономике, ожидаемом экономическом эффекте от мероприятий данной Программы речь не идёт, то и эта цель «повисает в воздухе».

Очевидно, что если цели Программы не определены, то для чего нужна такая Программа? В тексте есть ответ и на этот вопрос: «По предложению Всемирного экономического форума для готовности стран к цифровой экономике используется последняя версия международного индекса сетевой готовности, представленная в докладе «Глобальные цифровые технологии» за 2016 год …

Отсюда следует несколько важных выводов. Во-первых, авторы сами признают, что их Программа является следствием рекомендаций Давосского форума, которые упоминались ранее (см. §1.1).

Во-вторых, она исходит не из того, чтобы что-то производить, уметь, создавать новое, а из приоритета предоставления услуг по сравнению с производством, и интересов «квалифицированного потребителя». В частности, это отразилось на системе высшего образования в России, т.е. если раньше отечественная система высшего образования готовила «созидателей», то теперь – «потребителей».

В-третьих, вместо вещей сущностных, внутренних, акцент делается на внешних, подсказанных со стороны, на места в рейтингах. Как уже показала практика, например, на проекте

в области высшего образования, в соответствии с которым к 2020 году 5 российских вузов должны войти в первую сотню «*некого зарубежного рейтинга*» (вопрос доверия к такому рейтингу), этот путь мало перспективен.

Кроме того, Программа объясняет почему Россия находится в пятом десятке рейтинга готовности стран к цифровой экономике. «Такое значительное отставание в развитии цифровой экономики от мировых лидеров объясняется проблемами нормативной базы для цифровой экономики и недостаточно благоприятной средой для ведения бизнеса и инноваций и, как следствие, низким уровнем применения цифровых технологий бизнес-структурами». Другими словами, причина отставания России – отсутствие необходимой законодательной и нормативной правовой базы!

Вместе с тем существует несколько стратегических задач, которые должно решать Правительство Российской Федерации уже сейчас [26]. Вот некоторые из них:

– создание и развитие элементной компонентной базы;

– создание государственной системы анализа и снижения рисков природных и техногенных катастроф и социальной нестабильности;

– компьютерная модернизация машиностроительного комплекса России;

– создание информационно-технологической инфраструктуры обеспечения информационной-безопасности.

1.4 Угрозы национальной безопасности России в связи с цифровой трансформацией и возможности их нейтрализации

Цифровая трансформация экономики Российской Федерации угрожает государственной безопасности по следующим направлениям:

1. Кибертерроризм и кибершпионаж, ведущиеся против России США, их союзниками [38], а также другими странами и иностранными террористическими и преступными организациями, а также отдельными лицами и группами лиц. Ярким подтверждением такой деятельности является директива экс-президента США Б. Клинтона от 16 апреля 1993 года «*Public Encryption Management*» («О государственном регулировании шифрованием информации» [39]), которая однозначно устанавливает, что вывозимые (за пределы государства, т.е. США) криптографические средства защиты информации не должны служить препятствием для органов электронной разведки США при добывании ими информации. Другими словами, любые программно-аппаратные средства защиты информации (в том числе и криптографические), используемые в Интернет-сети, являются «прозрачными» для специальных служб США (Приложение 1).

Более того, беглый американский шпион Э. Сноуден опубликовал материалы о деятельности специальных служб США, которые подтвердили глобальность и «глубину проникновения» проводимого ими компьютерного шпионажа [40].

2. Те же угрозы со стороны внутренних преступных сообществ, террористических организаций, радикальных религиозных, нацистских и прочих экстремистских группировок, и антигосударственных сил. В этой связи необходимо отметить тот факт, что специальные службы США (в частности, научно-исследовательская лаборатория военно-морского флота США, *U.S. Naval Research Laboratory*) разработали так называемые «маскирующие ИТС» (МИТС), обеспечивающие маскирование пользователей и передаваемую ими информацию.

Анализ различных зарубежных источников по тематике МИТС показал, что американские спецслужбы популяризируют такие системы путём «восхваления» их, и представляя использование подобных МИТС, как противодействие злоумышленникам и правительственным органам «недемократических» государств, пытающихся вскрыть (отыскать) «беззащитных пользователей» и передаваемую ими информацию с целью последующей дискредитации, вплоть до физической расправы или уголовного преследования со всеми вытекающими последствиями. Это – «спасительный жест доброй воли» со стороны США для «несвободных» граждан других стран.

На самом деле, всё выглядит с точностью «до наоборот». МИТС – это «приманка» для разного рода криминальных и террористических групп («нечистых на руку» пользователей Интернет-сети), которые, используя такие системы, фактически, раскрывают себя и свою противоправную деятельность, что обеспечивает эффективную защиту национальных интересов США и борьбу с преступностью. Более того, деятельность самих правоохранительных органов США «не заметна постороннему глазу». Другими словами, МИТС скрывают преступников от простых пользователей Интернет-сети, но при этом криминальные группы остаются «видимыми» для спецслужб США. Это одна из форм (способ) обеспечения национальной безопасности США.

3. Уход от налогообложения, незаконный вывоз капитала, отмывание преступно полученных доходов с использованием криптовалют (т.е. систем на основе БЧ-технологии, СБЧ).

БЧ-технология [28…31] представляет неизменяемые распределённые системы цифровых реестров без центрального хранилища/репозитария и, как правило, не имеющие единого центра управления. В настоящее время наблюдается большой ажиотаж вокруг использования БЧ-технологии, хотя сама технология, с одной стороны, многим ещё не совсем понятна, а с другой (и это главное) – не нова. Поверхностное представление о БЧ-технологии как о феномене с «волшебными свойствами» приводит к многочисленным прогнозам о возможности революционных преобразований на основе её применения целых отраслей экономики и, прежде

всего, в кредитно-финансовой сфере. Бытует мнение, что СБЧ станут одной из основ цифровой экономики Российской Федерации.

Появление СБЧ было предопределено всеми предшествующими этапами развития информационных технологий (ИТ), постоянно требующих их совершенствования с целью дальнейшего повышения уровня (качества), прежде всего, государственного управления и/или прикладных коммерческих ИТС. Поэтому, несмотря на применение в БЧ-технологии определённых инновационных решений, не стоит переоценивать её «безграничные», революционные возможности применения во всех сферах цифровой экономики. Безусловно, СБЧ займут определённую нишу на рынке ИТ, в частности в сфере развития криптовалютных систем. Но, как и для всяких других прикладных ИТС перспективы их практической реализации будут определяться возможностью выполнения основных принципов обеспечения информационной безопасности [10,29], среди которых аутентификация (персонификация) и обеспечение неотказуемости для всех без исключения участников информационного взаимодействия, обеспечение надёжности подсистемы обеспечения криптоключами.

В настоящее время разработчики и сторонники СБЧ просто игнорируют указанные принципы, либо минимизируют их значимость. Другими словами, СБЧ пока что являются не надёжными системами, которые несут колоссальные материальные и финансовые риски. Отчасти это связано с принципиальной особенностью современных СБЧ, определённым преимуществом которых провозглашается *принцип анонимности*, обеспечивающий практически полное отсутствие централизованного (государственного) регулирования. С другой стороны, его реализация, очевидно, приведёт к появлению новой сферы криминальной (и возможно террористической) деятельности. Таким образом, без решения указанной проблемы фундаментального характера давать какие-либо прогнозы о перспективах применения БЧ-технологий, особенно в сфере государственного управления, цифровой экономики, на объектах критической информационной инфраструктуры, пока что явно преждевременно.

4. Осуществление незаконной предпринимательской деятельности посредством использования Интернет-сети, включая электронную торговлю и финансовые услуги. Фактически, речь идёт о преступлениях в киберпространстве.

По данным МВД за первую половину 2021 года в РФ зарегистрировано свыше 271 тыс. преступлений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, сообщает МВД [41]. При этом доля киберпреступлений в общей структуре преступности превысила 26%. Более половины цифровых преступлений (57%) относится к категориям тяжких и особо тяжких (155 тыс.).

Две трети преступлений совершается через Интернет-сеть, а остальные – с помощью средств мобильной связи. Наибольший прирост IT-преступлений был зафиксирован в Чечне

(177%), Дагестане (141%), Московской (126%) и Тульской (118%) областях, а также в Туве (110%).

Процесс цифровизации криминала в России означает, что число традиционных преступлений снижается, а цифровых – растет. По данным Сбербанка, потери российской экономики от киберпреступлений в 2020 году составили 3,5 трлн руб. А к концу 2021 года – к началу 2022-го они могут достигнуть около 6 трлн руб.

Для борьбы с киберпреступностью, негативно влияющей на создание и совершенствование цифровой экономики, необходимо разработать и внедрить *национальную информационно-технологическую инфраструктуру обеспечения информационной безопасности* (ИТИБ), которая бы предоставляла следующие услуги:

– обеспечение целостности (*integrity*). Услуги по обеспечению *целостности данных* позволяют защитить данные от их неавторизованной или случайной модификации. Такая модификация включает вставку, удаление и замена данных. Для обеспечения гарантий целостности данных, ИТС должна быть способна обнаруживать *неавторизованную* модификацию данных. Цель – получатель данных проверяет, что они не были изменены;

– обеспечение конфиденциальности (*confidentiality*). Услуги по обеспечению *конфиденциальности* ограничивают доступ к содержанию уязвимых (критичных) данных только теми пользователями, которым предоставлено право просмотра данных. Способы и средства обеспечения конфиденциальности предотвращают несанкционированное раскрытие информации неавторизованными пользователями или процессами;

– идентификация и аутентификация (*identification and authentication*). Услуги по *идентификации и аутентификации* обеспечивают подтверждение подлинности передачи, сообщения и его источника (т.е. источник является именно тем, за кого себя выдаёт). Цель – получатель данных определяет их источник и убеждается в его подлинности;

– обеспечение неотказуемости (*non-repudiation*). Услуги по обеспечению *неотказуемости* предотвращают попытку пользователя отказаться от участия в предшествующих действиях. Цель – гарантировать, что получатель данных уверен в надёжности отправителя.

Основными методами, которые способны обеспечить предоставление перечисленных выше услуг обеспечения ИБ, являются *криптографические методы*. *Криптография* – совокупность процедур (функций) преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для злоумышленника. Кроме того, криптографические функции позволяют решить задачу *неотслеживаемости информации*, т.е. невозможности получения нарушителем содержательной информации с помощью наблюдения за действиями законных пользователей, т.е. с помощью перехвата и анализа трафика.

В этой связи, следует отметить, что разработчики Программы в «Дорожной карте» определили следующие этапы обеспечения ИБ, как одного из направлений развития цифровой экономики:

1. В 2018 году должны быть «решены наиболее актуальные проблемы защиты прав и свобод граждан в цифровом пространстве». Не решена ни одна из проблем;

2. В 2020 году должны быть «создан каркас инфраструктуры[4] безопасности цифровой экономики, в том числе в области новейших технологий, обеспечен цифровой суверенитет Российской Федерации». «Каркас инфраструктуры» не создан;

3. В 2024 году «Российская Федерация является одним из мировых лидеров в области информационной безопасности». Это положение Программы говорит о полном невежестве её авторов (незнание истории России). С исторической точки зрения, Россия намного опередила США в этой области, и поэтому она уже *является лидером* в области обеспечения ИБ. Это подтверждают сохранившиеся исторические архивные документы. Первые профессиональные криптографы на Руси появились при Иване Грозном (1530-1584) [42]. Они находились на службе в Посольском приказе, созданном царём в 1549 году, и который отвечал за внешнюю политику страны, т.е. за долго до образования США (1776 год). В одном из архивных документов, в частности, упоминается, что в 1633 году в государстве Российском было издано первое отечественное учебное пособие по криптографии [43]. Более того, *отечественная криптографическая наука занимает передовые позиции* в этой отрасли знаний и способна надёжно защитить (и защищает) национальные интересы Российской Федерации.

Таким образом, исходя из положений Программы, для обеспечения ИБ цифровой экономики нужна соответствующая ИТИБ. Однако, на сегодняшний момент такой инфраструктуры нет, а есть совокупность не связанных между собой СОИБ различных ИТС.

Чтобы понять сущность такой ИТИБ, следует рассмотреть инфраструктуру современной модели экономики. К такой инфраструктуре относятся различные транспортные сообщения (автомобильные и железные дороги, авиасообщения, морские и речные маршруты), первичные сети электросвязи, сети электроснабжения, инженерные коммуникации (водоснабжение, теплоснабжение и т.п.), системы финансово-материального обеспечения и т.д. Одним из главных требований ко всем перечисленным видам инфраструктуры – надёжность и обеспечение безопасности, т.е. предотвращение разного рода экологических катастроф и чрезвычайных происшествий, которые способны нанести серьёзный ущерб здоровью граждан и биосфере, а значит и экономике в целом.

[4] Авторы Программы не дали определение термина «каркас».

Если проанализировать, например, системы общественного транспорта, то *пассажиры доверяют надёжности транспортных средств* (автобусов, трамваев, поездов, самолётов, кораблей и т.д.) и *безопасности самих транспортных магистралей* (автодорогам, железнодорожным путям, авиационным и водным маршрутам). Такое доверие основано на сертификации транспортных средств, которые оснащены всеми соответствующими (необходимыми) средствами безопасности, и паспортизации транспортных магистралей, которые включают все необходимые средства управления и обеспечения надёжного (безаварийного) движения транспортных средств.

Следовательно, ИТИБ должна объединить СОИБ существующих и перспективных ИТС, гарантировать надёжную доставку данных, которыми обмениваются взаимодействующие стороны (субъекты, объекты), и предоставлять для взаимодействующих сторон перечисленные выше услуги по обеспечению ИБ, а это станет основой *доверия* граждан и организаций к ИТИБ.

1.5 Информационно-телекоммуникационная инфраструктура цифровой экономики

По мнению некоторых экономистов, например, [44,45], цифровая трансформация пройдёт несколько этапов преобразований, даже несмотря на различия процессов такой трансформации в каждой отдельной социально-экономической системе. Другими словами, существует ряд ключевых, общих для всех этапов, отражающих суть процесса цифровой трансформации.

Во-первых, планирование, которое должно учесть все экономические потребности организаций. В начале процесса цифровой трансформации очень важно определить направления развития, а также совокупность технологий, которые помогут в этом развитии. При этом потребуется инвентаризация имеющихся ресурсов, включая информационные, выделив из них те, которые необходимо модернизировать. На этом этапе может даже потребоваться пересмотр приоритетов в проектах с учётом новых экономических потребностей, а также выявление недостатков и пробелов, которые могут стать препятствием на пути цифровой трансформации.

Во-вторых, вопросы кадрового обеспечения. Тут уместен известный исторический тезис, что «*кадры решают всё*». Но прежде кадры необходимо обучить навыкам работы с новыми технологиями. Этот процесс может вызвать множество трудностей, поскольку при современных экономических моделях сотрудники организаций различных форм собственности должны были знать только определённые системы, которые планировалось использовать ещё многие годы. Для успеха цифровой трансформации сотрудники должны быть готовы к любым возможным изменениям рабочих процессов, если эти изменения необходимы для повышения

эффективности и продуктивности производственной деятельности. Такая готовность означает и умение мыслить творчески, и знание потенциала новых технологий, и умение использовать их с максимальной эффективностью.

И в-третьих, отказ от устаревших технологий в пользу инновационных. Сохранение и модернизация старых технологий зачастую препятствует развитию организаций в целом. На обслуживание старых технологий тратится множество ресурсов, которые можно было бы потратить на внедрение новых технологий, более простых в использовании, повышающих эффективность и качество производства и обслуживания заказчиков, а также ускоряющих анализ экономических и иных данных, необходимых при принятии решений. Очевидно, что переход организаций к модели цифровой экономики предусматривает, в первую очередь, внедрение в их основную экономическую деятельность передовых ИТС с учётом рисков для организаций, связанных с (*а*) использованием самих ИТС и (*б*) взаимодействием со своими партнёрами и (*в*) потребителями.

Вместе с тем, любая ИТС и обрабатываемая в ней информации должны быть защищены путём решения (с помощью СОИБ) следующих *частных задач обеспечения ИБ*:

1. *Доступность* (систем и данных только для их использования по предназначению). Доступность представляет собой требование, предназначенное для обеспечения гарантий того, что система функционирует без задержек и для авторизованных пользователей не будет отказов в обслуживании. Решение этой задачи позволяет предотвратить:
    1.1. Преднамеренные или случайные попытки, направленные на:
        1.1.1. Осуществление неавторизованного удаления данных, или;
        1.1.2. Создание нештатной ситуации, связанной с отказом в обслуживании и доступе к данным;
    1.2. Попытки использования системы или данных в противоправных целях.

Доступность в большинстве случаев – первоочередная задача обеспечения ИБ;

2. *Целостность* (системы и данных). Целостность имеет два аспекта:
    2.1. Целостность данных (свойство, при котором данные не могут изменяться противоправным способом при их хранении, обработке и передаче);
    2.2. Целостность системы (качественная характеристика, при реализации которой система в период своего функционирования в штатном (не изменённом) режиме свободна от всякого рода противоправных манипуляций);

Целостность является наиболее важной задачей обеспечения ИБ для организации после доступности.

3. *Конфиденциальность* (данных и системной информации). Конфиденциальность представляет собой требование, в соответствие с которым частная и конфиденциальная информация должна быть не раскрываемой для неавторизованных пользователей. Защита конфиденциальности применяется к данным в процессе их хранения, обработки и передачи.

Для многих организаций конфиденциальность весьма часто является менее важной по сравнению с доступностью и целостностью. И всё-таки, для некоторых систем и определённых типов данных *конфиденциальность чрезвычайно важна*;

4. *Идентифицируемость* (для отдельного уровня Интернет-архитектуры [134]). Идентифицируемость представляет собой требование, в соответствие с которым все действия субъекта могут быть однозначно отслежены и зафиксированы для данного субъекта.

Идентифицируемость очень часто является требованием стратегии безопасности организации и *непосредственно обеспечивает неотказуемость*, воспрепятствование противоправным действиям, локализацию ошибок, выявление и парирование вторжений, а также последующее восстановление и проведение требуемых мероприятий.

5. *Гарантированность* (того, что все предшествующие четыре задачи решаются (или решены) адекватно). Гарантированность является основой убеждённости (доверия) в том, что средствам обеспечения безопасности (и технические, и эксплуатационные) работают по своему прямому предназначению, то есть защищают систему и реализуемые в ней процессы обработки информации. Считается, что предыдущие четыре задачи (целостность, доступность, конфиденциальность и идентифицируемость) решаются (или решены) адекватно, когда:

5.1. Обеспечена необходимая функциональность, и она корректно реализуется;

5.2. Имеет место эффективная защита от непреднамеренных ошибок и сбоев (вызванных пользователями или программным обеспечением);

5.3. Имеет место эффективная система нейтрализации преднамеренного преодоления защиты или её обхода.

Гарантированность является очень важной задачей, без решения которой не могут быть решены другие задачи обеспечения ИБ. Однако, обеспечение гарантированности является изменяемой задачей. То есть необходимое число гарантий (уровень гарантированности) зависит от конкретной системы.

Решение указанных выше задач предусматривает создание в каждой организации СОИБ в рамках корпоративной (ведомственной) ИТС.

Переход к цифровой экономике повлечёт за собой объединение ИТС (вместе с СОИБ) различных организаций в *единую ИТИЦЭ* на основе первичной сети электросвязи (передачи данных, рисунок 1.2). Очевидно, что обязательной подсистемой ИТИЦЭ должна стать ИТИБ,

к задачам которой относятся, помимо предоставления перечисленных выше услуг по обеспечению ИБ, (1) защита первичной сети электросвязи и (2) формирование *единой системы доверия* в интересах цифровой экономики, так как без доверия к ИТИЦЭ она не будет востребована гражданами и бизнесом, либо такое доверие будет иррациональным с вытекающими отсюда негативными последствиями.

Рисунок 1.2 – Модель единой информационно-телекоммуникационной инфраструктуры цифровой экономики

В этой связи следует отметить, что Минцифры при формировании единой ИТИЦЭ делает основной акцент именно на создании современной первичной сети электросвязи (передачи данных). Вместе с тем, вопросы обеспечения ИБ практически не рассматриваются.

1.6 Проблема обеспечения доверия к ИТИЦЭ (ИТИБ)

При анализе ИБ приходится учитывать и психологию человека. Классическая цель ИБ – предотвратить угрозы (нарушения), связанные с обеспечением конфиденциальности, целостности, доступности и неотказуемости, с помощью внедрения средств нейтрализации угроз, которые, как правило, описываются в технических требованиях к ИТС, и, в частности, к СОИБ. Цель функционирования средств нейтрализации угроз – сформировать доверие, которое представляет собой феномен человека. Доверие может помочь клиентам использовать

ИТС теми способами, которые бы они избегали в условиях отсутствия доверия, и поэтому на практике ИТС становится более значимой и более мощной системой.

Доверие – это очень общее понятие, которое можно использовать практически в любом контексте, и представляет собой *степень, с которой один субъект готов зависеть от чего-то или кого-то в конкретной ситуации, ощущая при этом относительную безопасность, даже если возможны и негативные последствия*. С точки зрения обеспечения ИБ, целесообразно придать доверию более конкретное смысловое значение, которое может быть необходимым при формальном моделировании ИТИБ.

Основная причина необходимости обеспечения ИБ заключается в том, что некоторые злонамеренные субъекты в конкретной ситуации могут попытаться атаковать ИТС, а СОИБ должна отражать такие атаки. Как правило, наличие злонамеренного функционирования субъектов в ИТС – причина не только обеспечения ИБ, но также – необходимое и обязательное условие формирования доверия.

Доверие должно основываться на объективном доказательстве. Иррациональное доверие основано не на объективных доказательствах, а, например, на вере или на неопределённом и «туманном» чувстве, которое не может быть логически обосновано, и иногда такое доверие может «упорно» сохраняться, даже несмотря на наличие доказательств обратного. Даже если доверие, в конечном счёте, субъективно, то одним из преимуществ будет общее суммарное доверие максимально большего числа пользователей, которое основано на одних и тех же объективных доказательствах. Как правило, можно ожидать, что и разработчики будут доверять своим (создаваемым ими) ИТС аналогичным образом. Однако существуют признаки того, что *это не всегда бывает правилом*.

Разработчик, знающий уязвимости в ИТС, которую он создал, может отказаться от раскрытия такой информации по нескольким причинам. Одной из более или менее объективных причин такого отказа может быть то, что, публикуя такую информацию, потенциальные нарушители могут узнать о системных уязвимостях столько же, сколько и правомочные пользователи. В конце концов, если никто не знает об уязвимости, она и не будет использована. Тем не менее, такая стратегия может быть весьма опасной, и если злоумышленник сможет обнаружить и использовать уязвимость, о которой уже знал производитель, то негативные последствия могут быть серьёзными.

Люди часто бывают иррациональны, как и доверие. Это может быть незначительной или значительной проблемой для самого пользователя, так как это, по крайней мере, его собственный выбор. С другой стороны, такая ситуация может быть опасной для разработчиков ИТС, так как возможно в дальнейшем, что они не смогут восстановить нарушенное доверие с помощью объективных доказательств. Естественно, разработчики ИТС хотят сформировать

максимально возможное общественное доверие к своим системам, в то время как реальное доверие пользователей не всегда может быть основано на объективных доказательствах. Здесь может быть только одна рекомендация – желательно, чтобы разработчики всегда раскрывали (при необходимости и под жёстким контролем) все относящиеся к безопасности доказательства, которые пользователи объективно должны знать, а пользователи должны стараться обосновывать своё доверие, главным образом, с помощью объективных доказательств.

Пользователь ИТС никогда не сможет получить полную информацию о системе, которой он пользуется, ни о внешних или внутренних угрозах. Более того, он не способен определить точный уровень защищённости ИТС. Собрав как можно больше данных об ИТС, пользователь получит представление или убеждённость в её безопасности, или, другими словами, он сформирует некоторое доверие к системе. С этой точки зрения, безопасность может рассматриваться как идеалистическая цель разработчиков ИТС, в то время как доверие представляет собой фактическое неполное знание пользователей о том, насколько были успешны разработчики при достижении своей идеалистической цели. Такая ситуация, характеризующаяся неполным знанием ИТС, будет всегда иметь место, а проблема, с которой приходится сталкиваться, заключается в том, как такую ситуацию преодолеть.

1.6.1 Прямое доказательство уровня защищённости

Всесторонняя оценка защищённости системы в условиях неполного знания ИТС будет основываться на доказательствах, полученных из различных источников. Между прямым и косвенным доказательствами можно провести различие. *Прямое доказательство* – доказательство, полученное в результате исследования системы, например, путём оценки защищённости, а также путём непосредственной эксплуатации системы и, следовательно, на основе полученного опыта. *Косвенное доказательство* – доказательство, например, на основе рекомендаций и предложений. Прямые доказательства могут быть сгруппированы в системное доказательство, доказательства на основе данных о сетевой среде и об инциденте, затрагивающем обеспечение ИБ. Такое группирование хорошо сочетается с типовой моделью анализа рисков, представленной на рисунке 1.3.

В соответствии с моделью анализа рисков, анализ и объединение данных об угрозах (сетевая среда, например, Интернет-сеть) и уязвимостях (недостатки и ошибки в ИТС и, в частности, в СОИБ) порождают вероятности практических нарушений ИБ, но только функционирование ИТС может показать, реализуются ли на практике какие-либо из этих возможных нарушений в форме инцидентов ИБ. Реализованное на практике возможное нарушение ИБ – это самое худшее из того, что может произойти, и поэтому необходимо, чтобы ИТС обладала очень высоким уровнем защищённости, а СОИБ могла противостоять реальным нарушениям.

Тем не менее, одна из целей анализа рисков заключается в том, чтобы уравнять стоимость обеспечения ИБ (СОИБ) с потерями, которые вызваны реальными нарушениями ИБ. Прямое следствие этого заключается в том, что «адекватное» доверие к ИТС и входящей в неё СОИБ – реальная цель самой ИТС и входящей в неё СОИБ.

Рисунок 1.3 – Прямое доказательство уровня защищённости ИТС

1.6.2 Косвенное доказательство уровня защищённости

С интуитивной точки зрения, человек склонен доверять тому, кому доверяют те, которых он уже знает и которым он доверяем сам. Этот принцип широко используется и службах обеспечения безопасности, например, когда субъект должен полагаться на доверенные третьи стороны (ДТС), центры распространения криптографических ключей или центры сертификации с целью формирования доверия к ИТС.

Если пользователь не способен получить прямое доказательство с целью формирования своего доверия к системе, либо потому, что он не имеет доступа к ней, либо потому, что он не обладает опытом, чтобы оценить её, то он зависит от косвенных доказательств. Посредник может порекомендовать в обратном направлении, что следующему за ним субъекту в цепочке можно доверять, и так далее, пока не будет достигнут целевой субъект (цепочка доверия). Такого рода рекомендации могут быть формальными и в явном виде, например, выдача сертификата соответствия по результатам проведённой экспертизы, или неявными, например, когда пользователь просто доверяет ИТС, потому что другие пользователи, которым он сам доверяет, используют ту же систему и, возможно, доверяют ей.

На рисунке 1.4 показан один из возможных способов оценки системы пользователем, относительно которой он не способен получить прямых доказательств. Доказательства, к которым он имеет прямой доступ, могут поступать от других пользователей, центра сертификации, консультантов, аналитиков и т.п. Их доказательства могут, в свою очередь, поступать от

экспертов (специалистов по оценке) или производителей, которые имеют доступ к прямым доказательствам.

На рисунке 1.4 представлена последовательность доказательств в случае оценки защищённости. В реальной жизни, пользователь обычно будет иметь доступ, как правило, к различным типам как прямых, так и косвенных доказательств. Например, он может получить прямое доказательство из результатов анализа инцидентов ИБ, произошедших в течение функционирования ИТС, или анализа угроз, существующих в сетевой среде, в которой функционирует ИТС. В дополнение к отчёту об экспертной оценке защищённости он может получить косвенные доказательства в виде рекомендаций по ИБ. Различие между прямым и косвенным доказательствами заключается в том, что первое следует из прямого непосредственного наблюдения за системой и сетевой средой, в которой система функционирует, а второе следует от посредников (мыслящих субъектов), которыми могут быть люди, коллективы или общественность в целом. Поэтому пользователь обязан учитывать возможное злонамеренное или иррациональное поведение посредников.

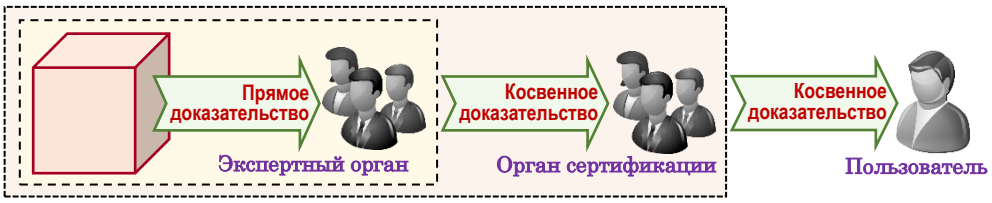

Рисунок 1.4 – Косвенное доказательство уровня защищённости ИТС

Строго говоря, неверно считать, что доверие само по себе «плавно течёт» через посредников. Рекомендация доверенной стороны доверять той или иной ИТС на самом деле является только частью доказательства, которое пользователь должен сам рассматривать вместе с другими частями доказательства. В результате, все части доказательства сформируют у пользователя субъективное убеждение, которое и будет его доверием к ИТС.

Таким образом, разработка и внедрение ИТС, включающей СОИБ, должны предусматривать процедуры формирования доверия у граждан и бизнеса, которые будут её активными пользователями, а основа такого доверия – высокий уровень защищённости ИТС. Если ИТС, входящие в состав ИТИЦЭ, будут обладать высоким уровнем защищённости, то можно говорить и о высоком уровне защищённости всей ИТИЦЭ.

1.7 Информационно-технологические инфраструктуры обеспечения безопасности на основе инфраструктуры открытых ключей

Опыт зарубежных экономически развитых государств (например, США и Евросоюз) показывает, что современные ИТИБ представляют собой инфраструктуры открытых ключей

(ИОК, *Public Key Infrastructure – PKI*), на основе которых строятся различные модели систем управления криптографической защитой в ИТС. Такие системы формируют доверие между взаимодействующими в киберпространстве субъектами.

Название ИОК происходит от названия одной из отраслей криптографической науки *криптографии с открытыми ключами* (или ассиметричных криптографических систем, АКС). В АКС используется класс алгоритмов, в которых субъект $\mathcal{A}$ имеет закрытый ($private$) ключ $\mathcal{K}_3$, а другой субъект информационного взаимодействия $\mathcal{B}$ (а также другие участники информационного взаимодействия) имеет открытый ($public$) ключ $\mathcal{K}_0$ субъекта $\mathcal{A}$. Открытый и закрытый ключи формируются одновременно, а данные зашифровываются с помощью $\mathcal{K}_0$ и могут расшифровываться с помощью $\mathcal{K}_3$. Другими словами, любой может зашифровать сообщение с помощью $\mathcal{K}_0$ субъекта $\mathcal{A}$, и потом только субъект $\mathcal{A}$, владелец парного $\mathcal{K}_3$, может расшифровать полученной зашифрованное сообщение.

Ассиметричные алгоритмы не совсем подходят для зашифрования больших сообщений, так как они относительно медленны (т.е. требуют проведение значительно большего количества вычислительных операций по сравнению с симметричными алгоритмами). Но зато, эти алгоритмы используются для проведения процедур аутентификации, обеспечения целостности и неотказуемости, а также для защиты конфиденциальности при обеспечении ключами. Ассиметричные алгоритмы используются при проведении трёх процедур: формирование электронных подписей (ЭП), доставка ключей и согласование ключей.

1.7.1 Электронная подпись

Субъект $\mathcal{A}$ может сформировать ЭП сообщения, используя для этого компендиум[5] сообщения и свой закрытый ключ. Для аутентификации субъекта $\mathcal{A}$, как отправителя, другой субъект $\mathcal{B}$ также формирует компендиум сообщения и использует $\mathcal{K}_0$ субъекта $\mathcal{A}$ для подтверждения подлинности ЭП. Если для формирования ЭП использовался другой $\mathcal{K}_3$, то результат подтверждения подлинности ЭП будет отрицательный.

ЭП позволяют проверить целостность данных. Если данные были искажены после формирования ЭП, то при проверке будет сформирован другой компендиум сообщения. А это повлечёт формирование другой (не совпадающей) ЭП. Таким образом, если целостность данных была нарушена, то процедура проверки ЭП даст отрицательный результат.

В некоторых ситуациях, ЭП может использоваться для обеспечения неотказуемости. Если субъект $\mathcal{B}$ может продемонстрировать, что только субъект $\mathcal{A}$ является владельцем $\mathcal{K}_3$, то

[5] Результат вычисления однонаправленной функции по последовательности всех символов, входящих в сообщение.

субъект $\mathcal{A}$ не сможет отказаться от формирования ЭП. Как правило, субъекту $\mathcal{B}$ придётся полагаться на ДТС, чтобы удостовериться, что субъект $\mathcal{A}$ обладал $\mathcal{K}_3$.

Кроме того, ЭП используются при проведении аутентификации в ИТС. В ИТС можно подтвердить параметр подлинности субъекта $\mathcal{A}$, используя для этого запросно-ответный протокол информационного обмена. ИТС формирует случайным образом запрос, а субъект $\mathcal{A}$ подписывает его. Если ЭП подтверждается с помощью открытого ключа субъекта $\mathcal{A}$, то ЭП могла быть сформирована только субъектом $\mathcal{A}$. Этот тип аутентификации наиболее приемлем там, где обеспечивается удалённый доступ к информации, размещённой, например, в сервере, т.е. система сетевого управления защищается от атак типа «маскарад» (*masquerade*), или там, где обеспечивается физический доступ в особо охраняемую (запретную) зону.

1.7.2 Доставка ключей

Некоторые ассиметричные алгоритмы (например, RSA-алгоритм[6]) могут использоваться для зашифрования и расшифрования данных. На практике эти алгоритмы никогда не используются для зашифрования больших объёмов данных, так как они значительно медленнее алгоритмов с симметричными ключами. Тем не менее, эти алгоритмы весьма приемлемы для зашифрования данных небольших размеров – например, симметричных ключей. Эта процедура носит название «доставка ключей» или «обмен ключами», и используется во многих протоколах [46]. Следующий пример демонстрирует доставку электронного почтового сообщения от субъекта $\mathcal{A}$ субъекту $\mathcal{B}$:

• субъект $\mathcal{A}$ формирует AES[7]-ключ [47] и зашифровывает сообщение. Субъект $\mathcal{A}$ зашифровывает AES-ключ, используя для этого $\mathcal{K}_0$ субъекта $\mathcal{B}$, и передаёт субъекту $\mathcal{B}$, и зашифрованный ключ, и зашифрованное сообщение;

• субъект $\mathcal{B}$ использует свой $\mathcal{K}_3$ для расшифрования AES-ключа субъекта $\mathcal{A}$, а затем он расшифровывает с помощью AES-ключа субъекта $\mathcal{A}$ зашифрованное сообщение и получает открытый текст.

В этом случае, субъект $\mathcal{A}$ использует ассиметричную криптографию для обеспечения конфиденциальности при распределении ключа (так называемый «*принцип нулевого разглашения*», *zero knowledge*). Эта процедура не может обеспечить дополнительных услуг безопасности, так как субъект $\mathcal{A}$ использует $\mathcal{K}_0$ субъекта $\mathcal{B}$, а сообщение мог сформировать кто бы то ни было.

---

[6] RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) – криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

[7] Усовершенствованный стандарт шифрования (*Advanced Enciphering Standard*) – алгоритм симметричного блочного шифрования.

1.7.3 Согласование ключей

Другие ассиметричные алгоритмы (например, алгоритм *Диффи-Хэллмена*[8] [48]) могут использоваться для согласования ключей [49]. Предположим, что субъекты $\mathcal{A}$ и $\mathcal{B}$, каждый, формируют пару ключей с использованием алгоритма Диффи-Хэллмена. Субъект $\mathcal{A}$ обладает своим $\mathcal{K}_3$ и $\mathcal{K}_0$ субъекта $\mathcal{B}$. В свою очередь, субъект $\mathcal{B}$ обладает своим $\mathcal{K}_3$ и $\mathcal{K}_0$ субъекта $\mathcal{A}$. С помощью математического алгоритма субъекты $\mathcal{A}$ и $\mathcal{B}$, оба, формируют одно и то же значение «уникального слова» (*secret*). Субъект $\mathcal{C}$ может обладать обоими открытыми ключами, но он не сможет вычислить значение этого «уникального слова». Субъекты $\mathcal{A}$ и $\mathcal{B}$ могут использовать значение «уникального слова», которое они вычислили независимо друг от друга, в качестве AES-ключа и защитить свои сообщения при проведении процедуры информационного обмена.

Существуют и другие способы согласования ключей, которые также обеспечивают безусловную (скрытую) аутентификацию. Если субъект $\mathcal{B}$ может восстановить открытый текст, то он убеждается в том, что только субъект $\mathcal{A}$ мог зашифровать этот текст. Так как, только он мог сформировать такое же значение «уникального слова».

1.7.4 Инфраструктура открытых ключей

Очевидно, что криптографические способы, в своей совокупности, востребованы при реализации всего комплекса услуг по обеспечению безопасности. Каждый класс алгоритмов обладает своими преимуществами и недостатками.

Симметричные криптоалгоритмы необходимы при обеспечении конфиденциальности. Кроме того, эти алгоритмы способны обеспечить, в некоторой степени, целостность и аутентификацию, но они полностью не приемлемы для обеспечения неотказуемости. «Ахиллесовой пятой» для симметричных криптоалгоритмов, несмотря ни на что, является процедура распределения ключей.

Ассиметричные криптоалгоритмы являются высокоэффективными при обеспечении целостности, аутентификации и распределении ключей. Алгоритмы формирования ЭП используют алгоритмы вычисления однонаправленных функций для обеспечения высокой эффективности.

Система управления криптографической защитой на основе (инфраструктуры) открытых ключей реализует все перечисленные выше криптографические способы обеспечения ИБ и объединяет ДТС, которые определяют её структуру. ДТС, которые именуются *центрами*

---

[8] *Diffie-Hellman* — алгоритм, позволяющий двум сторонам получить общий секретный ключ, используя незащищённый от прослушивания, но защищённый от подмены, канал связи.

сертификации (ЦС) и *центрами регистрации* (ЦР), реализуют процедуры обеспечения неотказуемости на основе применения ЭП. ЦС и ЦР привлекаются для формирования параметра подлинности (ПП) владельца $\mathcal{K}_З$, что существенно упрощает решение проблемы идентификации и аутентификации, и, соответственно, неотказуемости. Кроме того, системы управления криптографической защитой на основе (инфраструктуры) открытых ключей обеспечивают процедуры распределения ключей, и на их основе формируются *системы доверия* со стороны пользователей ИТС.

Мировой опыт показывает, что для обеспечения основных направлений своей экономической деятельности большинство ИТС, включающих прикладные государственные и коммерческие АИС, используют системы управления криптографической защитой на основе (инфраструктуры) открытых ключей с целью реализации всей совокупности служб обеспечения ИБ.

1.8 Национальная ИОК в Российской Федерации

Национальная ИОК в Российской Федерации находится на этапе своего становления, она ещё не сформировалась и не стала полнофункциональной системой, которая способна решать задачи обеспечения ИБ. Процесс развития национальной ИОК, практически, приостановлен. Минцифры не уделяет должного внимания созданию эффективной национальной ИОК, ограничиваясь ведением Реестра состояния доверенных служб. Такое «бездействие» является следствием отсутствия государственной политики развития ИОК, как основы обеспечения безопасности ИТИЦЭ. ИОК в Российской Федерации представляет собой большое число УЦ, большая часть которых не входит в какие-либо ИТС, и которые никак не объединены в единую систему, способную защитить цифровую экономику.

Анализ современного состояния национальной ИОК показывает, что все УЦ, независимо от их форм собственности (государственные или частные), зарегистрированные Минцифры в Реестре состояния доверенных служб (РСДС), построены по чрезвычайно уязвимой схеме, которая предусматривает объединение двух центров в один: «УЦ ≡ ЦС + ЦР». Выбор такой модели ДТС в России был предопределён желанием организаций, создающих УЦ, предотвратить риск, связанный с выбором ЦР и взаимодействием с ним. УЦ самостоятельно устанавливает и контролирует содержание $\text{СЕРТ}_{\text{ОК}}$, включая (возможно удалённый) контроль ЦР по защищённому каналу связи. Другими словами, это резко снижает доверие к УЦ, так как он может осуществлять мошенническую сертификацию (издавать фальсифицированные $\text{СЕРТ}_{\text{ОК}}$ на имя пользователя такого УЦ, т.е. пользователь становится «жертвой» мошеннической сертификации) для достижения своих корыстных целей или в условиях давления криминальных структур. В такой ситуации уязвимым становиться пользователь такого УЦ (ИОК).

Более того, сами сотрудники УЦ могут быть мошенниками, или стать «жертвами» шантажа преступников, или быть в сговоре с криминалом. В таких ситуациях, они, получив преступным путём персональные данные физического лица, не являющегося клиентом их УЦ, способны выпустить на его имя фальшивый СЕРТ$_{ОК}$ и использовать последний при проведении разного рода финансовых и имущественных транзакций. В частности, стал известен новый изощрённый способ «честного отъёма» недвижимости у граждан [146], особенно у людей преклонного возраста (пенсионеров), сущность которого в следующем (рисунок 1.5, [200]).

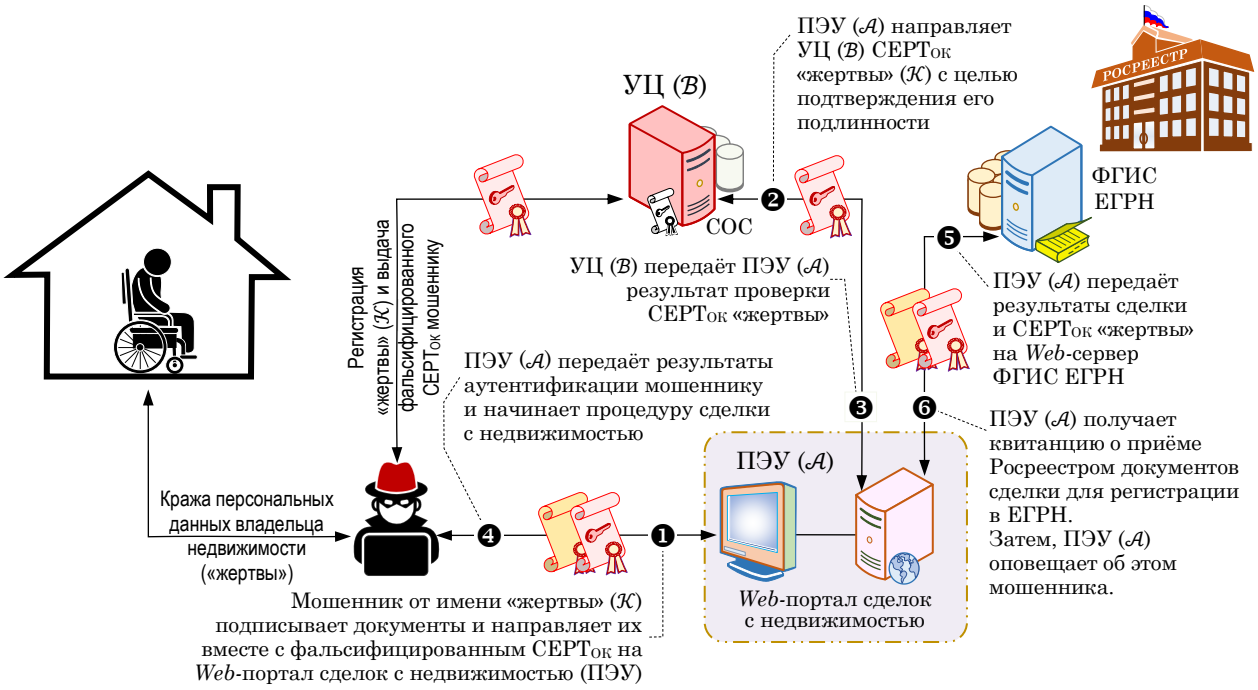

Рисунок 1.5 – Модель мошеннической схемы «отъёма недвижимости» с использованием национальной ИОК в Российской Федерации

Мошенники преступным путём узнают пожилого владельца квартиры (как правило одинокого и немощного), «добывают его персональные данные» и через коррумпированных (или шантажируемых) сотрудников УЦ получают фальшивый СЕРТ$_{ОК}$. Далее преступники с помощью фальшивого СЕРТ$_{ОК}$ проводят электронные сделки с недвижимостью «жертвы» (которая де-юре является владельцем фальшивого СЕРТ$_{ОК}$), например, совершают акт дарения подставному лицу (также находящемуся в криминальном сговоре). Тем более, такая процедура, в принципе, не вызовет подозрений, т.е. пожилой человек перед смертью решил подарить свою недвижимость дальнему родственнику или кому-то другому. Преступники рассчитывают и на то, что ничего не подозревающий истинный владелец квартиры вряд ли узнает о совершённом акте дарения недвижимости, т.е. он не будет направлять запрос о собственной квартире в Единый государственный реестр недвижимости (ЕГРН) до конца своей жизни. Единственный документ, который может раскрыть факт смены владельца недвижимости, –

платёжный документ за оказанные жилищно-коммунальные услуги и энергопотребление. Для снижения такого «риска» (провала мошеннической операции), преступники перепродают квартиру многократно среди членов преступной группы, а это отдаляет момент регистрации нового владельца и передачу такой информации в муниципальные органы жилищно-коммунального хозяйства (ЖКХ). Они также рассчитывают на то, что старый человек вряд ли обнаружит в платёжном документе ЖКХ фамилию нового владельца квартиры вследствие, например, плохого зрения или ограниченности его когнитивных способностей. А после кончины настоящего владельца квартиры, последняя без каких-либо препятствий переходит в собственность мошенника, который поступит с ней по своему усмотрению.

Очевидно, что это – «современный технологичный способ» незаконного овладения чужой недвижимостью, причём скрытый и не вызывающий каких-либо подозрений, и который основан на несовершенстве (уязвимости) КЗСУ на основе ИОК ИТС. Здесь следует отметить ещё одну очень важную уязвимость ИОК – неспособность ИОК и, соответственно, ЕГРН проверить законность (обоснованность) выпуска $СЕРТ_{ОК}$ и автоматическая регистрация Росреестром мошеннической сделки и нового(ых) владельца(ев) недвижимости (вследствие доверия к фальшивому $СЕРТ_{ОК}$).

Таким образом, модель «УЦ ≡ ЦС + ЦР» обладает очень низким уровнем безопасности и серьёзной уязвимость по сравнению с системой, в которой ЦС мог бы находится под контролем государственного ведомства. Указанная модель позволяет некоторому УЦ формировать содержание $СЕРТ_{ОК}$, фальсифицировать контент и издавать мошеннический $СЕРТ_{ОК}$. В Российской Федерации были вскрыты факты противоправной деятельности отдельных УЦ, от которой пострадали ни в чём неповинные граждане [3,41,143…146].

Следовательно, КЗСУ (системы доверия) на основе ИОК ИТС в РФ стали наукоёмкими технологическими *системами, способствующими совершению различных киберпреступлений*! В этой связи необходимо ускоренное преобразование и реализация новой модели КЗСУ (системы доверия) на основе ИОК ИТС, а также создание на основе объединения КЗСУ ИТС *национальной системы доверия* в интересах цифровой экономики Российской Федерации, что является *стратегической задачей*, решение которой носит безотлагательный характер.

1.9 Проблема уникальности параметров подлинности в рамках национальной инфраструктуры открытых ключей

Решение стратегической задачи построения на базе ИОК ИТС национальной ИОК в Российской Федерации предусматривает и решение частной, но не менее важной задачи – создание национальной системы уникальных ПП на основе уникальных идентификаторов

(УИД). Эта задача – прямое следствие решения проблемы нейтрализации угроз безопасности цифровой экономики Российской Федерации. В §1.5 рассматривались задачи обеспечения ИБ, среди которых была проанализирована *задача обеспечения идентифицируемости*, решаемая системой управления криптографической защитой на основе (инфраструктуры) открытых ключей. В частности, применение ЭП и СЕРТ$_{ОК}$, содержащих УИД, позволяет решить эту задачу.

За последнее время участились случаи *создания и использования поддельных Web-сайтов* (гипертекстовые АИС, ГАИС), которые дублируют подлинные ГАИС, принадлежащие конкретным законным ПЭУ, и тем самым вводят в заблуждение пользователей Интернет-сети. Злоумышленники, использующие поддельные *Web*-сайты, «выманивают» у пользователей их персональные данные, включая любую банковскую информацию, и в дальнейшем проводят незаконные финансовые операции от имени реальных владельцев банковских счетов. Кроме того, более изощрённой мошеннической деятельностью является продажа через поддельные *Web*-сайты фальшивых железнодорожных или авиабилетов, билетов на различные культурно-спортивные мероприятия и фиктивных туристических путёвок [143].

Причина такой противоправной деятельности – неспособность системы управления криптографической защитой на основе (инфраструктуры) открытых ключей в ИТС вскрыть факты мошенничества и отсутствие единой системы идентификации субъектов и объектов в Интернет-сети, в частности, в её российском сегменте. Основной формой данных, используемой в ИОК, является СЕРТ$_{ОК}$, который с помощью криптографического способа «привязывает» УИД (ПП) владельца сертификата к его $\mathcal{K}_0$. *Фактически ИОК формирует систему доверия на основе СЕРТ$_{ОК}$*, которая позволяет ИОК-пользователям удостовериться в подлинности взаимодействующих с ними субъектами.

На практике возможны два варианта разработки и применения мошеннических *Web*-сайтов:

1. Злоумышленник (злонамеренный ПЭУ) устраивает «маскарад», управляя поддельным *Web*-сайтом, и *использует украденный СЕРТ$_{ОК}$*[9], принадлежащий законному ПЭУ, *Web*-портал которого имитирует злоумышленник;

2. Злоумышленник (злонамеренный ПЭУ) устраивает «маскарад», управляя поддельным *Web*-сайтом, который имитирует *Web*-портал, принадлежащий законному ПЭУ, но при этом, злоумышленник *использует свой собственный СЕРТ$_{ОК}$*, полученный электронным

[9] Потенциальной угрозой для безопасности самого сертификата является угроза, при которой нарушитель выдаёт себя за истинного владельца сертификата, который указан в этом СЕРТ$_{ОК}$. Такое несанкционированное использование сертификата называется *кражей сертификата* [92,110].

способом в зарубежном УЦ, и подлинность которого подтвердить на территории РФ не представляется возможным вследствие отсутствия трансграничного взаимодействия отечественной ИОК с ИОК других государств.

Для распознавания поддельных (мошеннических) *Web*-сайтов необходим способ (специализированный КПО), который реализует проверку и подтверждение подлинности $СЕРТ_{ОК}$ ПЭУ со стороны пользователя, инициализирующего такую процедуру [201].

В настоящее время основой электронного информационного взаимодействия является глобальная Интернет-сеть (её российский сегмент), соответствующая 5-уровневой модели взаимодействия открытых прикладных систем (Интернет-архитектура [134]). Однако, управление Интернет-сетью, в частности, распределение глобальных сетевых идентификаторов, осуществляется структурами, подконтрольными США. А так как США рассматривают Интернет-сеть в качестве инструмента захвата мирового киберпространства и глобального компьютерного шпионажа (§1.4), они не допустят, чтобы национальные системы уникальных параметров подлинности (УИД) на основе глобальных Интернет-идентификаторов стали частью международной системы идентификации Интернет-пользователей [40]. При этом невозможно представить, что в ближайшей перспективе ситуация изменится.

Другими словами, в глобальном масштабе необходима *международная система идентификации Интернет-пользователей*, которая позволит резко снизить уровень киберпреступности на основе точной идентификации злоумышленников и при условии выполнения принципа «неотвратимости наказания». Международная система идентификации Интернет-пользователей должна охватывать все государства, и при этом каждая страна должна иметь свою уникальную (неповторяющуюся) область идентификаторов для своих граждан, организаций и систем, которые пользуются услугами глобальной Интернет-сети.

Таким образом, проблемы обеспечения ИБ, которые следуют из процессов формирования цифровой экономики Российской Федерации, являются системными и комплексными (междисциплинарными). И поэтому принимаемые решения должны быть такими же.

1.10 Постановка задач диссертационной работы

На основе проведённого анализа проблем обеспечения ИБ цифровой экономики в Российской Федерации можно заключить, что в России назрела *острейшая проблема реформирования и совершенствования существующей национальной ИОК*, являющейся основой ИТИБ. Предложенная Правительством РФ Программа «Цифровая экономика в Российской Федерации» не содержит целевых установок и способов решения проблем обеспечения информационной безопасности в условиях цифровой экономики, а содержит только констата-

цию необходимости решения указанных проблем. Более того, авторы Программы сами признают, что она является следствием рекомендаций Давосского форума 2015 года, которые направлены на повышение уровня влияния *технологий манипуляции общественного сознания и управления обществом*, живущим в основном в виртуальном пространстве. При этом эксперты Давосского форума вообще не упомянули актуальные вопросы кибербезопасности в связи с переходом у новому IV экономическому укладу (цифровой экономике).

В современном Интернет-сообществе бытует иллюзорное мнение о защищённости Интернет-сети. Однако, такое мнение, «подпитываемое» специальными службами США, – это лишь «ширма» для деятельности специальных служб США при ведении ими широкомасштабного и всюду проникающего компьютерного шпионажа. Иллюзия защищённости Интернет-сети порождает иллюзию демократии и защиты прав человека с помощью такой сети. А на самом деле, такая иллюзия даёт благодатную почву для подрыва демократии и нарушений прав человека и информационной незащищённости пользователей Интернет-сети.

Таким образом, для решения проблем обеспечения ИБ цифровой экономики Российской Федерации необходимо:

1. Провести реорганизацию и обновление национальной ИОК за счёт интеграции КЗСУ на основе ИОК ИТС, входящих в состав ИТИЦЭ, в единую общероссийскую систему, способную решать задачи и предоставлять услуги по обеспечению ИБ;

2. Создать единую общероссийскую систему доверия на основе объединения КЗСУ (ИОК) ИТС, входящих в состав ИТИЦЭ, которая, в свою очередь, реализует важнейшие принципы обеспечения ИБ, включая надёжные процедуры идентификации и аутентификации, и обеспечение неотказуемости;

3. Разработать в рамках КЗСУ (систему доверия) на основе ИОК методы парирования угроз, связанных с нарушением прав и свобод граждан и бизнеса, которые обеспечат надёжность и гарантированность процедур предоставления электронных услуг и проведения коммерческих электронных транзакций (включая финансовые транзакции);

4. Разработать систему уникальной идентификации субъектов и объектов в киберпространстве на основе их параметров подлинности, которая обеспечивала бы, в том числе, реализацию принципа неотказуемости.

Таким образом, ***цель диссертационной работы*** можно кратко сформулировать следующим образом: «*Разработка системы управления криптографической защитой (системы доверия) на основе инфраструктуры открытых ключей с целью повышения уровня защищённости ИТС, образующих ИТИЦЭ РФ*».

Решаемые в диссертационной работе ***научно-технические задачи*** формулируются следующим образом:

1. Анализ взаимосвязи концепций доверия и безопасности в ИТС, а также выбор и обоснование выбора методов и средств (математического аппарата субъективной логики) для построения и анализа КЗСУ (системы доверия) на основе ИОК с целью повышения уровня защищённости ИТС.

2. Анализ организации и компонентов ИОК, а также решаемые ею задачи по обеспечению безопасности. Проведение сравнительного анализа основных архитектур и современных моделей организации ИОК, реализованных за рубежом, а также анализа проблем безопасности и рисков пользователей ИОК. Исследование уязвимостей, характерных для российских УЦ и снижающих доверие к ним.

3. Сравнительный анализ архитектур обеспечения параметрами подлинности пользователей и провайдеров электронных услуг, и определение необходимых условий, обеспечивающих доверие пользователей к провайдерам электронных услуг, и провайдеров к пользователям. Анализ параметров подлинности, содержащихся в $СЕРТ_{ОК}$ и атрибутных сертификатах ИОК, а также систем (структур) доверия на основе ИОК.

4. Синтез модели КЗСУ (системы доверия) на основе ИОК с использованием математического аппарата субъективной логики, и анализ полученной модели системы доверия с точки зрения решения задач обеспечения безопасности. Разработка методов защиты граждан и бизнеса при предоставлении электронных услуг и проведении коммерческих электронных процедур (включая финансовые транзакции) на основе синтезированной модели системы доверия, а также построение модели единой системы идентификации Интернет-пользователей и провайдеров электронных услуг, которая позволит снизить уровень киберпреступности в мировом информационном пространстве.

5. Внедрение полученных в пунктах 2…4 результатов в научно-исследовательскую и практическую деятельность организаций и компаний.

Выводы по Главе 1

Данная глава посвящена анализу проблем обеспечения безопасности цифровой экономики Российской Федерации. В частности, показано, что современное развитие российского общества направлено на *цифровизацию* (*цифровую трансформацию*) всех его сфер, включая экономику, науку, здравоохранение, образование, культуру и т.д. Определены источники концепции «*цифровая экономика*», которая получила всемирное распространение и стала предметом многочисленных научных, экономических и общественных дискуссий, которые проводятся на государственном и экспертном уровне. Начало международному обсуждению цифровой экономики было положено на Давосском форуме в 2015 году.

Анализ рекомендаций давосских экспертов показал их практическую направленность – повышение на качественно новый уровень *технологии манипуляции общественного сознания и управления обществом*, живущим в основном в виртуальном пространстве.

Вместе с тем, были выявлены очевидные недостатки и проблемы Программы «Цифровая экономика Российской Федерации». В частности, в Программе рассматриваются не различные финансово-инвестиционные «манёвры», а конкретные технологии, которые, по идее разработчиков Программы, должны изменить экономику России к лучшему. Было показано, что цели, содержащиеся в Программе, никак не конкретизируются, т.е. не определены. Авторы сами признают, что их Программа является следствием рекомендаций Давосского форума. Более того, Программа исходит не из того, чтобы что-то производить, уметь, создавать новое, а из приоритета предоставления услуг по сравнению с производством, и интересов «квалифицированного потребителя».

Далее представлен анализ угроз национальной безопасности Российской Федерации в связи с цифровой трансформацией и рассмотрены возможные пути их нейтрализации. Показано, что такими угрозами являются: кибертерроризм и кибершпионаж, ведущиеся против России США, их союзниками; угрозы со стороны внутренних преступных сообществ, террористических организаций, радикальных религиозных, нацистских и прочих экстремистских группировок, и антигосударственных сил; уход от налогообложения, незаконный вывоз капитала, отмывание преступно полученных доходов с использованием криптовалют (систем на основе БЧ-технологии); осуществление незаконной предпринимательской деятельности посредством использования Интернет-сети, включая электронную торговлю и финансовые услуги. Фактически, речь идёт о преступлениях в киберпространстве.

Также в данной главе рассмотрена информационно-телекоммуникационная инфраструктура цифровой экономики. ИТИЦЭ представляет собой объединение ИТС (вместе с СОИБ) различных организаций на основе первичной сети электросвязи (передачи данных). Очевидно, что обязательной подсистемой ИТИЦЭ должна стать ИТИБ, включающая СОИБ ИТС, и которая должна решать задачи предоставления перечисленных выше услуг по обеспечению ИБ, защиты первичной сети электросвязи и формирования национальной системы доверия в интересах цифровой экономики.

Далее рассмотрена проблема обеспечение доверия к ИТИЦЭ, включающей ИТИБ. Разработка и внедрение ИТИЦЭ должны предусматривать процедуры формирования доверия у граждан и бизнеса, которые будут её активными пользователями, а основа такого доверия – высокий уровень защищённости ИТС, образующих ИТИЦЭ. Для решения указанной проблемы желательно, чтобы разработчики ИТС (вместе с СОИБ) всегда раскрывали (при необ-

ходимости и под жёстким контролем) все относящиеся к безопасности доказательства, которые пользователи объективно должны знать, а пользователи должны стараться обосновывать своё доверие, главным образом, с помощью объективных доказательств. Все объективные (прямые и косвенные) доказательства сформируют у пользователя (бизнеса) субъективное убеждение, которое и будет его доверием к ИТС, образующим ИТИЦЭ.

Опыт зарубежных экономически развитых государств (например, США и Евросоюз) показывает, что современные ИТИБ представляют собой ИОК, на основе которых строятся различные модели систем доверия в киберпространстве между взаимодействующими субъектами. ИОК обеспечивает процедуры распределения ключей и на их основе образуют *системы доверия* со стороны пользователей ИОК. Таким образом, разработка и реализация модели объединённой КЗСУ (ИОК) и создание на её основе системы доверия в интересах цифровой экономики Российской Федерации становится *стратегической задачей*, решение которой носит безотлагательный характер.

В заключительной части данной главы рассмотрена проблема создания национальной системы уникальных ПП на основе уникальных идентификаторов. Эта задача – прямое следствие решения проблемы нейтрализации угроз безопасности цифровой экономики Российской Федерации. Показано, что в глобальном масштабе необходима международная система идентификации Интернет-пользователей (физических лиц и организаций), которая позволит резко снизить уровень киберпреступности на основе точной идентификации злоумышленников и при условии выполнения принципа «неотвратимости наказания».

Также в результате проведённого анализа сформулирована *цель диссертационной работы*, а также *научно-технические задачи*, которые должны быть решены в диссертационной работе.

Глава 2 АНАЛИЗ ВЗАИМОСВЯЗИ ДОВЕРИЯ И БЕЗОПАСНОСТИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Что такое *доверие*, почему оно необходимо и как мы используем его? Эти вопросы могут показаться слишком трудными для ответа, и поэтому многие стараются их вообще избежать. В большинстве научных исследованиях по проблемам обеспечения ИБ именно так и поступают. Полагая, что существует «абсолютное доверие» к некоторым частям ИТС, можно сосредоточиться на более конкретных проблемах, т.е. где «разместить доверие» и как его «распространить», чтобы получить наиболее оптимальные способы и протоколы обеспечения ИБ.

Доверие – важнейший фактор человеческого общения, но имеет ли доверие по-прежнему смысл, если ИТС взаимодействуют с другими удалёнными ИТС? Независимо от степени использования людьми ИТС, распределённая ИТС по-прежнему представляет собой социальное опосредованное взаимодействие между пользователями, и, соответственно, можно сделать вывод о том, что в такой ИТС доверие имеет определённую значимость и востребованность.

С точки зрения ИБ, людям доверяют потому, что они считаются честными, тогда как ИТС доверяют потому, что они считаются *безопасными*, и это создаёт основу для описания двух разных типов доверия. В распределённой ИТС, включающей, как пользователей, так и системные объекты, наиболее приоритетным будет взаимодействие с самыми безопасными или честными и, следовательно, заслуживающими доверия субъектами, поскольку это минимизирует возможность дискредитации рискованных транзакций. В этой связи необходимо решить три основные проблемы. Во-первых, важно правильно понимать концепцию доверия и то, как она проявляется в качестве человеческого фактора. Во-вторых, необходимо знать, как доверие может быть извлечено из реального мира в качестве параметра. И в заключении, следует проанализировать, как доверие может быть интегрировано в формальные модели, чтобы использовать его в качестве параметра среди других параметров с целью повышения уровня защищённости ИТС и повышения качества обслуживания.

Данная глава сфокусирована на первой и более фундаментальной проблеме точного понимания взаимосвязи доверия и безопасности в ИТС. Эта тема лежит в стыке двух научных направлений теории распределённых вычислений и ИБ. Далее представлен анализ доверия в условиях ограниченных знаний в области психологии и поведенческой науки.

2.1 Обзор основных научных работ по теме исследований

В [50,51] представлены две важные работы, которые предлагают формальную модель для получения новых доверительных взаимосвязей на основе существующих. В [50] представлена классификация доверия (*trust classification*). В соответствие с этой классификацией доверие к

определённому классу означает, что объекту можно доверять при решении конкретной задачи, например, при генерации ключей, хранении секретных данных или синхронизации часов (времени), без необходимости доверия при решении других задач. Таким образом, существует несколько доверенных взаимосвязей между одной и той же парой субъектов. В [51] определены правила и алгоритмы обеспечения открытыми ключами на основе доверенных взаимосвязей. Но ни в одной из этих работ нет попыток определить, что представляет из себя само доверие, как таковое.

В работе [52] представлено расширение [50], которое предполагает относительное доверие. В ней представлен метод извлечения параметров доверия из реального мира с целью их использования в формальных моделях, таких как [50] и [51]. Кроме того, авторы утверждают, что этот метод можно использовать при принятии решения о признании или непризнании субъекта в качестве приемлемого для выполнения важной процедуры. Фактически, этом метод – чисто статистический, и основан на предположении, что все доверенные субъекты ведут себя последовательно и, в конечном счёте, предсказуемо. Весьма сомнительно, что этот упрощённый подход приемлем для количественного анализа сложного поведения возможных злонамеренных субъектов. Скорее всего, этот метод наиболее приемлем для оценки достоверности, либо в большинстве случаев его можно использовать в качестве необходимого, но не достаточного теста для проверки надёжности.

В [53] проанализирована концепция доверия, связанного с доверенными системами и требованиями рынка. Автор утверждает, что доверие не есть свойство системы, как принято считать, а есть результат сделанной наблюдателем оценки человека, организации или наблюдаемого объекта. Это имеет очень важное значение для способа, с помощью которого проводится оценка безопасности, поскольку в таком случае акцент смещается от системы к взаимосвязи между наблюдателем и системой. Оценка безопасности в соответствии с [54] и [55] даёт определённый уровень гарантированности и, таким образом, является примером метода извлечения параметров доверия из реального мира, а наблюдение в [53] влечёт за собой трудности при определении надёжной и безусловной основы для оценки и определения гарантий безопасности.

В работе [56] проанализировано распространение доверия в системах контроля и управления доступом, в которых процедура может быть выполнена только определёнными действующими корректно людьми. Если протокол обеспечения ИБ спроектирован для его реализации только установленным составом участников, то он показывает, что дополнительное доверие между взаимодействующими участниками может создать нежелательные сочетания способных реализовать протокол участников, а это, в свою очередь, может ослабить схему безопасности. Представлен способ определения всех таких комбинаций участников как функция дополнитель-

ных доверительных взаимосвязей, которые могут появиться, а это, в свою очередь, может использоваться при проверке стойкости протокола к попыткам реализации нежелательных процедур.

В работе [57] используется вероятностный подход к доверию, связанному с протоколами безопасности. Такие протоколы разработаны на основе *BAN*-логики[10] [58], и они привязывают вероятности к утверждениям и правилам логики с целью определения минимального уровня доверия к предназначению протокола. Тем не менее, предположение о том, что доверие может быть смоделировано как вероятность, очень сильно упрощено и не учитывает его человеческие аспекты.

В работах [19…25,59…65] был совершён «прорыв» в области концепции «доверие» и её связи с концепцией «безопасность». В указанных работах были получены важнейшие аналитические результаты, которые были представлены в новом научном направлении «субъективная логика» (СЛ). Математический аппарат СЛ является современным аналитическим «инструментом», позволяющим получить количественные оценки уровня доверия в различных ИТС и, частности, структурах доверия на основе ИОК.

2.2 Определение доверия с точки зрения нарушителя

Определим некоторые понятия, которые будут использоваться далее. Характеристики *честный* (*honest*), *нечестный* (*dishonest*), *надёжный* (*straight*) и *ненадёжный* (*crooked*) могут использоваться только для описания человеческих качеств, а не систем. Он – честный, если он держит слово, и – нечестный, если нет. Он – надёжный, если он соблюдает правила, и – ненадёжный, если нет. И, следовательно, ненадёжному человеку вполне можно доверять, проиллюстрируем это на примере. Если не́кто говорит вам, что он собирается украсть вашу машину, и затем совершает кражу, то он – честный жулик, потому что он сдержал своё слово и одновременно с этим нарушил закон, и что самое интересное, его честность заслуживала доверия в данном конкретном случае [20].

Речь пойдёт о двух важных словосочетаниях, а именно честный/надёжный (*honest/straight*), что будет означать *благонадёжный* (*benevolent*), и нечестный/ненадёжный (*dishonest/crooked*), что будет означать *злонамеренный* (*malicious*). В дальнейшем будут рассматриваться только эти два словосочетания, так как вероятнее всего никто не будет взаимодействовать с добрыми/ненадёжными или недобрыми/надёжными субъектами.

[10] BAN – эта аббревиатура сформирована из первых букв авторов [58], **B**urrows M., **A**badi M. и **N**eedham R.

Доверие – позитивная концепция (понятие). Оно означает, что мы ожидаем что-нибудь позитивное от надёжного субъекта, или другими словами, мы ожидаем от него, что он будет обладать желаемым нами свойством или вести себя так, как мы этого хотим. В частности, в [66] было предложено множество определений термина «*доверия*», многие из которых зависят, либо от системы, в которой осуществляется интерактивное взаимодействие, либо от субъективной точки зрения наблюдателя. Общее определение, которое дано в [66], звучит следующим образом: ***Доверие*** *– это степень, с которой один субъект готов зависеть от чего-то или кого-то в конкретной ситуации, ощущая при этом относительную безопасность, даже если возможны и негативные последствия*.

Несмотря на то, что это достаточно общее определение, оно явно и неявно включает в себя основные составляющие доверия, а именно: *1)* зависимость от доверенной стороны, *2)* надёжность доверенной стороны и *3)* риск в случае, если доверенная сторона не функционирует так, как предполагалось. Смысл этого определения заключается в том, что требования к обеспечению доверия напрямую коррелируют с влиянием риска [23].

Понятия «быть безошибочным» («*fault free*») или «вести себя правильно» («*behave correctly*») были бы слишком общими, и они, по указанным ниже причинам, относится к понятию «*достоверности*» и более общему понятию «*надёжности*». Главное логическое обоснование ИБ заключается в том, что в определённой ситуации некоторые субъекты будут вести себя злонамеренно и пытаться атаковать или манипулировать ИТС. Поэтому доверие, затрагивающее безопасность ИТС, должно каким-то образом отражать *сопротивляемость* (*резистивность*) по отношению к злонамеренным угрозам.

Если бы в мире не было злонамеренного поведения, то доверие больше не было бы нужным понятием, так как всему можно было бы доверять, причём без исключения. С другой стороны, полное отсутствие доверия будет означать, что враждебность и предательство проникли повсюду и в каждого. Это означает, что актуальность (наличие) доверия зависит от фактора неопределённости, который указывает на то, что не́кто может быть доброжелательным или злонамеренным, либо просто от существования обоих типов поведения в обществе. В дальнейшем будем полагать, что это является истиной, и пусть она составляет основу анализа доверия, представленного ниже.

Доверительное взаимодействие требует, по крайней мере, участие двух сторон (взаимодействующих субъектов). Вначале сфокусируемся на доверенной стороне и, соответственно, на доверяющей стороне, и в каждом случае зададим вопрос, что требуется от субъекта, чтобы он стал стороной доверительного взаимодействия.

2.3 Доверенная сторона

Понимая, что людям можно доверять, и что можно доверять ИТС, очевидно, что состояние самой доверенной стороны может варьироваться в широких пределах. Различие между просто системой и клиентами, использующими посредников (интерфейсы между пользователем и системой), не очевидно, потому что их действия и заинтересованность очень часто глубоко интегрированы в процедуры ИТС. Тем не менее, на основе определения чисто технической системы, как системы, которая не подвержена влиянию со стороны человека во время своего функционирования, в дальнейшем будем различать класс «*мыслящих субъектов*» (субъектов системы), называемых пользователями/клиентами, и класс системных объектов, называемых «*логическими объектами*», а также определим сущность доверия к каждому классу.

2.3.1 Доверие к клиенту («мыслящему субъекту»)

Анализируя человека, мы будем ему доверять, если мы уверены в том, что он *доброжелателен*, и не будем доверять ему, если мы уверены в противоположном. Таким образом, пользователь должен быть, либо *доброжелательным*, либо *злонамеренным*. Никогда нельзя быть абсолютно уверенным в чьей-либо доброжелательности, и поэтому доверие не может быть более чем *вера* (*убеждённость*). Следовательно, можно надеяться, что существует конечное число причин (факторов), которые определяют, каким образом поведёт себя человек, либо доброжелательно, либо злонамеренно, но в любом случае невозможно получить всеобъемлющие знания о его естественном состоянии и всех других влияющих на его состояние факторов. Поэтому поведение пользователя невозможно предсказать, даже самим пользователем.

Исходя из практических целей, и каким бы ни был основной способ, мы будем называть способ информационного взаимодействия, реализуемый клиентом, т.е. выбор между доброжелательным и злонамеренным действием, *независимым волеизъявлением* (*free will*). Мы называем субъекты (клиентов), которые реализуют этот способ (независимое волеизъявление), *мыслящими*. Считается, что мышление характерно только человеческой деятельности, но было бы неверно исключать некоторых животных, обладающих *примитивным мышлением*. По этой причине, при дальнейшем использовании выражений, подобных «поведению человека», мы также затрагиваем на некоторые аспекты поведения животных. Граница между мыслящими и логическими объектами когда-нибудь неизбежно сотрётся, и, возможно, в далёком будущем придётся воспринимать машины как мыслящие. Тем не менее, в настоящее время мы будем рассматривать людей, группы людей и коллективы организации как мыслящие субъекты, но никогда как

одиночная чисто техническая система. Такой тип доверительного взаимодействия показан на рисунке 2.1 и означает первый тип доверия: *доверие к мыслящему субъекту представляет собой веру в то (убеждённость в том), что он будет вести себя без злого умысла*.

Рисунок 2.1 – Доверие к мыслящему субъекту

Не существует универсального правила или способа формального определения «*доверия к людям*». Поэтому во многих организациях имеют место злонамеренные, но доверенные сотрудники, что представляет собой чрезвычайно опасную угрозу, так как она не может быть парирована известными способами обеспечения ИБ.

2.3.2 Доверие к логическому объекту

Алгоритмы, протоколы, комплексы технических средств (КТС), КПО, ПАК или даже более сложные вычислительные комплексы, системы и сети вряд ли могут быть охарактеризованы как мыслящие или обладающие *независимым волеизъявлением* (или *стремлением*), но, тем не менее, мы хотели бы иметь возможность им доверять.

Самое простейшее определение логического объекта, затрагивающее доверие, будет звучать так, это объект, который не является мыслящим. Другими словами, логический объект не обладает человеческим характером и независимым (самостоятельным) желанием/стремлением. Логический объект обычно представляет собой чисто техническую систему, хотя можно рассмотреть вопрос о включении участия человека, исключив мыслительные аспекты человеческого поведения.

Так как у логического объекта нет независимого желания (волеизъявления), то он не будет доброжелательным или злонамеренным. И поэтому доверие заключается не в том, как он будет себя вести, а в том, что он будет парировать любую попытку вредоносного манипулирования со стороны внешнего нарушителя. Таким образом, речь идёт о третьей стороне, а именно о *внешней угрозе*. Этот тип доверительной взаимосвязи проиллюстрирован на рисунке 2.2.

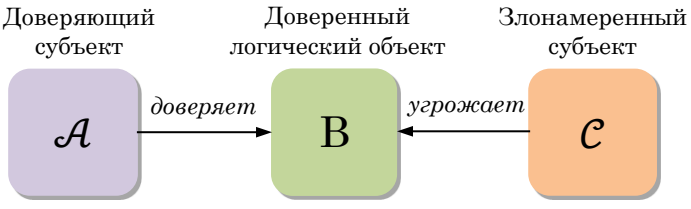

Рисунок 2.2 – Доверие к логическому объекту

Угроза представляет собой потенциальное нежелательное манипулирование или атаку. Даже если известно, что не́кто попытается атаковать, то априори невозможно узнать, кто именно проведёт атаку или на что она будет нацелена. С другой стороны, решение о том, будет ли внеш-

ний субъект пытаться провести вредоносную атаку или нет, должно быть следствием его независимого желания, и, следовательно, угрожающий субъект должен рассматриваться как мыслящий субъект в соответствии с приведённым выше определением. Из этого следует определение второго типа доверия.

Доверие к логическому объекту представляет собой веру в то (убеждённость/уверенность в том), что он будет противодействовать вредоносным манипуляциям мыслящего субъекта.

2.4 Доверяющая сторона

Доверие – это вера в то (или уверенность/убеждённость в том), что один субъект знает о существовании другого субъекта. Во-первых, обязательно должна быть причина такой веры, и во-вторых, вера отражает надежду на то, что субъект будет себя вести или функционировать соответствующим образом. *Причина доверия* может состоять из многих элементов, таких как прошлый опыт, знания о характере субъекта, рекомендация других субъектов или какое-либо поручительство. Это указывает на то, что причина доверия сложна и очень часто основана на неопределяемых объёмах исходной информации, и что она требует от мыслящего субъекта способности доверять. Поэтому мы утверждаем, что только мыслящие субъекты способны сформировать доверие, как это определено в предыдущем разделе, и такое доверие имеет смысл только для человека. Это скорее философское предположение, и оно может быть подтверждено несколькими наблюдениями.

На стороне доверенной стороны всегда есть мыслящий субъект, либо доверенный субъект (непосредственно сам клиент), либо злонамеренный субъект (нарушитель). Поэтому вполне естественно, что доверяющему субъекту нужны аналогичные аналитические способности, чтобы правильно оценить, можно ли доверять субъекту (противоположной стороне) или, другими словами, поведение мыслящего субъекта может быть оценено только другими мыслящими субъектами. Таким образом, доверяющий субъект обязательно должен быть мыслящим, а доверие становится взаимосвязью (взаимоотношением), в которой участвуют равнозначные мыслящие субъекты. Если мы признаём, что доверие в какой-то степени является результатом убеждённости или веры, а не просто оценкой вероятности, и что убеждённость и вера являются внутренними состояниями человека, то мы также приходим к выводу, что способность доверять и не доверять, по существу, представляет собой человеческую способность, которая не может быть присуща компьютерам. Прямым следствием этого является то, что приемлемое формирование доверительных взаимосвязей (взаимоотношений) никогда не может быть полностью автоматизировано. Рассмотрим несколько примеров, иллюстрирующих это.

Если ЭВМ поручено проверять людей на благонадёжность, используя для этого, например, опросные листы (анкеты с несколькими вопросами), то будет ли ЭВМ, затем, доверять тем, кто прошёл тест? Или, если ЭВМ сравнивает отпечатки пальцев и рисунки сетчатки глаз с аналогичными хранимыми значениями известных доверенных лиц, то будет ли в дальнейшем эта ЭВМ доверять лицам, отпечатки пальцев и рисунки сетчатки глаз которых совпали с некоторой записью в списке значений? Ответ в обоих случаях, как указывалось выше, будет «нет»!

В первом случае, любой человек смог бы ответить на вопросы, как заслуживающий доверия, путём простого изучения набора правильных ответов, так как они не являются конфиденциальными. Даже если бы использовались другие критерии, то он всё равно был бы способен обмануть систему на основе собственного анализа её функционирования. И в результате, разработчикам системы пришлось бы постоянно обновлять и модифицировать критерии, причём так, что её (систему), в конце концов, нельзя было бы больше называть автоматизированной.

Второй случай – хорошо известный способ аутентификации на основе биометрических параметров. На самом деле, речь идёт об уникальности отпечатков пальцев и рисунков сетчатки глаз, которые являются доверенными, а также целостности системы и списке предварительно сохранённых значений этих параметров. Система просто «переносит» это доверие с помощью формальной реализованной в системе модели на человека, обладающего соответствующими отпечатками пальцев и рисунками сетчатки глаз.

Логический объект может быть настроен так, что он будет доверять другим субъектам, но он всегда будет это делать от имени мыслящих субъектов. В таком случае, задача, каким образом можно ввести параметры доверия в систему, соответствует проблеме извлечение доверия из реального мира для ввода его формальную модель. Как только логические системы получили инструкции и описания начальных доверительных взаимосвязей, то можно представить себе системы, которые автоматически формируют новые доверительные взаимоотношения в соответствии с некоторой формальной моделью. Это соответствует проблеме встраивания доверия в формальные модели с целью оптимизации процесса обеспечения ИБ.

2.5 Доверительные взаимосвязи / взаимоотношения

Далее представлен обзор основных типов доверительных взаимосвязей с точки зрения участвующих субъектов (сторон). В соответствие с определениями, представленными в §2.2 и §2.3, доверие в ИТС предусматривает участие трёх субъектов (сторон): мыслящего доверяющего субъекта, логического доверенного субъекта и мыслящего внешнего угрожающего (злонамеренного) субъекта.

Комбинируя эти три стороны различными способами, проиллюстрируем различные доверительные взаимосвязи, два типа из которых уже были сформулированы в §2.2 и §2.3. Представленное ниже описание – всего лишь иллюстративное, и не претендующее быть всеобъемлющим.

В каждом случае, всегда существуют две мыслящие ипостаси: доверяющая ($\mathcal{A}$[11]) и угрожающая ($\mathcal{C}$). Логическая ипостась (B) является, либо самостоятельным объектом, либо частью мыслящего субъекта. Таким образом, представленные на рисунке 2.3 реальные субъекты изображены в форме закруглённых прямоугольников или квадратов, содержащих комбинации функциональных ролей $\mathcal{A}$, B и $\mathcal{C}$. Как отмечалось ранее, субъект считается мыслящим, если он выступает хотя бы в одной мыслящей ипостаси. Можно заметить, что ситуация, показанная на рисунке 2.3.*а*, совпадает с той, которая показана на рисунке 2.2, и что доверительная взаимосвязь, показанная на рисунке 2.3.*в*, в реальности является обобщением доверительного взаимодействия, которое показано на рисунке 2.1. Но с другой стороны, если представить, что субъект $\mathcal{C}$ – злоумышленник, то рисунок 2.3.*в* отражает модель взаимодействия клиента с мошенническим *Web*-сайтом, контролируемым злоумышленником. На рисунке 2.3.*б* показан доверяющий субъект, который может рассматриваться, либо как клиент, либо как организация, доверяющая сама себе с точки зрения её сопротивляемости или обеспечения защищённости от внешних угроз. Представленная на рисунке 2.3.*г* доверительная взаимосвязь может иметь отношение к разработке политики и обучению персонала, поскольку она иллюстрирует ограничения, налагаемые на пользователя, заставляя его, либо сотрудничать, либо стать нарушителем. На рисунке 2.3.*д* показан взгляд хакера на систему, которую он хочет атаковать. На нём также отображено то, как разработчики систем обязаны ставить себя на место нарушителя (атакующего), чтобы понять потенциальные угрозы. На рисунке 2.3.*е* показан *новый ранее не исследованный случай* (*модель компьютерного шпионажа*), когда злонамеренный субъект «скрытно» узурпировал логический объект, т.е. получил НСД к нему. При этом доверяющий субъект (доверяющий логическому объекту и управляющий им) «не подозревает», что злонамеренный субъект манипулирует логическим объектом.

2.6 Преступное намерение

Как это было определено в §2.2, *преступное намерение* (*злонамеренность*) – это сочетание нечестности и ненадёжности. То, что конкретно представляет собой злонамеренное поведение, никогда не может быть абсолютным, а может быть определено только на основе политики безопасности, морально-этических норм, контрактов/договоров и законодательства. Вследствие

[11] В дальнейшем, если это не будет оговорено отдельно, для обозначения мыслящих субъектов используются буквы с особым начертанием (например, $\mathcal{A}, \mathcal{B}, \mathcal{C}$), а для обозначения логических объектов – обычные буквы (например, A, B, C).

этого, сетевые сегменты безопасности (ССБ) с различными политиками могут иметь противоречивые взгляды на то, что представляет собой «злонамеренное поведение», а это указывает на наличие серьёзной проблемы создания прочной основы для проведения безопасных транзакций между такими ССБ. Вместо того, чтобы рассматривать вопросы обеспечения ИБ при взаимодействии ССБ, которые составляют проблему для формального моделирования, проанализируем более совершенную основу для определения вредоносного поведения в целом.

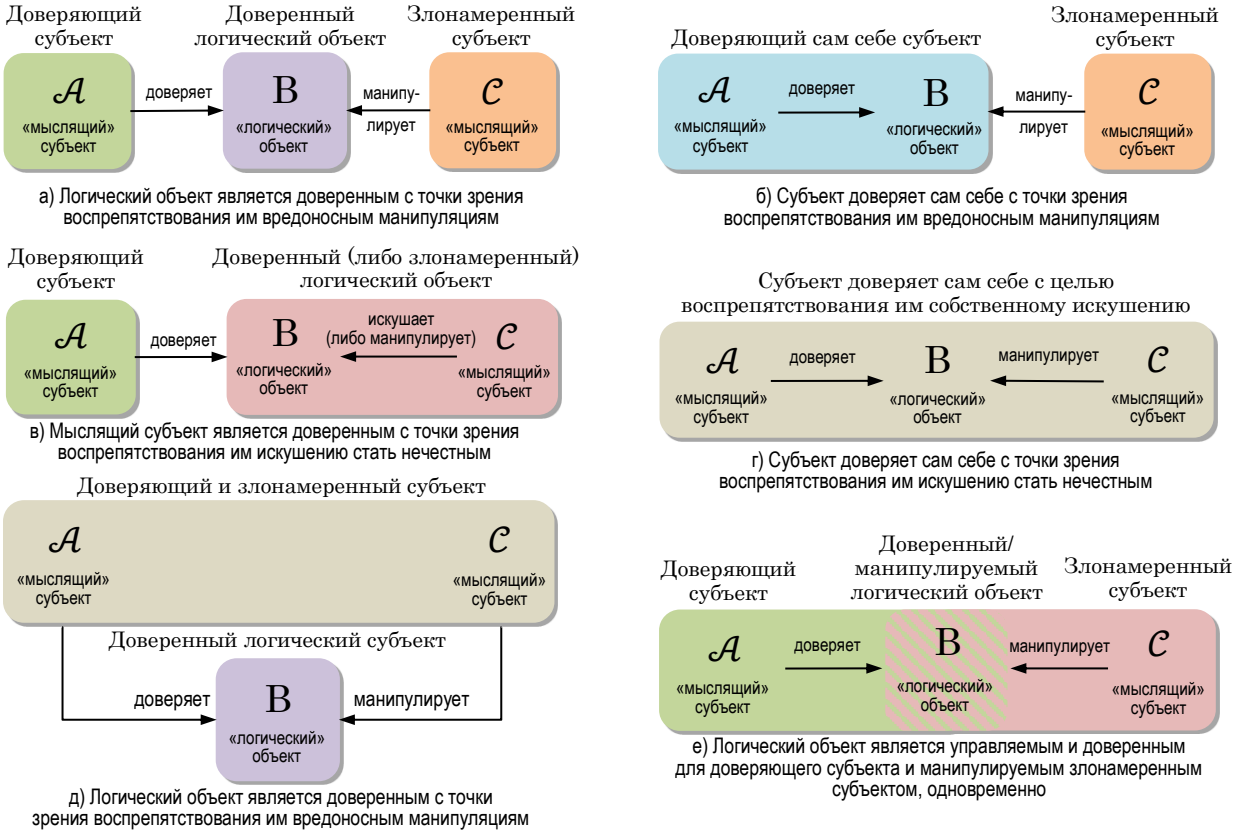

Рисунок 2.3 – Функциональные роли, основанные на доверительных взаимосвязях

Ни один человек не является абсолютно доброжелательным, и каждый из нас должен признать, что даже доброжелательные могут стать злоумышленниками. Как показано на рисунке 2.3.*г*, можно доверять себе, чтобы обладать необходимым умением правильно разбираться в самых разных ситуациях с целью предотвращения искушений стать злонамеренным, но это скорее напоминает психически больного человека. Кто мы такие, когда хотим быть нечестными, и кто мы такие, когда сопротивляемся этому? Способны ли мы отделить злонамеренное поведение от хорошего поведения? Если даже мы не можем согласиться с самими собой в том, каким должно быть хорошее поведение, можем ли мы все вместе согласиться с этим? Вполне возможно представить себе субъекты, принадлежащие к различным политическим или экономическим областям, в которых определённые публично признанные нормы хорошего поведения по отдельным

пунктам могут быть несовместимы. И что же нам тогда делать? Неужели злонамеренные субъекты непременно осознают, что они злоумышленники? Ответы на эти неудобные вопросы, как правило, основаны на чём-то более совершенном и общепринятом, что всегда позволяет отличить корректное поведение от злонамеренного. Одно из возможных решений этой фундаментальной проблемы можно найти в «Категорическом Императиве» И. Канта[12] (КИК), который гласит: «*Всегда поступайте только в соответствие с моральными принципами, которые в любое время могли бы стать всеобщим нравственным законом*».

Предположим, что есть человек с раздвоенной личностью, как было описано выше, и назовём эти личности г-н *Мыслящий* ($\mathcal{P}$) и г-н *Логичный* ($\mathcal{R}$). $\mathcal{P}$, как указывает его имя, полностью управляется своими мыслями (душевными переживаниями), а $\mathcal{R}$ использует логические аргументы, когда анализирует предлагаемые $\mathcal{P}$ действия (процедуры) на предмет их корректности в случае их выполнения. $\mathcal{R}$ действительно может применять различные критерии для своего рассуждения, но Канту совершенно не ясно, на что конкретно указывают логические аргументы. Он обнаружил, что, поскольку мы все обладаем логическими аргументами, то они могут нам подсказать что делать, и чтобы это было бы возможно для всех. Этот критерий, установленный КИК, а также аргумент, указывают нам на то, что следует отказаться от тех действий и поступков, которые не соответствуют этому критерию. Таким образом, мы не должны хотеть делать то, чего бы мы сами не могли пожелать, чтобы это сделали остальные.

В качестве примера того, как можно применять КИК, предположим, что «наш человек» с раздвоенной личностью задаётся вопросом, платить ли налоги? $\mathcal{P}$ предлагает не платить, а если $\mathcal{R}$ использует краткосрочную прибыль в качестве критерия для принятия своего решения, то платёж налогов может быть не осуществлён. Однако, такое действие не сможет пройти проверку на основе КИК. В случае неплатежа и полагая, что другие используют те же самые критерии, действия нашего кандидата могут привести к предсказуемому результату, т.е. к «разрушению» общества из-за недостаточного объёма налоговых платежей, поступающих в государственную казну, и мы можем предположить, что это совсем не то, что в итоге хотелось бы ему увидеть.

Применение КИК не всегда будет таким же простым, как в приведённом примере, но он все равно позволяет встроить весьма относительную концепцию вредоносного поведения в более полную и единую конструкцию. Однако, вряд ли КИК будет использоваться на практике, т.е. при описании злонамеренного поведения в документе, определяющим политику (стратегию) безопасности.

---

[12] *Центральное понятие этики* Иммануила Канта (немецкий философ, 1724-1804), безусловное общеобязательное формальное правило поведения всех людей независимо от их происхождения, положения, обстоятельств [67].

2.7 Многообразие и взаимозависимость доверия

Ранее рассматривалось только разнообразие целевых субъектов, т.е., что доверие варьировалось как функция доверенной стороны. Необходимо также понимать, что точно означает термин «доверенный» (или «быть доверенным»). В работе [53] указано, что доверие относится к области действия, а в работе [50] дана классификация доверия, которая с более формальной точки зрения отражает то же самое. В рамках этой концепции мы будем использовать термин «*цель доверия*» (*trust purpose*). В критериях оценки защищённости, например, [54,68], тот же самый аспект может быть отражён с помощью описания функциональности. В таком случае, цель доверия отражает точно то, ради чего доверяют целевому объекту. Но многообразие на этом не заканчивается, так как доверие также зависит от доверенного источника (или источника доверия, т.е. от того, кто доверяет), другими словами, не каждый доверяющий субъект будет иметь одинаковое доверие к одному и тому же доверенному объекту при одной и той же цели доверия. Мы будем называть это *многообразием источников* (*origin diversity*). Три типа такого многообразия представлены на рисунке 2.4.

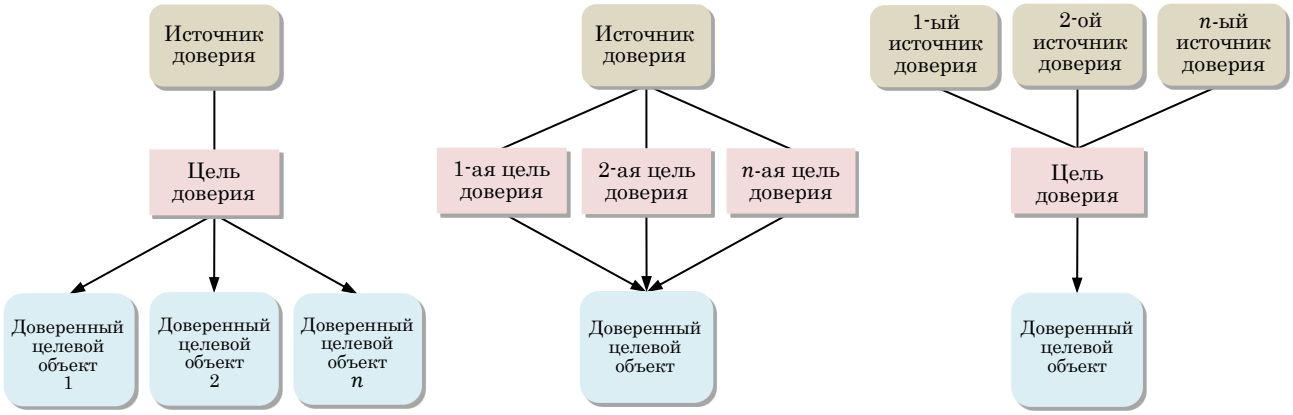

Рисунок 2.4 – Многообразие доверия

Не вдаваясь в детали, можно заметить, что отдельные доверительные взаимоотношения очень часто связаны и взаимозависимы. При *многообразии целевых объектов* это может означать, что если один конкретный целевой объект считается доверенным, то другие тоже.

Что касается *разнообразия целей доверия*, то целесообразно рассматривать людей и системы раздельно. Если сотруднику доверяют управление высокозащищённой системой, то можно ли ему доверять в том, что он не обманет нас со своими проездными документами? Оба действия зависят от его доброжелательности и будут относительно, но не абсолютно, зависимыми. В случае систем, которые, как правило, предоставляют различные и независимые услуги,

они по-прежнему могут быть зависимыми. Если, например, несколько услуг предоставляются с низким качеством, то очевидно, что вся система была плохо спроектирована и реализована, вследствие чего каждая служба обладает низким уровнем доверия.

Многообразие источников доверия, как правило, обусловлено различным уровнем знаний у доверяющих субъектов, что приводит к различным уровням их доверия к целевому объекту. Другой аспект, который следует учитывать в том случае, когда целевой объект является мыслящим, – это знание целевого объекта о доверяющем субъекте, т.е. что благонадёжность целевого объекта зависит от доверяющей стороны. Кроме того, даже в случае идентичных знаний у источников доверия, всё равно могут возникнуть различные уровни доверия.

Нет необходимости говорить о том, что сочетание трёх указанных типов многообразия может породить очень большое количество доверительных взаимоотношений, и, более того, могут существовать и другие, отличные от упомянутых здесь, типы многообразия. Такова реальность, которую нужно учитывать при попытке осмыслить и применить понятие «доверие» в качестве параметра при моделировании ИТС.

2.8 Доверие как знания о защищённости (безопасности)

Существует существенное различие между тем, на чём основано доверие в реальной жизни, и на чём оно должно основываться при решении задач обеспечения ИБ. Люди могут быть иррациональными, и поэтому могут доверять. Иррациональное доверие не основано на знаниях, а, например, на вероисповедании, и иногда может продолжать существовать «назло» знаниям. Такой тип доверия может быть весьма полезен в иных ситуациях, но может быть чрезвычайно опасным с точки зрения обеспечения ИБ. Поэтому единственным типом доверия в распределённых системах должно быть, насколько это возможно, доверие, основанное на знаниях.

«*Знания*» – это информация, которая может использоваться в определённых целях. В таком случае, интерес представляет информация, которая может быть использована при определении благонадёжности. Поэтому любая информация, которая «помогает решить» эту задачу, в последствие становится знанием в интересах указанной цели.

Пользователь ИТС никогда не может получить всеобъемлющие знания о используемой им системе или об угрозах, и более того он не способен точно оценить защищённость (безопасность) ИТС. Накапливая знания об ИТС в том объёме насколько это возможно, у пользователя формируется некоторое представление или мнение о защищённости (безопасности) системы, или, другими словами, формируется определённое доверие к системе. Таким образом, доверие отражает знания пользователя о защищённости (безопасности) ИТС. *Доверие и безопасность, выражаясь фигурально, представляют собой две стороны «одной медали»*. Безопасность отражает идеалистическую сторону, например, формальное моделирование, проектирование и

разработку, или, кратко, какой бы мы хотели видеть ИТС с теоретической точки зрения. С другой стороны, доверие отражает реальную сторону ИТС, так как никакая формальная модель не отражает всех знаний о системе, и что ошибки при разработке ИТС всегда будут иметь место, несмотря на строгое соблюдение всех процедур проектирования и внедрения.

Интересно отметить, что с точки зрения использования общего языка, можно доверять, и людям, и системам, но только системы могут быть безопасными. Если взглянуть на причину такого различия с точки зрения знаний, то вероятнее всего оно следует из того, что любые реальные знания о людях всегда будут несовершенными и весьма ограниченными, тогда как знания о системах могут достигать высокой степени корректности и полноты.

В распределённых ИТС может существовать *иерархия доверительных взаимосвязей*, в которых одни устанавливают более или менее необходимый для пользователя конкретной прикладной АИС (входящей в ИТС) уровень доверия, а другие используются только в качестве дополнительного условия (промежуточного доверия) при установлении требуемого (окончательного) уровня доверия. Примером такого дополнительного (промежуточного) доверия может быть доверие к криптографическим ключам или даже доверие к АИС, входящей в ИТС, так как ключ или такая АИС являются всего лишь средствами предоставления услуг пользователю. Примерами окончательного доверия может быть доверие к аутентификации документа или конфиденциальности доставки сообщения.

Явно установленное доверительное взаимодействие можно охарактеризовать как *прямое (непосредственное) доверие* (*direct trust*). Доверительные взаимосвязи также могут быть неявными, т.е. потенциальными, но пока ещё не существующими, когда между доверяющей и доверенной сторонами существует непрямой маршрут доверия. Использование термина «*установленное доверие*» («*derived trust*») указывает на формирование нового явного доверительного взаимодействия, либо на основе доверительных взаимосвязей, либо на основе знаний о системе. Как только новое доверительное взаимодействие установлено и сформировано окончательно, оно сразу становится прямым доверием. Более того, установление доверия означает только способ формирования нового доверия на основе уже существующего доверия. Это очень напоминает концепцию получения знаний, так как причина доверия существовала ещё до того, как оно было установлено, но доверие тогда ещё не было очевидным.

Рисунок 2.5 иллюстрирует то, как «добываются» знания или устанавливается доверие на различных уровнях, образующих иерархию доверия в структуре оценки безопасности ИТС (или прикладной АИС, входящей в ИТС). Каждый тип доверия обозначен символами от a до e.

В первую очередь, необходимо доверять самому методу оценки (оценивания), доверие к которому обозначено как a. Процесс оценивания формирует новое знание о системе, что показано с помощью непрерывной стрелки, направленной к базе знаний. Успешная оценка формирует

доверие к системе, которое обозначено символом b. Горизонтальная прерывистая стрелка «$b \dashrightarrow c$» указывает на то, что такое доверие было установлено, и не существовало до процедуры оценивания. Доверие к системе и знания о системе, а также способы обеспечения безопасности будут, например, устанавливать доверие к документу, подписанному с помощью ЭП, которое обозначено символом d. Знание о том, что, например, документ был подписан с помощью ЭП, становиться частью базы знаний, что показано с помощью непрерывной стрелки. Горизонтальная прерывистая стрелка «$d \dashrightarrow e$» указывает на то, что такое доверие было установлено, и сразу после этого оно становится прямым доверием (в форме доверия e).

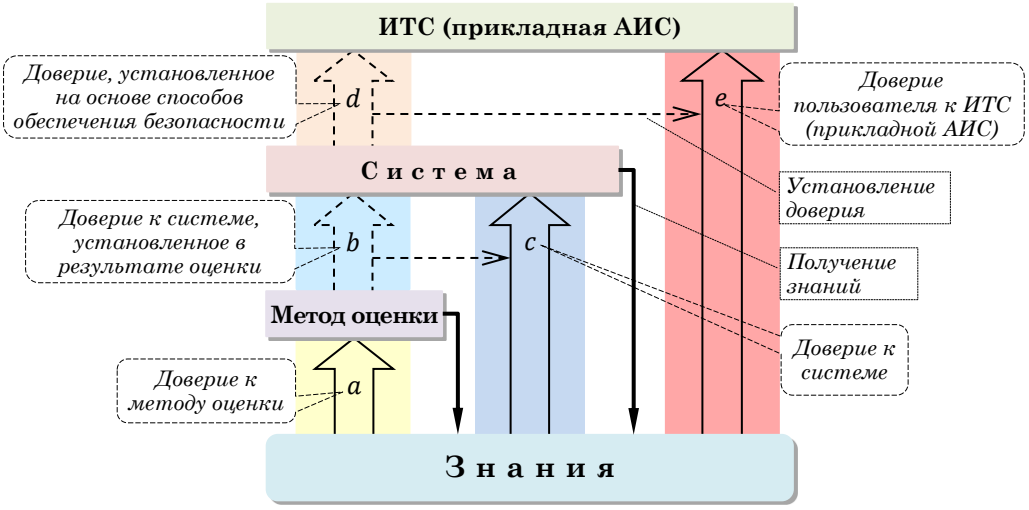

Рисунок 2.5 – Доверие на основе знаний

Следует заметить, что иерархия доверия (рисунок 2.5) рекурсивна в том смысле, что установленное доверие может использоваться для формирования следующего доверия, и что формальная проверка также может быть формально перепроверена. Основополагающее доверие e и, в определённой степени доверие c отражают не только безопасность, то есть потенциал отражения вредоносных атак, но также и другие аспекты функциональной надёжности, поскольку эти аспекты способствуют увеличению уровня окончательного доверия a.

Представленная на рисунке 2.5 модель, вследствие своего рекурсивного характера, является высокодинамичной. Любое изменение доверия a оказывает прямое воздействие на b и, следовательно, на d и e. Аналогично, любое изменение доверия c также оказывает влияние на d и e. Динамизм в модели усиливается за счёт того, что сама модель рекурсивна. Когда целью является стабильный процесс обеспечения безопасности, то и доверие должно быть стабильным. Очевидно, что для этого знания должны быть как можно более полными, так как это снижает вероятность быть обескураженным новыми знаниями, раскрывающими слабые места или нарушения в системе обеспечения безопасности.

2.9 Доверие как стратегическая игра

У мыслящих субъектов может быть стимул для злоупотребления доверием других. В качестве примера из сферы распределённых ИТС можно представить себе злонамеренного субъекта, который в течение определённого периода времени ведёт себя корректно с целью повышения уровня доверия к нему со стороны других субъектов, а затем внезапно проводит ложную кредитную транзакцию, предусматривающую привлечение большого объёма финансовых средств, и впоследствии исчезает из сети[13].

Этот пример показывает, что *доверием можно манипулировать*, а кто в конце концов станет победителем может зависеть от того, кто умнее. Не нужно много рассуждать, чтобы обосновать, что доверяющий и доверенный субъекты могут оказаться в бесконечном цикле с обратной связью. Причиной возникновения такого цикла являются знания равнозначных субъектов друг о друге в сочетании с их силой разума (интеллектом). Первый цикл «говорит»: субъект $\mathcal{A}$ доверяет субъекту $\mathcal{B}$, однако, когда $\mathcal{B}$ знает, что ему доверяют, он может манипулировать $\mathcal{A}$. Второй цикл «говорит»: $\mathcal{A}$ знает, что $\mathcal{B}$ планирует совершить злонамеренное действие, основываясь на доверии со стороны $\mathcal{A}$, которое, по мнению $\mathcal{A}$, имеет $\mathcal{B}$, и в конечном счёте $\mathcal{A}$ больше не доверяет $\mathcal{B}$. И затем снова, $\mathcal{B}$ знает, что ему не доверяют, и он решает сотрудничать с целью завоевания какого-либо доверия. Это рассуждение может продолжаться до бесконечности и принимает очертания *стратегической игры*. Взаимодействие внезапно становится рекурсивным и, с теоретической точки зрения, бесконечно сложным. Очевидно, что такой ход событий нежелателен, и поэтому цикличность должна быть нарушена.

Кажется, что единственный способ предотвращения цикличности заключается в ограничении знаний субъектов об их доверительных взаимосвязях. Это весьма парадоксально, и может показаться невозможным, потому что человек предпочитает взаимодействовать только с теми, кому больше всего доверяет, но тем самым он раскрывает своё доверие. Всё это, по-видимому, говорит о весьма пессимистических перспективах будущего развития распределённых систем, и, действительно, если бы субъекты были слишком эгоистичны и заботились только о своей прибыли и персональной выгоде, то следствием этого стало бы полное разрушение любой распределённой системы.

До сих пор не был всесторонне рассмотрен вопрос о том, что является побудительным мотивом для благонадёжного или злонамеренного поведения. Поскольку в большинстве функционирующих распределённых ИТС обеспечивается тот или иной уровень доверия, то считается, что большинство участников таких систем по своей природе благонадёжны, или что они видят

[13] Это классический пример способа проведения атак типа «маскарад», он весьма характерен для ИТС на основе технологии «блокчейн» (*blockchain*).

преимущества функционирования всей ИТС и, в конечном счёте, преимущества своего благонадёжного поведения. Таким образом, цикл, упомянутый выше, теряет свой порочный характер и звучит следующим образом: «*я доверяю вам, а вы доверяете мне, и мы оба довольны и счастливы, осознавая это*».

Похоже, что сотрудничество в стратегической игре основано на особом типе взаимодействия. Скорее всего, другой субъект также будет стремиться к сотрудничеству, потому что в таком случае он будет в выигрыше. Но если доверительные взаимосвязи основаны на стратегическом анализе, как этот, то распределённые ИТС становятся похожими на огромные стратегические игры, напоминающие поля сражений, а не стабильную среду для взаимодействия и предоставления услуг. Может возникнуть вопрос, а как обеспечить ИБ такого вида доверия в условиях, когда оно слишком нестабильно и непредсказуемо. Может возникнуть и ещё один вопрос, а можно ли такое доверие вообще называть доверием, исходя из определения, представленного в §2.2, поскольку в нём уже нет упоминания о благонадёжности. Тем не менее, если принять благонадёжность, как таковую, за стратегический фактор, то можно определить доверие и в таком смысле, потому что честное и надёжное поведение, которое было названо *благонадёжностью*, в конечном счёте можно рассматривать как эгоистичное или корыстное, а также как и самое выгодное или выигрышное на протяжении длительного времени. Это свидетельствует о том, что благонадёжность может быть «внедрена» с учётом чисто стратегических и эгоистических факторов, и что она не должна быть неотъемлемым метафизическим (неизменным) свойством доверенной стороны.

Как уже упоминалось, с целью обеспечения стабильного уровня защищённости следует также обеспечить стабильность доверительных взаимосвязей. Оценка чей-то надёжности, как совокупности стратегических факторов, должно быть сосредоточена на том, чтобы убедиться, является ли благонадёжное поведение доверенного субъекта его основополагающим и неизменным стратегическим принципом. В последствие этот простой критерий, несмотря на то, что его трудно оценить и формализовать, будет иметь решающее значение при определении надёжности мыслящего субъекта.

2.10 Сравнение защищённости (безопасности) и надёжности

Если исключить вредоносный субъект из модели, и сделав логические объекты целями данного анализа, то наиболее приемлемым термином будет «надёжность», а не защищённость (безопасность). Доверие к надёжной системе может придать иное значение этому понятию, которое отличается от используемого до сих пор, так как оно больше не будет связано с безопасностью. Надёжность может анализироваться с помощью статистических методов, в которых количество информации конечно. Она охватывает такие аспекты, как интенсивность отказов и время

восстановления. Оба понятия защищённость (безопасность) и надёжность вписываются в более общее понятие «*функциональная надёжность или благонадёжность*» [69].

При анализе надёжности ИТС все вредоносные угрозы должны полностью игнорироваться, даже если они реально имеют место. После выполнения этого требования субъекты предстают в совершенно ином свете. Системе можно доверять за то, что она не уязвима относительно злонамеренных манипуляций, несмотря на то, что она может быть полностью ненадёжной и всё разрушить сама. В дальнейшем надёжность системы охватывает её качество, которое обеспечили не злонамеренные разработчики, и которое указывает на отсутствие недостатков.

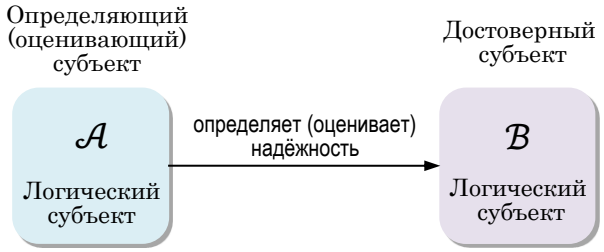

Рисунок 2.6 – Определение (оценка) надёжности

Оценка (определение) надёжности может быть смоделирована как двоичное отношение, представленное на рисунке 2.6. По определению, оцениваемый объект всегда является логическим. Тогда следует задать вопрос, а является ли оценивающий субъект логическим или мыслящим. Мы убеждены, что идеальная[14] оценка надёжности должна быть чисто логической процедурой, и, следовательно, такая оценка надёжности ИТС является, по своей сути, взаимодействием между логическими субъектами.

Выше было описано доверие к мыслящим и логическим субъектам, а также надёжность логических объектов. Для полноты общей картины необходимо исследовать, до какой степени можно оценить надёжность людей или мыслящих субъектов. Какие человеческие качества имеют значение для решения этой задачи, или что делает людей надёжными, кроме благонадёжности? Человеческие качества, такие как умение и опыт, кажутся важными, но, вероятно, есть и другие характеристики. И опять, с интуитивной точки зрения, необходимо, чтобы мыслящий субъект оценивал такие человеческие качества, что указывает на взаимодействие между мыслящими субъектами.

Таблица 2.1 – Сравнение безопасности и надёжности

Что представляет из себя субъект, которому доверяют в случае обеспечения:		
	Безопасности:	**Надёжности:**
Мыслящий ($\mathcal{P}$): Взаимосвязь:	Благонадёжный $\mathcal{P} \rightarrow \mathcal{P}$	Умеющий и опытный $\mathcal{P} \rightarrow \mathcal{P}$
Логический (R): Взаимосвязь:	Противодействие атакам $\mathcal{P} \rightarrow \mathrm{R} \leftarrow \mathcal{P}$	Непрерывное функционирование $\mathrm{R} \rightarrow \mathcal{R}$

Различие между защищённостью (безопасностью) и надёжностью резюмируется в таблице 2.1. В данном случае, термин доверие имеет более общий смысл, отличающийся от того,

[14] В смысле «теоретически точная».

который использовался ранее, и который также охватывает надёжность ИТС и умение (опыт) людей.

Кроме того, каждая строка в таблице указывает на тип взаимосвязи, т.е. существует ли она между мыслящими субъектами или логическими объектами. Например, запись $\mathcal{P} \rightarrow \mathrm{R} \rightarrow \mathcal{P}$ означает, что мыслящий субъект $\mathcal{P}$ доверяет логическому объекту R с точки зрения противодействия атакам, осуществляемым мыслящим субъектом $\mathcal{P}$.

2.11 Доверие и вероятность

Теперь ответим на два важных вопроса. Во-первых, можно ли рассматривать отсутствие доверия из-за неполных знаний или невежества как *энтропию информации*, а во-вторых, можно ли моделировать *доверие как вероятность*.

Идея рассматривать неопределённость доверия как *энтропию* – весьма реалистична. Действительно, если бы можно было определить объём знаний о субъекте (которые вообще возможно получить), и он был бы конечным, то стал бы известен «объём невежества», и задача сводилась бы просто к замене большего объёма невежества на возможный объём знаний. Это проиллюстрировано на рисунке 2.7.

К сожалению, *объём получаемых знаний невозможно определить*, так как знания могут быть даже бесконечны, и независимо от того, сколько знаний будет приобретаться, невежество всегда будет сохраняться. Проблема применения энтропии Шеннона к доверию заключается в том, что она основана на статистической вероятности относительно известного множества, например, алфавит или пространство сообщений. Если используется понятие «энтропия» с целью анализа доверия, то энтропия должна пониматься в более широком смысле, а не только в смысле статистического понятия по Шеннону.

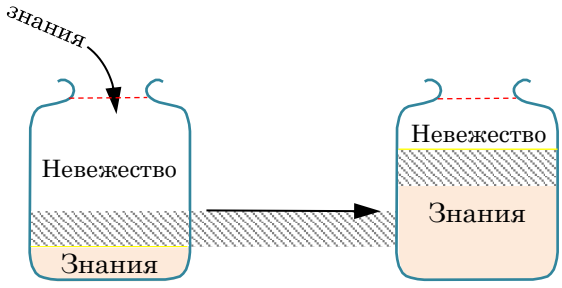

Рисунок 2.7 – Упрощённая модель знаний

Вопрос о том, можно ли моделировать доверие как вероятность, является весьма спорным. В [63] представлена точка зрения, которая заключается в том, что вероятность всегда является субъективным понятием, поскольку она определяет меру неопределённости, которую «ощущает» конкретный человек в конкретной ситуации. Объективная или физическая вероятность – это понятие бессмысленное. Такая же точка зрения отражена в [70]. В этом смысле, доверие вполне соответствует вероятности, поскольку оно является *субъективной верой/убеждённостью*.

Однако субъективная вероятность обладает объективными требованиями по соблюдению правил когерентности, таких как аксиомы и теоремы теории вероятностей, и по обоснованию

таких оценок с помощью объективных доказательств. В §2.8 было показано, что доверие основывается на знаниях, которые можно воспринимать как объективные доказательства, и в этом смысле доверие и вероятность по-прежнему совпадают. Но с другой стороны, виды доказательств, используемых для оценки доверия, могут оказаться непригодными для получения, с точки зрения теории, вероятностных оценок. Например, трудно понять, как гарантированный уровень оценки защищённости может быть преобразован во что-то, что соответствует оценке вероятности. Что касается аксиом и теорем теории вероятностей, то рассмотрим всего лишь один пример, доказывающий, что они не могут быть применены к оценке доверия напрямую.

Если покупатель $\mathcal{A}$ совершил хорошую покупку в некотором магазине, владелец которого $\mathcal{S}$, а затем $\mathcal{A}$ рекомендует владельца магазина покупателю $\mathcal{B}$, то в соответствие с теорией вероятности итоговое доверие $\mathcal{B}$ к владельцу магазина $\mathcal{S}$ будет равно:

$$t(\mathcal{B} \to \mathcal{S}) = t(\mathcal{B} \to \mathcal{A}) \cdot t(\mathcal{A} \to \mathcal{S}) ,$$

где $t(\mathcal{X} \to \mathcal{Y})$ отображает оценку того, насколько $\mathcal{X}$ доверяет $\mathcal{Y}$. Однако, возможен случай, когда владельцу магазина не нравится покупатель $\mathcal{B}$, и более того, владелец магазина может обманывать его. Тогда становится очевидным, что приведённая выше формула не корректна (не выполнима).

Проблема состоит в том, что теория вероятности не рассматривает субъекты, которые делают вероятностные оценки, касающиеся доверия, как уже упоминалось в §2.7. Говоря другими словами, *доверие не обязательно транзитивно, тогда как вероятность транзитивна*. Приведённый пример не говорит о том, что теория вероятности не может использоваться при моделировании доверия, он просто говорит о том, что её нельзя применять напрямую и в общем смысле. Её применение возможно, если ввести некоторые ограничения на такое применение. Например, использовать теорию вероятностей только в случае оценки доверия к логическим объектам, когда влияние взаимосвязей между доверяющим субъектом и угрожающей стороной можно проигнорировать.

2.12 Доверие в ИТС

Сама идея доверия в ИТС впервые была предложена в 1994 году [71]. В 1997 году [22,59] для исследования доверия в ИТС была разработана СЛ, как совокупность методов и средств (математический аппарат) для синтеза и анализа систем доверия. В частности, СЛ использовалась для анализа доверия в области обеспечения ИБ ИТС, например, когда анализировались структуры доверия на основе ИОК. Целостная теория СЛ и её приложения представлены в монографии [19], опубликованной в 2016 году.

2.12.1 Основы СЛ

Общая идея СЛ заключается в расширении вероятностной логики до формализованного подхода (формализма) за счёт прямого дополнения, т.е. включения ① неопределённости вероятностей и ② выразителя субъективной веры (убеждённости), как это показано на рисунке 2.8.

Рисунок 2.8 – Общая идея субъективной логики

Аргументы в СЛ называются *субъективными мнениями* (или просто *мнениями*). Мнение[15] может содержать *множество неопределённости* в смысле *неопределённости вероятностей*. В литературе по статистике и экономике тип неопределённости, выражаемый в СЛ множеством неопределённости, обычно называется *вероятностью 2-го порядка* или *неопределённостью 2-го порядка*. В этом смысле, классическая вероятность представляет собой *неопределённость 1-го порядка* [72,73]. Более точно, неопределённость 2-го порядка представляется в терминах *функции плотности вероятности* относительно вероятности 1-го порядка.

Интеграл от непрерывной функции плотности вероятности всегда равен 1, что следует из *аксиомы аддитивности* в теории вероятности. Помимо данного требования, функция плотности вероятности может иметь любую форму и тем самым отображать произвольные формы неопределённости 2-го порядка. Множество неопределённости в субъективных мнениях соответствует неопределённости 2-го порядка, которая может быть выражена в форме *функции плотности вероятности распределения Дирихле* (ДФПВ).

ДФПВ обычно отражают случайную выборку статистических событий, которая является основой для случайной интерпретации мнений как статистических оценок вероятности. Множество неопределённости в модели Дирихле отражает *бессмысленность* доказательства. Интерпретация множества неопределённости, как бессмысленности доказательства, отражает следующее свойство, «*чем меньше наблюдений, тем больше множество неопределённости*».

[15] Мнение – суждение, выражающее оценку чего-нибудь, отношение к чему-нибудь, взгляд на что-нибудь [74].

Кроме того, мнения могут отражать доказательства на основе структурированных знаний (т.е. доказательств не на основе статистических данных), которые являются основой для *эпистемологической*[16] *интерпретации мнений* как знаний на основе оценок вероятности. Множество неопределённости, с точки зрения эпистемологического мнения, отражают бессмысленность структурированных знаний о конкретном событии или его исходе, которое может произойти только один раз, и которое, следовательно, не может быть подвергнуто статистическому анализу. В СЛ рассматриваются два вида мнений: *статистическое*, которое основано на анализе многократно повторяющихся событий (их результатов/исходов), и *эпистемологическое,* которое основано на анализе неповторяющихся (одиночных) событий (их результатов/исходов).

Выразитель субъективного мнения тесно связан с доверием, потому что, когда разные субъекты имеют разные мнения об одном и том же утверждении (состоянии), аналитик должен определить или установить уровни доверия к различным субъектам/источникам, прежде чем их мнения могут быть интегрированы в модель логического анализа.

В классической Байесовской теории, очень часто, понятие *априорной вероятности* не отличается, в явном виде, от оценок вероятности. Такое не соответствие, от части, является следствием того, что априорная вероятность и вероятности обозначаются одним и тем же математическим символом p. В то же время СЛ позволяет однозначно разделять вероятности и априорные вероятности за счёт использования символа p или P для вероятностей и символа a – для априорных вероятностей.

Понятие *функции веры/убеждённости*, которое связано с понятием субъективных мнений, берёт своё начало в модели верхней и нижней вероятностей в [75]. Позднее в [76] была предложена модель для выражения функций веры/убеждённости. Основная идея, лежащая в основе функций доверия, состоит в том, чтобы отказаться от принципа аддитивности теории вероятностей, то есть сумма вероятностей для всех попарно непересекающихся состояний должна составлять в целом 1. Вместо этого функция веры/убеждённости даёт аналитикам возможность определять множество убеждений в элементах показательного множества[17] (*powerset*) в пространстве состояний. Основное преимущество такого подхода состоит в том, что невежество (незнание), т.е. отсутствие доказательств истинности тех или иных состояний, может быть точно выражено через отображение множества убеждений на всё пространство состояний. Кроме того, *неоднозначность* может быть выражена через отображение множества убеждений в подмножества показательного множества.

Модель субъективного мнения расширяет классическую модель функции веры/убеждённости в теории веры/убеждённости в том смысле, что мнения учитывают априорные вероятности,

[16] Эпистемология – раздел философии, изучающий сущность познания и критерии его истинности [74].
[17] Множество всех подмножеств множества $\mathcal{S}$, включая пустое множество $\{\emptyset\}$ и само множество $\mathcal{S}$.

а функции убеждённости игнорируют их. Таким образом, *важной характеристикой СЛ* является *включение априорных вероятностей*, что также позволяет определить биективное отображение между субъективными мнениями и ДФПВ.

Определение новых операторов для субъективных мнений заключается в добавлении ещё одного параметра «*неопределённость*» к известным вероятностным операторам. Многие востребованные операторы СЛ уже определены. Операторы СЛ реализуют адаптивный вычислительный аппарат, необходимый при моделировании большого числа различных ситуаций, в которых входные аргументы могут зависеть от неопределённости. Субъективные мнения эквивалентны ДФПВ и *функции плотности вероятности бета-распределения* (БФПВ), благодаря чему, СЛ также позволяет проводить логические доказательства, используя такие ФПВ.

При проведении исследований могут быть определены разные, но тождественные формальные отображения субъективных мнений, которые позволяют рассматривать неопределённые вероятности с разных точек зрения. После чего, можно описать модели на основе формального подхода и отображений, которые наиболее приемлемы для описания конкретной ситуации, связанной с обеспечением ИБ реальной ИТС. СЛ включает те же основные операторы, которые известны в двоичной логике и классической теории вероятностей, а также некоторые новые, характерные только для СЛ, операторы (Приложение 2).

Преимущество СЛ относительно классической теории вероятностей и двоичной логики состоит в том, что СЛ позволяет получить точное выражение неопределённости и неоднозначности, и поэтому реальные ситуации могут быть смоделированы и проанализированы более точно по сравнению с классическими вероятностными моделями. Частичная неосведомлённость эксперта и отсутствие доказательств могут быть учтены в ходе анализа и явно отображены в заключении (выводах). СЛ может использоваться при обеспечении принятия решений, так как она позволяет субъектам, принимающим решения, получить больше информации о достоверности (надёжности) оценок конкретных ситуаций и возможных будущих событий.

2.12.2 Элементы СЛ

Теперь кратко рассмотрим основные формализованные элементы в СЛ.

2.12.2.1 Область и гипербласть анализа

В СЛ используется понятие *области анализа* (ОА, *domain*), которая представляет собой пространство состояний, состоящее из множества величин (значений). Такие величины могут называться состояниями, событиями, выходными данными, гипотезами или предположениями.

ОА отображает возможные состояния в изменяемой ситуации. Величины ОА могут быть наблюдаемыми или скрытыми, как в классическом Байесовском моделировании. Предполагается, что различные величины ОА являются единственными и исчерпывающими, т.е. изменяемая ситуация может находиться только в одном состоянии в любой момент времени, а все возможные значения состояния включены в ОА.

ОА могут быть двоичными (включать только две величины) или m-ичными (включать m величин), где $m > 2$. Двоичная ОА обозначается как $\mathbb{X} = \{x, \bar{x}\}$, где $\bar{x}$ – отрицание x (рисунок 2.9,*а*). На рисунке 2.9,*б* показан пример четверичной ОА $\mathbb{Y} = \{y_1, y_2, y_3, y_4\}$.

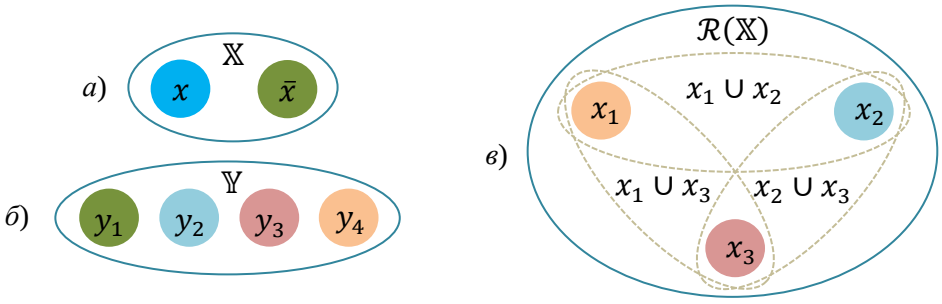

Рисунок 2.9 – Двоичная (*а*), четверичная (*б*) ОА и гиперобласть анализа (*в*)

Как правило, ОА конкретизируются для отображения реальных ситуаций с целью их практического анализа тем или иным способом. Величины в m-ичной ОА называются *подмножествами с одиночным элементом*, т.е. они предназначены для отображения одного возможного состояния или события. Существует возможность объединения таких подмножеств в *составные величины*.

Предположим, что имеет место троичная ОА $\mathbb{X} = \{x_1, x_2, x_3\}$. Гиперобласть анализа $\mathbb{X}$ (ГА) представляет собой уменьшенное показательное множество $\mathcal{R}(\mathbb{X})$, представленное на рисунке 2.9,*в*, на котором показаны одиночные величины x_1, x_2 и x_3, а также составные величины $(x_1 \cup x_2)$, $(x_1 \cup x_3)$ и $(x_2 \cup x_3)$.

Определение 2.1 (Гиперобласть анализа). Пусть $\mathbb{X}$ будет ОА, и пусть $\mathcal{P}(\mathbb{X})$ означает показательное множество $\mathbb{X}$. Показательное множество содержит все подмножества $\mathbb{X}$, включая пустое множество $\{\emptyset\}$ и саму ОА $\{\mathbb{X}\}$. *Гиперобласть анализа*, обозначаемая как $\mathcal{R}(\mathbb{X})$, представляет собой уменьшенное показательное множество $\mathbb{X}$, т.е. показательное множество, за исключением величины «пустое множество» $\{\emptyset\}$ и величины ОА $\{\mathbb{X}\}$.

ГА отображается как:

$$\mathcal{R}(\mathbb{X}) = \mathcal{P}(\mathbb{X}) \backslash \{\{\mathbb{X}\}, \{\emptyset\}\}\,. \qquad \square$$

2.12.2.2 Субъективные мнения

Субъективные мнения отражают веру/убеждённость в истинность предположений в условиях неопределённости, а также могут указывать на выразителя (субъекта) мнения, когда это необходимо. В СЛ мнения обозначаются как $\omega_X^{\mathcal{A}}$, где X указывает, например, на целевую переменную или предположение, относительно которого выражается мнение, и $\mathcal{A}$ указывает на субъект, который выражает своё мнение о X, т.е. выразитель веры/убеждённости. Верхний индекс можно опустить, если выразитель веры/убеждённости не определён (только подразумевается) или вовсе не имеет значения.

Правило, в соответствие с которым субъект $\mathcal{A}$ выражает своё субъективное мнение о целевой переменной X, означает, что существует прямая вера (взаимосвязь) $\mathcal{A}$ в X, формально обозначаемая как $[\mathcal{A}, X]$. Аналогично, правило, в соответствие с которым субъект $\mathcal{A}$ доверяет субъекту (объекту) $\mathcal{E}(E)$, означает, что существует прямое доверие (взаимосвязь) $\mathcal{A}$ к $\mathcal{E}(E)$, формально обозначаемая как $[\mathcal{A}, \mathcal{E}(E)]$. Такие взаимосвязи можно отобразить с помощью направленных рёбер в графе (векторов). В таблице 2.2 обобщены указанные обозначения.

«*Верить в…*» («*быть убеждённым в…*») и «доверять кому/чему» – очень близкие понятия. Основное различие состоит в том, что *доверие подразумевает зависимость и риск*, которые не нужно учитывать в случае веры/убеждённости. Таким образом, абстрагируясь от зависимости и риска в доверительных отношениях, субъективная логика использует одно и то же формальное отображение для мнений о вере/убеждённости и мнений о доверии.

Таблица 2.2 – Обозначение взаимосвязей на основе веры/убеждённости и доверия

Тип взаимосвязи	Формальное обозначение	Обозначение в виде ребра графа (вектора)	Интерпретация
Вера/убеждённость	$[\mathcal{A}, X]$	$\mathcal{A} \longrightarrow X$	Мнение субъекта $\mathcal{A}$ о переменной X
Доверие	$[\mathcal{A}, \mathcal{E}(E)]$	$\mathcal{A} \longrightarrow \mathcal{E}(E)$	Доверительное мнение субъекта $\mathcal{A}$ о субъекте (объекте) $\mathcal{E}(E)$

Само по себе мнение – это составная функция:

$$\omega_X^{\mathcal{A}} = (b_X,\ u_X, a_X)\ , \tag{2.1}$$

где b_X – распределение множества убеждений, u_X – множество неопределённостей и a_X – распределение априорной вероятности.

В СЛ определено три *основных класса мнений*. Если ОА $\mathbb{X}$ – двоичная, то переменная X и мнение – *двоичные*. Если ОА $\mathbb{X}$ – m-ичная ($m > 2$), и переменная – случайная переменная $X \in \mathbb{X}$, то мнение – m-*ичное*. Если ОА $\mathbb{X}$ – m-ичная ($m > 2$), и переменная – *гиперпеременная* $X \in \mathcal{R}(\mathbb{X})$, то мнение – h-*ичное*.

Кроме того, каждый основной класс мнений может быть разделён на четыре подкласса в соответствии с *уровнями достоверности* (обратно пропорционально множеству неопределённости). Если $u_X = 1$, то мнение – *бессмысленное* («пустое»). Если $0 < u_X < 1$, то мнение – условно *неопределённое*. И если $u_X = 0$, то мнение – *догматичное* (категоричное). Если единственная величина считается истиной (*TRUE*) за счёт присвоения этой величине множества убеждений со значением 1, то мнение – *абсолютное*. Таким образом, комбинируя три основных мнения, зависящих от ОА, и четыре подкласса, зависящих от достоверности, получаем *12 различных классов мнений*.

Теперь рассмотрим отображение мнений на примере двоичного мнения. Двоичная ОА включает только две величины, а переменная, как правило, имеет одну из двух величин. Пусть двоичная ОА определена как $\mathbb{X} = \{x, \bar{x}\}$, тогда двоичная случайная переменная $X \in \mathbb{X}$ может быть определена как $X = x$. *Мнения о двоичной переменной называются двоичными мнениями*, а для их математического отображения используется специальное обозначение.

Определение 2.2 (Двоичное мнение). Пусть $\mathbb{X} = \{x, \bar{x}\}$ будет двоичной ОА с двоичной случайной переменной $X \in \mathbb{X}$. Двоичное мнение об истинности/наличии величины x представляет собой упорядоченную четвёрку $\omega_x = (b_x, d_x, u_x, a_x)$, которая удовлетворяет требованию аддитивности:

$$b_x + d_x + u_x = 1\ , \tag{2.2}$$

где соответствующие параметры определены следующим образом:

b_x: *множество убеждений* в то, что x – «*истина*» (*TRUE*, т.е. $X = x$),

d_x: *множество неверия*, т.е. x – «*ложь*» (*FALSE*, т.е. $X = \bar{x}$),

u_x: *множество неопределённости* отображает бессмысленность доказательства,

a_x: *априорная вероятность* x без какого-либо доказательства. □

Ниже представлены различные типы двоичных мнений:

1) $b_x = 1$ или $d_x = 1$: *абсолютное мнение*, которое тождественно значениям «*истина*» (*TRUE*) или «*ложь*» (*FALSE*) в булевой алгебре;

2) $b_x = 0$ или $d_x = 0$: *мнение* $\ddot{\omega}_x$, которое максимизировано относительно неопределённости;

3) $u_x = 0$: *догматическое мнение* $\underline{\omega}_x$, и классическая вероятность;

4) $0 < u_x < 1$: *частично неопределённое мнение*;

5) $u_x = 1$: *бессмысленное мнение* $\widehat{\omega}_x$, т.е. нулевое множество убеждений.

Прогнозируемая вероятность двоичного мнения о величине x определяется следующим равенством:

$$\mathrm{P}(x) = b_x + a_x u_x \,, \tag{2.3}$$

Дисперсия двоичных мнений определяется как:

$$\mathrm{Var}(x) = \frac{\mathrm{P}(x)(1-\mathrm{P}(x))u_x}{W+u_x}\,, \tag{2.4}$$

где W – *неинформативный априорный весовой коэффициент*, который должен иметь значение $W = 2$ [19].

На рисунке 2.10 представлен так называемый «*треугольник двоичного мнения*» в трёхмерной системе координат. Горизонтальные оси обозначают «веру/убеждённость» (справа) и «*неверие*» (слева), а вертикальная ось обозначает «*неопределённость*». Нижняя сторона треугольника обозначает ось вероятности (от нуля (слева) до единицы). На рисунке 2.10 в качестве примера показана точка (двоичное мнение) $\omega_x = (0.40, 0.20, 0.40, 0.90)$. Прогнозируемая вероятность двоичного мнения в соответствие с (2.3) равна $\mathrm{P}(x) = 0.76$ (точка на оси вероятности). Априорная вероятность $a_x = 0.90$, также показана (точка) на оси вероятности.

Кроме того, на рисунке 2.10 показан *указатель* (*director*) – прерывистая прямая, соединяющая точку неопределённости ($u_x = 1$) с точкой априорной вероятности ($a_x = 0.90$), а также *линия проекции* (*projector*), которая параллельна указателю и соединяет точку ω_x с осью вероятности в точке $\mathrm{P}(x) = 0.76$ (прогнозируемая вероятность).

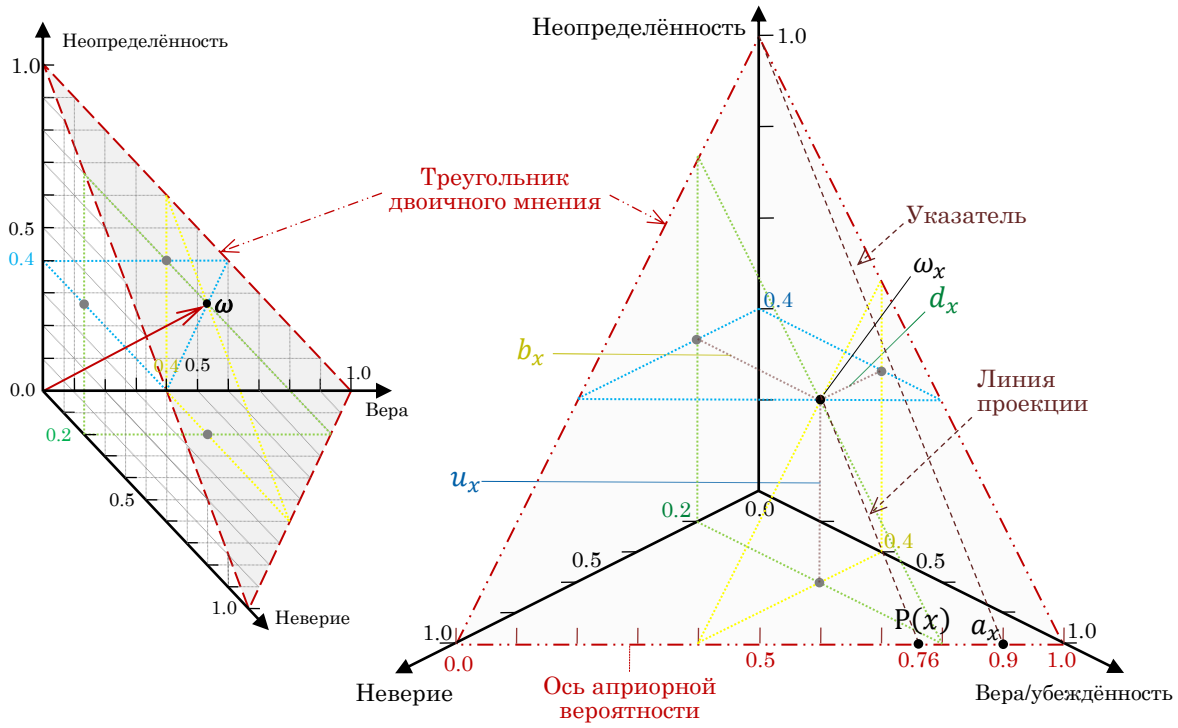

Рисунок 2.10 – Треугольник двоичного мнения в декартовой (трёхмерной) системе координат

Недостатком такого трёхмерного отображения является то, что с его помощью нельзя (или чрезвычайно сложно) отобразить m-ичное мнение. Поэтому в СЛ очень часто используется барицентрическая система координат[18] (БСК). На рисунке 2.11 показан «треугольник двоичного мнения» в БСК, который отображает рассмотренный ранее пример двоичного мнения $\omega_x = (0.40, 0.20, 0.40, 0.90)$. БСК с n вершинами представляет собой симплекс с n углами и размерностью $(n-1)$. Равносторонний треугольник – пример двухмерного симплекса. В «треугольнике двоичного мнения» оси веры/убеждённости, неверия и неопределённости – перпендикуляры, проведённые из соответствующих углов треугольника. Очевидно, что если $d_x = 1$ или $b_x = 1$ (и $u_x = 1$), то мнение эквивалентно значениям «*истина*» (*TRUE*) или «*ложь*» (*FALSE*) в булевой алгебре, а СЛ становится эквивалентной двоичной логике. Если точка мнения расположена на нижней стороне треугольника, т.е. $u_x = 0$, то СЛ становится эквивалентной вероятностной логике.

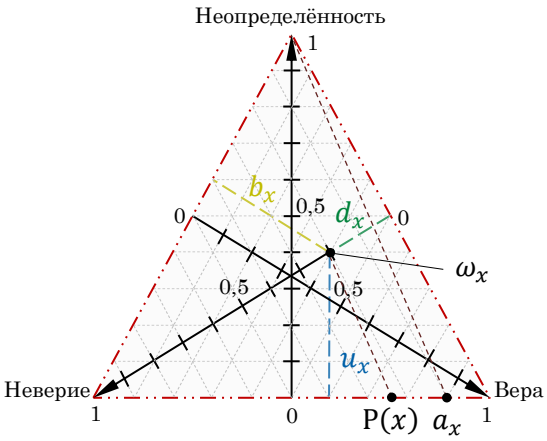

Рисунок 2.11 – Треугольник двоичного мнения в БСК [59]

Если точка мнения располагается в одном из трёх углов треугольника, т.е. когда $b = 1$, $d = 1$ или $u = 1$, то СЛ «превращается» *трёхзначную логику*, которая сопоставима, но не совпадает с *логикой Клини* (*Kleene logic* [78]), в которой используются предположения «*истина*», «*ложь*» или «*неизвестно*» (*UNKNOWN*). *Логика Клини не включает априорные вероятности*, и поэтому с её помощью нельзя получить прогнозируемую (апостериорную) вероятность из аргумента «*неизвестно*» (*UNKNOWN*).

Теперь в качестве примера рассмотрим троичную ОА $\mathbb{X} = \{x_1, x_2, x_3\}$ и соответствующую случайную переменную X, используя БСК.

Определение 2.3 (m-ичное мнение). Пусть $\mathbb{X}$ будет ОА, которая больше двоичной ОА, т.е. такой, что $m = |X| > 2$. Пусть X будет случайной переменной в $\mathbb{X}$. m-ичное мнение о случайной переменной X представляет собой упорядоченную тройку $\omega_X = (\boldsymbol{b}_X, u_X, \boldsymbol{a}_X)$, где

$\boldsymbol{b}_X$ – *распределение множества убеждений* по всей ОА $\mathbb{X}$;

u_X – *множество неопределённости*, которое отражает бессмысленность доказательства;

$\boldsymbol{a}_X$ – *распределение априорной вероятности* по всей ОА $\mathbb{X}$, а m-ичная аддитивность удовлетворяет равенству:

[18] В БСК положение точки определяется как центр массы, или *барицентр*, а сами массы расположены в вершинах этой системы [77].

$$u_X + \sum_{x \in \mathbb{X}} \boldsymbol{b}_X(x) = 1. \quad \square \tag{2.5}$$

На рисунке 2.12 представлен тетраэдр, в котором, в качестве примера, рассмотрено троичное мнение ω_X, которое имеет распределение множества убеждений $\boldsymbol{b}_x = \{0.20, 0.20, 0.20\}$, множество неопределённости $u_x = 0.40$ и распределение априорной вероятности $\boldsymbol{a}_x = \{0.750, 0.125, 0.125\}$.

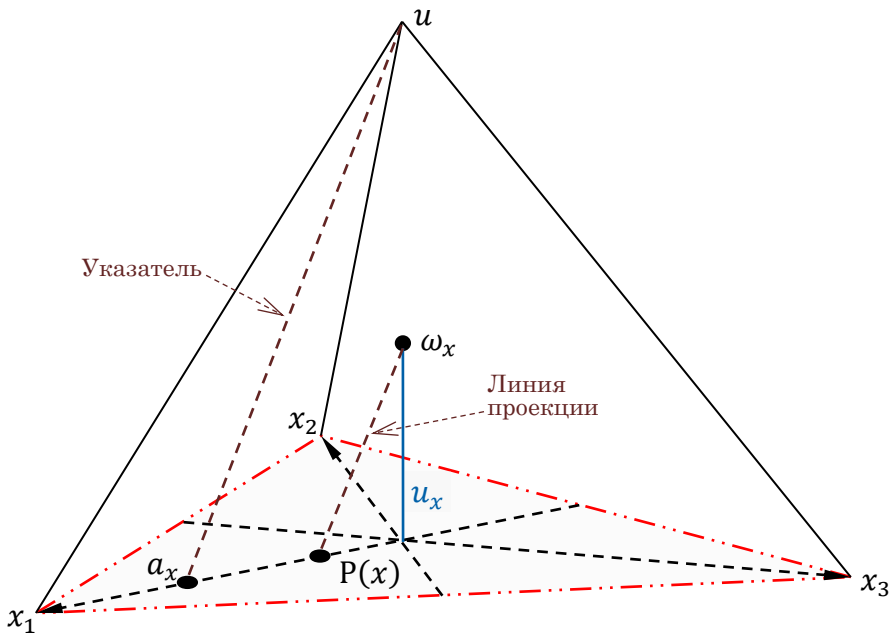

Рисунок 2.12 – Треугольник троичного мнения в БСК для ОА $\mathbb{X} = \{x_1, x_2, x_3\}$ [19]

Распределение прогнозируемой вероятности m-ичных мнений определяется следующим равенством:

$$\mathbf{P}_X(x) = \boldsymbol{b}_X(x) + \boldsymbol{a}_X(x)u_X \,, \forall x \in \mathbb{X} \,. \tag{2.6}$$

Тогда распределение прогнозируемой вероятности троичных мнений, в примере на рисунке 2.12, $\mathbf{P}_X = \{0.50, 0.25, 0.25\}$. Дисперсия m-ичных мнений определяется как:

$$\mathrm{Var}(x) = \frac{\mathbf{P}_X(x)(1-\mathbf{P}_X(x))u_x}{W+u_x}, \tag{2.7}$$

где $W = 2$.

2.12.3 Понятие доверия в ИТС

Доверие – это направленная взаимосвязь между двумя субъектами (взаимодействующими сторонами), которых можно назвать *доверяющей* и *доверенной сторонами*. Следует полагать, что доверяющая сторона, в той или иной форме, должна быть «*мыслящим субъектом*», а это означает, что она обладает способностью оценивать и принимать решения, основываясь на полученной информации и предыдущем опыте. Доверенная сторона может представлять *доверенный*

субъект, т.е. физическое лицо или организацию, а также *доверенный объект*, т.е. абстрактные понятия, например, информация, утверждение (предположение) или криптографический ключ [20].

У доверительной взаимосвязи есть своё предназначение, т.е. она имеет определённую целью или определённую область действия, например, «*быть подлинным*» в случае доверия субъекта к криптографическому ключу (доверенному объекту), или «*предоставлять надёжную информацию*» в случае доверия Интернет-пользователя к корректности статьи в *Web*-энциклопедии (*Wikipedia*). Понятие *цель доверия*, иногда используемое в литературе [79], совпадает с предназначением доверия. *Обоюдное доверие* означает, что оба взаимодействующих субъекта доверяют друг другу в одной и той же области действия, однако, это возможно только тогда, когда обе стороны являются мыслящими субъектами, способными провести некоторую формализованную процедуру оценки надёжности, риска и политики обеспечения ИБ.

Доверие влияет на взгляды и действия доверяющей стороны, а также может оказывать влияние на доверенную сторону и другие компоненты окружающей инфраструктуры, например, путём стимулирования обратного (обоюдного) доверия [80]. В некоторых научных трудах используются различные интерпретации термина «*доверие*», что весьма часто является источником противоречий [66]. Существуют две основные интерпретации, т.е. рассматривать доверие как:

i. осознанную надёжность чего-либо или кого-либо – *доверие к надёжности*;

ii. решение принять участие в действии (процессе, процедуре) в зависимости от чего-либо или кого-либо – *доверие при принятии решения*.

2.12.3.1 Доверие к надёжности

Как следует из названия, доверие к надёжности можно интерпретировать как оценку надёжности чего-либо или кого-либо, независимо от любого реального обязательства или решения. Такая интерпретация представлена в [81].

Определение 2.4 (Доверие к надёжности). Доверие к надёжности – это субъективная вера (убеждение), с которой субъект $\mathcal{A}$ ожидает, что другой субъект $\mathcal{B}$ выполнит определённое действие, от которого зависит «благополучие/благосостояние» субъекта $\mathcal{A}$. □

В этом определении, доверие интерпретируется как вера/убеждение доверяющей стороны относительно надёжности доверенной стороны с точки зрения потенциальной *зависимости* доверяющей стороны от доверенной стороны. Другими словами, доверяющая сторона может выразить надёжность к доверенной стороне в терминах субъективного мнения, которое, таким образом, становится мнением о доверии.

Предположим, что субъект $\mathcal{A}$ имеет определённое убеждение (веру) относительно произвольной переменной X, отражающее доверительную взаимосвязь, которую можно формально

обозначить как $[\mathcal{A}, X]$. Кроме того, субъект $\mathcal{A}$ имеет некоторый уровень доверия к субъекту $\mathcal{E}$, отражающее доверительную взаимосвязь, которую можно формально обозначить как $[\mathcal{A}, \mathcal{E}]$. Важнейшее семантическое различие между наличием убеждения (веры) относительно переменной X и уровнем доверия к субъекту $\mathcal{E}$ состоит в том, что доверительная взаимосвязь $[\mathcal{A}, \mathcal{E}]$ предполагает, что субъект (доверитель) $\mathcal{A}$ потенциально или реально зависит от субъекта $\mathcal{E}$, в то время как доверительная взаимосвязь $[\mathcal{A}, X]$ такой зависимости не предполагает.

Под *зависимостью* понимается, что благополучие/благосостояние субъект $\mathcal{A}$ зависит от функционирования субъекта $\mathcal{E}$, которое субъект $\mathcal{A}$ не может точно предсказать или контролировать. Эта неопределённость относительно достижения субъектом $\mathcal{A}$ своих целей означает, что в случае, если субъект $\mathcal{E}$ не будет функционировать так, как предполагает субъект $\mathcal{A}$, то субъект $\mathcal{A}$ понесёт некоторый ущерб. В общем случае, неопределённость субъекта относительно достижения им поставленных целей определяется как *риск* [82].

Таким образом, особенность зависимости доверия заключается в появлении риска, который является функцией возможного ущерба, возникающего в результате возможной неспособности субъекта $\mathcal{E}$ оправдать оказываемое ему доверие.

Мнения о доверии – это двоичные мнения, так как выражаются относительно двоичных переменных, которые естественно могут принимать только два значения. Общая область доверия может быть обозначена как $\mathbb{X} = \{t, \bar{t}\}$, так что двоичная случайная переменная доверия T может принимать за одно из этих двух значений, которые, как правило, могут означать:

$$\text{Область доверия } \mathbb{T}: \begin{cases} t : \text{"Действие выполнено как предполагалось".} \\ \bar{t} : \text{"Действие не выполнено как предполагалось".} \end{cases}$$

Предположим, что субъекту $\mathcal{E}$ доверяют с точки зрения выполнения им конкретного действия (процедуры). Таким образом, двоичное мнение о доверии к субъекту $\mathcal{E}$ можно обозначить как $\omega_{t_\mathcal{E}}$. Однако, с целью более точного отображения мнений о доверии, как правило, используется обозначение $\omega_\mathcal{E}$, сохраняющее тот же смысл, т.е. $\omega_\mathcal{E} \equiv \omega_{t_\mathcal{E}}$.

Субъективные мнения о доверии к надёжности корректно вписываются в логическую структуру СЛ, либо в качестве входных аргументов, либо в качестве выходных результатов. Применение СЛ в логическом анализе на основе мнений о доверии отражает так называемое *вычислительное доверие* (или *доверие в ИТС*), которое является высокоэффективным способом логического анализа доверия, учитывающим субъективные факторы.

При логическом анализе доверия в ИТС (АИС) используются некоторые операторы СЛ, среди которых *оператор понижения доверия* и *оператор слияния доверия* (будут рассмотрены ниже). В частности, оператор понижения используется при определении мнений относи-

тельно маршрутов с транзитивным доверием, оператор слияния используется при слиянии нескольких маршрутов доверия. В сочетании, эти операторы понижения и слияния доверия формируют основные «строительные блоки» для сетей с субъективным доверием.

2.12.3.2 Доверие при принятии решения

Доверие может быть интерпретировано и более сложно, чем просто доверие к надёжности, в соответствие с определением в [83]. Например, в [83] отмечено, что наличие высокого (с точки зрения надёжности) доверия к человеку не обязательно является достаточным при принятии решения в ситуации, когда лицо, принимающее решение, зависит от этого человека, т.е. «*… возможно, что величина ущерба как такового (в случае нештатной ситуации) слишком огромна, чтобы выбрать то или иное направление при принятии решения, и это не зависит, ни от вероятности возникновения нештатной ситуации (даже если она очень мала), ни от возможного выигрыша (даже если он очень большой). Другими словами, эта опасность может показаться субъекту неприемлемым риском*» [83].

Проиллюстрируем различие между доверием к надёжности и доверием при принятии решения на практическом примере, сначала рассмотрим ситуацию с пожарной тренировкой, когда участников просят покинуть помещение из окна третьего этажа дома с помощью верёвки. Предположим, что во время пожарной тренировки участники обнаружили, что верёвка сильно изношена. Естественно, в такой ситуации участники учения оценят вероятность того, что верёвка удержит их (не порвётся) во время спуска, как весьма низкую (рисунок 2.13).

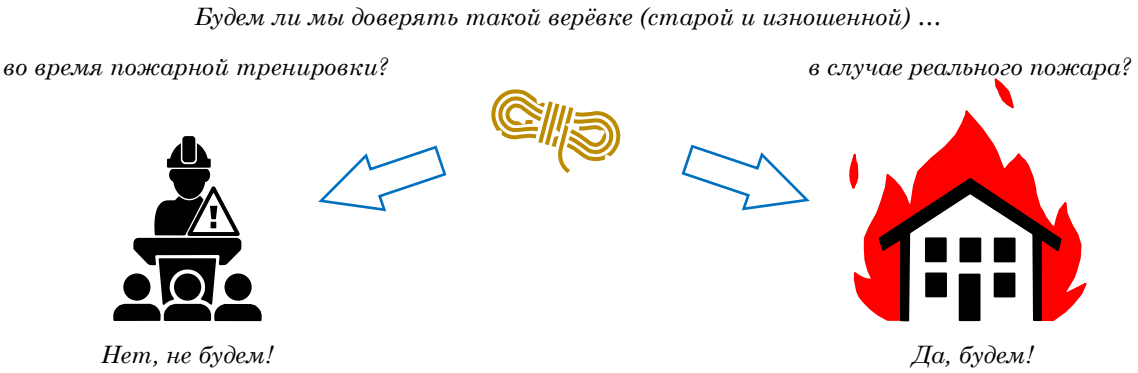

Рисунок 2.13 – Одно и тоже доверие к надёжности, но разное доверие при принятии решения

Пусть R обозначает верёвку, а также предположим, что существует двоичная область доверия $\mathbb{T}_R = \{t_R, \bar{t}_R\}$, в которой величины имеют следующие значения:

$$\text{Область доверия } \mathbb{T}_R: \begin{cases} t_R : \text{"Верёвка выдержит меня, пока я буду спускаться вниз".} \\ \bar{t}_R : \text{"Верёвка порвётся, если я попытаюсь спуститься вниз".} \end{cases}$$

Теперь, доверие субъекта $\mathcal{A}$ к надёжности верёвки можно представить как двоичное мнение $\omega_{t_R}^{\mathcal{A}}$, но используя упрощение, аналогичное тому, которое применялось в §2.12.2.1, получаем $\omega_R^{\mathcal{A}}$. Если субъект $\mathcal{A}$ думает, что верёвка порвётся, то он, чтобы продемонстрировать своё недоверие к верёвке, выразит его в форме двоичного мнения $\omega_R^{\mathcal{A}}$ с параметром неверия $d_R^{\mathcal{A}}$ близким к 1, и скорее всего откажется от её использования при спуске с третьего этажа дома.

Теперь представим, что тот же самый субъект попал в «ловушку», созданную реальным пожаром, охватившим весь дом, и что у него остался единственный выход, т.е. спуститься из окна третьего этажа горящего дома с помощью всё той же самой изношенной верёвки. Предположим, что мнение о доверии $\omega_R^{\mathcal{A}}$ осталось тем же самым как и раньше. Однако, в данной ситуации субъект $\mathcal{A}$ примет решение «доверять» верёвке при спуске из окна, даже если он думает, что верёвка может разорваться. Таким образом, доверие при принятии решения изменилось, хотя мнение о доверии к надёжности верёвки не изменилось. Этот парадокс легко объяснить тем фактом, что здесь речь идёт о двух разных типах доверия, а именно: *доверие к надёжности* и *доверие при принятии решения*.

Изменение доверия при принятии решения о является вполне разумным, поскольку вероятность получения травмы или смерти во время спуска сравнивается с вероятностью удушья и смерти от огня в результате пожара. Несмотря на то, что доверие к надёжности верёвки одинаково в обеих ситуациях, доверие при принятии решения изменяется в зависимости от сравниваемых различных значений полезности, связанных с разными способами действий в этих двух ситуациях. Решение в такой ситуации можно смоделировать с использованием формального подхода, т.е. в условиях неоднозначности и неопределённости [19]. Теперь дадим определение понятия «*доверие при принятии решения*».

Определение 2.5 (Доверие при принятии решения). *Доверие при принятии решения* – это готовность зависеть от чего-то или кого-то в конкретной ситуации с чувством относительной безопасности, даже если возможны негативные последствия [66]. □

В этом определении доверие, в первую очередь, трактуется как обязательство реально полагаться на конкретный объект и, в частности, включает в себя понятия зависимости от доверенной стороны, а также её *надёжности* и *риска*. Кроме того, данное определение косвенным образом охватывает ситуационные факторы, например, *полезность* (возможные результаты), *характеристики окружающей среды/инфраструктуры* (правоохранительные органы, контракты, способы обеспечения безопасности и т.д.) и *отношение к риску* (приемлемый риск, неприемлемый риск и т.д.).

И доверие к надёжности, и доверие при принятии решения отражают позитивную веру в то, от чего зависит благополучие доверяющей стороны. Доверие к надёжности наиболее точно

оценивается как вероятность или мнение о надёжности, тогда как доверие при принятии решения наиболее точно оценивается с точки зрения двоичного решения, основанного на множестве факторов [23]. Несмотря на то, что большинство известных моделей доверия и репутации предполагают доверие к надёжности, тем не менее, доверие при принятии решения также может быть смоделировано. ИТС, основанные на моделях доверия при принятии решений также должны рассматриваться как средства поддержки принятия решений.

2.12.3.3 Репутация и доверие

Понятие репутации тесно связано с понятием *благонадёжности*, но очевидно, что существует явное и важное различие.

Определение 2.6 (Репутация). Создавшееся общее мнение людей о достоинствах и недостатках кого-либо или о чего-либо, т.е. как люди думают о ком-то или о чём-то [74]. □

Это определение хорошо согласуется с точкой зрения исследователей социальных сетей [84,85], т.е. *репутация* – это количественная оценка, полученная из базовой социальной сети, которая видна (доступна) всем пользователям сети. Различие между доверием и репутацией можно проиллюстрировать с помощью следующих самых обычных и совершенно правдоподобных утверждений:

1) «*я доверяю вам, потому что у вас хорошая репутация*»;

2) «*я доверяю вам, несмотря на то, что у вас плохая репутация*».

Если предположить, что оба утверждения относятся к одной и той же области действия доверия, то утверждение *1)* означает, что взаимодействующая сторона осведомлена о репутации доверенной стороны и обосновывает своё доверие на этом, а утверждение *2)* – что взаимодействующая сторона обладает некоторой собственной информацией (данными) о доверенной стороне, например, на основании опыта непосредственного или личного (интимного) общения, и что эти факторы (данные) могут «перевесить» любую (даже негативную) репутацию доверенной стороны. Это наблюдение означает, что доверие, в конечном счёте, является личным и субъективным явлением, которое основано на различных факторах или доказательствах, и что некоторые из них имеют большую значимость, чем другие. Личный опыт обычно имеет гораздо большее значение, чем чьи-то доверительные рекомендации или репутация, но в отсутствие личного опыта доверие часто должно основываться на рекомендациях других людей.

Репутацию можно рассматривать как коллективную оценку благонадёжности (в смысле надёжности), основанную на рекомендациях или рейтингах членов сообщества. Субъективное доверие человека может быть получено путём объединения полученных рекомендаций и личного опыта.

Репутация может относиться к группе людей или к отдельному человеку. Репутация группы, например, может быть смоделирована как среднее значение индивидуальных репутаций всех её членов или как среднее значение репутационной оценки внешними сторонами группы в целом. Исследование в [86] показало, что человек, принадлежащий к конкретной группе, наследует априорную репутацию, основанную на репутации этой группы. Если группа заслуживает доверия, все её отдельные члены априори будут восприниматься как заслуживающие доверия, и наоборот.

Системы репутации – это автоматизированные системы определения репутационных рейтингов изделий или услуг. Системы репутации основаны на формировании обратных связей с пользователями и их оценках о собственной удовлетворённости изделиями или услугами, с которыми им приходилось сталкиваться (пользоваться), а также использовании рейтингов и обратных связей для формирования репутационных рейтингов. В целом, системы репутации широко используются в электронной коммерции, интерактивных социальных сетях и ГИТС.

Мнения о доказательствах, когда число наблюдений известно, хорошо подходят в качестве основы при вычислениях в системах репутации. Обратные связи могут быть представлены в виде наблюдений и могут быть объединены с помощью *оператора суммарного слияния*.

Определение 2.7 (Оператор суммарного слияния)[19]. Пусть $\omega^{\mathcal{A}}$ и $\omega^{\mathcal{B}}$ будут соответствующими мнениями субъектов $\mathcal{A}$ и $\mathcal{B}$ относительно одной и той же (гипер-) переменной X в ОА $\mathbb{X}$. Пусть мнение $\omega_X^{(\mathcal{A}\diamond\mathcal{B})}$ будет таким, что

Случай I: Для $u_X^{\mathcal{A}} \neq 0 \vee u_X^{\mathcal{B}} \neq 0$:

$$\begin{cases} \boldsymbol{b}_X^{(\mathcal{A}\diamond\mathcal{B})}(x) = \frac{\boldsymbol{b}_X^{\mathcal{A}}(x)u_X^{\mathcal{B}} + \boldsymbol{b}_X^{\mathcal{B}}(x)u_X^{\mathcal{A}}}{u_X^{\mathcal{A}} + u_X^{\mathcal{B}} - u_X^{\mathcal{A}}u_X^{\mathcal{B}}}\,, \\ u_X^{(\mathcal{A}\diamond\mathcal{B})} = \frac{u_X^{\mathcal{A}}u_X^{\mathcal{B}}}{u_X^{\mathcal{A}} + u_X^{\mathcal{B}} - u_X^{\mathcal{A}}u_X^{\mathcal{B}}}\,, \\ \boldsymbol{a}_X^{(\mathcal{A}\diamond\mathcal{B})}(x) = \frac{\boldsymbol{a}_X^{\mathcal{A}}(x)u_X^{\mathcal{B}} + \boldsymbol{a}_X^{\mathcal{B}}(x)u_X^{\mathcal{A}} - \left(\boldsymbol{a}_X^{\mathcal{A}}(x) + \boldsymbol{a}_X^{\mathcal{B}}(x)\right)u_X^{\mathcal{A}}u_X^{\mathcal{B}}}{u_X^{\mathcal{A}} + u_X^{\mathcal{B}} - 2u_X^{\mathcal{A}}u_X^{\mathcal{B}}} & \text{если } u_X^{\mathcal{A}} \neq 1 \vee u_X^{\mathcal{B}} \neq 1\,, \\ \boldsymbol{a}_X^{(\mathcal{A}\diamond\mathcal{B})}(x) = \frac{\boldsymbol{a}_X^{\mathcal{A}}(x) + \boldsymbol{a}_X^{\mathcal{B}}(x)}{2} & \text{если } u_X^{\mathcal{A}} = u_X^{\mathcal{B}} = 1\,, \end{cases} \tag{2.8}$$

Случай II: Для $u_X^{\mathcal{A}} = u_X^{\mathcal{B}} = 0$:

$$\begin{cases} \boldsymbol{b}_X^{(\mathcal{A}\diamond\mathcal{B})}(x) = \gamma_X^{\mathcal{A}}\boldsymbol{b}_X^{\mathcal{A}}(x) + \gamma_X^{\mathcal{B}}\boldsymbol{b}_X^{\mathcal{B}}(x)\,, \\ u_X^{(\mathcal{A}\diamond\mathcal{B})} = 0\,, \\ \boldsymbol{a}_X^{(\mathcal{A}\diamond\mathcal{B})}(x) = \gamma_X^{\mathcal{A}}\boldsymbol{a}_X^{\mathcal{A}}(x) + \gamma_X^{\mathcal{B}}\boldsymbol{a}_X^{\mathcal{B}}(x)\,, \end{cases} \text{где} \begin{cases} \gamma_X^{\mathcal{A}} = \lim\limits_{\substack{u_X^{\mathcal{A}}\to 0 \\ u_X^{\mathcal{B}}\to 0}} \frac{u_X^{\mathcal{B}}}{u_X^{\mathcal{A}} + u_X^{\mathcal{B}}} \\ \gamma_X^{\mathcal{B}} = \lim\limits_{\substack{u_X^{\mathcal{A}}\to 0 \\ u_X^{\mathcal{B}}\to 0}} \frac{u_X^{\mathcal{A}}}{u_X^{\mathcal{A}} + u_X^{\mathcal{B}}} \end{cases} \tag{2.9}$$

[19] Оператор слияния обозначается символом «◇». Причина выбора такого символа поясняется в §2.12.5.

Тогда $\omega_X^{(\mathcal{A}\diamond\mathcal{B})}$ называется статистическим мнением на основе суммарного слияния мнений[20] $\omega_X^{\mathcal{A}}$ и $\omega_X^{\mathcal{B}}$, которое отображает объединение мнений субъектов $\mathcal{A}$ и $\mathcal{B}$. Для обозначения этого оператора используется символ $\bigoplus$, тогда статистическая убеждённость на основе суммарного слияния может быть выражена как $\omega_X^{(\mathcal{A}\diamond\mathcal{B})} = \omega_X^{\mathcal{A}} \bigoplus \omega_X^{\mathcal{B}}$. □

2.12.4 Транзитивность доверия

В дальнейшем будем исходить из того, что формальный подход к доверию в ИТС подразумевает доверие, которое интерпретируется как *доверие к надёжности* (**Опред.2.4**). На основе предположения, что доверие является формой веры/убеждённости, а степень доверия может быть выражена как мнение о доверии.

2.12.4.1 Пример мотивации транзитивного доверия

Нам часто приходится делать выбор и принимать решения, основываясь на доверии. Рассмотрим абстрактный пример мотивации. Предположим, что у Маши возникли проблемы с зубами, которые она хочет вылечить, обратившись за помощью к стоматологу (в стоматологический центр). Также предположим, что Маша недавно переехала в город и, следовательно, не знает стоматологических центров в этом городе. Одним из её хороших и надёжных коллег по работе является Миша, которого она знала давно ещё до переезда в этот город, и который живёт в городе много лет. Когда у Маши возникли проблемы с зубами, она обратилась к Мише с просьбой подсказать ей, где лучше вылечить зубы (в каком стоматологическом центре). Маша интуитивно доверяет Мише так как он «сторожил» в этом городе. Миша сказал Маше, что он обычно лечит зубы в стоматологическом центре, в котором работает стоматолог по имени Тима. Миша, основываясь на своём непосредственном опыте (лечении зубов), считает, что Тима очень опытный стоматолог. Другими словами, Миша напрямую доверяет Тиме. Миша советует Маше вылечить зубы в стоматологическом центре, в которой работает Тима. Основываясь на своём доверии к Мише, а также на советах Миши, Маша формирует своё доверие к Тиме. Вновь сформированное доверие Маши к Тиме носит косвенный характер, поскольку оно не основано на непосредственном опыте общения между ними. Тем не менее, именно такое реальное доверие помогает Маше принять решение о стоматологическом центре, в котором она будет лечить зубы.

Этот пример демонстрирует транзитивность доверия, в том смысле, что Маша доверяет Мише, который доверяет Тиме, и поэтому Маша также доверяет Тиме. Это предполагает, что Миша действительно сказал Маше, что он доверяет Тиме, и что, с точки зрения Маши, является

[20] Эпистемологическое мнение вычисляется аналогично, но к этому вычислению добавляется операция максимизации неопределённости [19].

услышанным мнением или рекомендацией. Это проиллюстрировано на рисунке 2.14, на котором указаны порядковые номера, определяющие последовательность формирования доверенных взаимосвязей и рекомендаций.

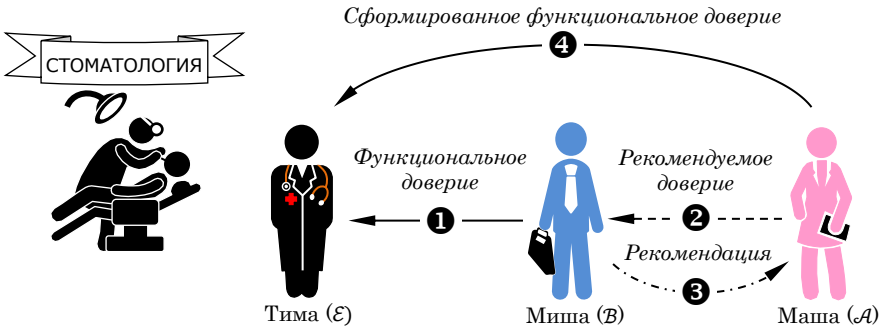

Рисунок 2.14 – Принцип транзитивного доверия

Доверие не всегда бывает транзитивным [87]. Предположим, например, что Маша доверила бы Мише заботиться о своём ребёнке, а Миша доверил бы Тиме вылечить свои зубы, и это вовсе не означает, что Маша доверила бы Тиме заботиться о своём ребёнке. Однако, когда определённые семантические требования будут удовлетворены [88], доверие может быть транзитивным, а система доверия может использоваться для формирования доверия. Например, каждое ребро доверия в транзитивной последовательности (цепи) доверия должно иметь одну и ту же область доверия. При попытке объединить доверие к няням и стоматологам транзитивность доверия нарушается, потому что области доверия не перекрываются.

Очевидно, что рассмотренный пример указывает на некоторую упорядоченность двоичного доверия между субъектами в последовательности транзитивного доверия. В реальных ситуациях доверие к надёжности, как правило, не только двоичное, поэтому многие исследователи предлагают измерять доверие с использованием нескольких дискретных уровней (например, вербальных утверждений), вероятностей или других непрерывных параметров. В случае использования вычислений таких показателей доверия, интуиция подсказывает, что доверие должно быть ослаблено или менее надёжным на основе транзитивности. Возвращаясь к приведённому ранее примеру, это означает, что доверие Маши к стоматологу Тиме через рекомендации Миши не может быть более полным или надёжным, чем доверие Миши к Тиме. А то, как полнота и надёжность доверия должны быть формально представлены, зависит от используемой (конкретной) формальной модели.

В некоторых ситуациях можно утверждать, что негативное доверие к рекомендующему субъекту может иметь, как это не парадоксально, положительный эффект, т.е. формировать более надёжное доверие к целевому субъекту. Такая модель основана на принципе, что *враг моего врага – мой друг*. Возвращаясь к предыдущему примеру, предположим, что Маша не доверяет

Мише, а Миша говорит ей, что он не доверяет Тиме. В таком случае, вполне вероятно, что Маша сформирует положительное доверие к Тиме, так как она могла рассуждать следующим образом: «*В действительности Миша думает, что Тима хороший стоматолог, но не хочет, чтобы я об этом знала. Миша пытается обмануть меня, и поэтому он даёт мне отрицательную рекомендацию относительно Тимы*».

Вопрос о том, как следует интерпретировать транзитивность недоверия, может быстро превратиться в очень сложную проблему, поскольку он может включать в себя несколько уровней обмана. Модели, основанные на таком типе логического анализа, не нашли достойного внимания в научных работах по системам доверия и репутации, и поэтому можно смело утверждать, что исследование таких моделей относится к дисциплинам интеллектуального анализа, а не к обеспечению интерактивного доверия. Однако, рассматриваемые в обеих дисциплинах фундаментальные вопросы и проблемы одинаковы.

Безопасный и консервативный подход к транзитивности доверия основан на предположении, что недоверие к узлу ИТС, который составляет часть транзитивного пути доверия, должно способствовать снижению доверия, с точки зрения мнения о целевом субъекте или переменной. Такой подход подразумевает использование оператора понижения доверия (будет рассмотрен ниже).

2.12.4.2 Рекомендуемое и функциональное доверие

Снова возвращаясь к предыдущему примеру, важно различать доверие к способности давать рекомендации (советы) о хорошем стоматологе, которое представляет собой *рекомендуемое доверие* (сформированное на основе рекомендации), и доверие к тому, что стоматолог – действительно хороший стоматолог, которое представляет собой *функциональное доверие* (доверие к профессиональной (функциональной) деятельности). Тем не менее, область (предназначение) доверия остаётся той же самой, а именно «*быть хорошим стоматологом*».

Полагая, что Миша продемонстрировал Маше, что он хорошо осведомлён в вопросах, связанных с лечением зубов, рекомендуемое доверие Маши к Мише относительно рекомендации хорошего стоматолога можно считать *прямым*. Полагая, что Тима несколько раз доказывал Мише, что он хороший стоматолог, функциональное доверие Миши к Тиме также можно считать прямым. Благодаря рекомендациям Миша, Маша также верит, что Тима – действительно хороший стоматолог. Однако, такое функциональное доверие должно рассматриваться как *косвенное* (непрямое), так как Маша лично не видела или проверяла профессионализм Тимы по лечению зубов.

Понятие «*рекомендуемое доверие*» отображает новый тип взаимосвязей на основе убеждений/доверия, которое дополняет взаимосвязи на основе убеждений и на основе функционального доверия. В таблице 2.3 представлены все три типа взаимосвязей на основе убеждений/доверия (она дополняет таблицу 2.2).

Таблица 2.3 – Обозначение взаимосвязей на основе веры/убеждённости и доверия

Тип взаимосвязи	Формальное обозначение	Обозначение в виде ребра (вектора) графа	Интерпретация
Вера/убеждённость	$[\mathcal{A}, X]$	$\mathcal{A} \rightarrow X$	Мнение субъекта $\mathcal{A}$ о переменной X
Функциональное доверие	$[\mathcal{A}, \mathcal{E}]$	$\mathcal{A} \rightarrow \mathcal{E}$	Мнение субъекта $\mathcal{A}$ относительно функционального доверия к субъекту $\mathcal{E}$
Рекомендуемое доверие	$[\mathcal{A}; \mathcal{B}]$	$\mathcal{A} \dashrightarrow \mathcal{B}$	Мнение субъекта $\mathcal{A}$ относительно рекомендуемого доверия к субъекту $\mathcal{B}$

2.12.4.3 Обозначение транзитивного доверия

В таблице 2.3 представлено обозначение взаимосвязей на основе простой веры/убеждённости и доверия с помощью ориентированных рёбер (векторов). Маршруты транзитивного доверия формируются путём соединения соседних рёбер (векторов) с помощью символа транзитивности «:», который, например, может интерпретироваться как связанная цепь (последовательность). Например, маршрут транзитивного доверия, проиллюстрированный на рисунке 2.14, можно формально отобразить следующим образом:

$$[\mathcal{A}, \mathcal{E}] \; = \; [\mathcal{A}; \mathcal{B}] : [\mathcal{B}, \mathcal{E}] \; . \qquad (2.10)$$

Таким образом, вектор рекомендуемого доверия от $\mathcal{A}$ до $\mathcal{B}$ обозначается как $[\mathcal{A}; \mathcal{B}]$, где символ «;» (точка с запятой) означает взаимосвязь на основе рекомендуемого доверия. Вектор функционального доверия от $\mathcal{B}$ до $\mathcal{E}$ обозначается как $[\mathcal{B}, \mathcal{E}]$, где символ «,» (запятая) означает взаимосвязь на основе веры/убеждённости или функционального доверия. Последовательное (транзитивное) соединение двух векторов (рёбер графа) доверия указывает на сформированный вектор (ребро) функционального доверия $[\mathcal{A}, \mathcal{E}]$.

Математически аппарат для вычисления сформированных мнений о доверии в сетях субъективного доверия (например, рисунок 2.14 и равенство 2.10) основан на применении оператора понижения доверия (представлен ниже).

Теперь немного изменим ранее рассмотренный пример. Пусть Миша (рисунок 2.15), на самом деле, не знает ни одного стоматолога, но он доверяет Томе, которая, по его убеждению, знает хорошего стоматолога. И по аналогии, Тома по просьбе Миши даёт ему положительную

рекомендацию относительно Тимы, которую Миша, в свою очередь, передаёт как свою рекомендацию Маше. В результате транзитивности получаем: Маша способна сформировать доверие к Тиме. Это со всей очевидностью иллюстрирует, что рекомендуемое доверие в данном примере связано со способностью давать рекомендации относительно стоматологов, которые могут лечить зубы, и что функциональное доверие в этом примере связано со способностью реально лечить зубы. В этом примере область доверительных взаимоотношений определяется выражением «*быть высоко квалифицированным стоматологом*».

Формализованное обозначение графа на рисунке 2.15 можно отобразить с помощью следующего равенства:

$$[\mathcal{A}, \mathcal{E}] \;=\; [\mathcal{A}; \mathcal{B}] : [\mathcal{B}; \mathcal{C}] : [\mathcal{C}, \mathcal{E}] \,. \tag{2.11}$$

Функциональное доверие для примера на рисунке 2.15 может быть представлено как двоичное мнение $\omega_{\mathcal{E}}^{\mathcal{C}}$, которое отражает уровень функционального доверия субъекта $\mathcal{C}$ к субъекту $\mathcal{E}$. Тождественное обозначение $\omega_{t_{\mathcal{E}}}^{\mathcal{C}}$ точно определяет веру в благонадёжность $\mathcal{E}$, выраженную через переменное значение $t_{\mathcal{E}}$, где $t_{\mathcal{E}}$ означает множество твёрдых убеждений (твёрдой веры), и указывает на то, что у субъекта $\mathcal{C}$ сформировалось высокое доверие к субъекту $\mathcal{E}$.

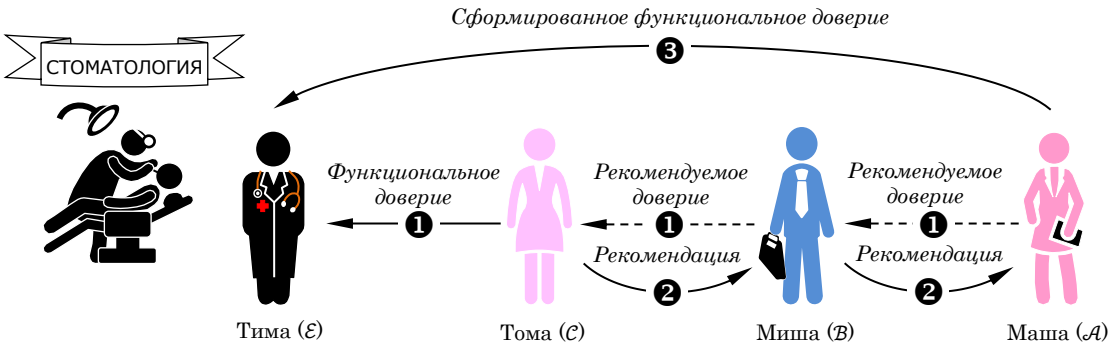

Рисунок 2.15 – Доверие формируемое на основе транзитивности

Аналогично, мнение $\omega_{\mathcal{B}}^{\mathcal{A}}$ отражает рекомендуемое доверие субъекта $\mathcal{A}$ к субъекту $\mathcal{B}$, и имеет тождественное обозначение $\omega_{t_{\mathcal{B}}}^{\mathcal{A}}$, в котором состояние $t_{\mathcal{B}}$ интерпретируется, например, как «*субъект $\mathcal{B}$ может дать хорошую рекомендацию относительно стоматологов*».

При решении различных задач по оценке того или иного субъективного мнения относительно доверия в сетях субъективного доверия можно воспользоваться более простым обозначением маршрутов транзитивного доверия, которое исключает чрезмерное использование квадратных скобок. В частности, для примера на рисунке 2.15 можно использовать следующее компактное выражение:

$$[\mathcal{A}, \mathcal{E}] \;=\; [\mathcal{A}; \mathcal{B}; \mathcal{C}, \mathcal{E}] \;\; . \tag{2.12}$$

2.12.4.4 Семантические требования транзитивности доверия

Различие между функциональным и рекомендуемым доверием может показаться незначительным. Интерпретация рекомендуемого доверия состоит в том, что Маша доверяет Мише относительно его рекомендаций о ком-либо (тот, кто может давать рекомендации (советовать) относительно кого-то и т.д.), кто может дать рекомендации относительно стоматологов. В то же самое время, рекомендуемое доверие всегда предполагает наличие функционального доверия конечному субъекту или веры в конечный субъект транзитивного маршрута, который представляет собой, как в ранее рассмотренном примере, хорошего стоматолога.

Вариант «*рекомендации доверия*» может рассматриваться как рекурсивный, и поэтому любая последовательность транзитивного доверия (произвольной длины) может быть отображена определённым способом. Это правило отображается с помощью следующего критерия.

Определение 2.8 (Критерий возникновения функционального доверия). Возникновение функционального доверия через рекомендуемое доверие возможно только тогда, когда последний вектор (ребро) доверия представлял функциональное доверие/убеждённость, а все предыдущие векторы (рёбра) доверия представляли рекомендуемое доверие. □

В реальных ситуациях, область (предназначение) доверия может характеризоваться как общая или конкретная. Например, знание стоматолога, который высококвалифицированно вставляет зубные протезы, является более конкретным по сравнению со знанием просто хорошего стоматолога, т.е. первая профессиональная область является подмножеством последней. Если область функционального доверия равна или является подмножеством областей рекомендуемого доверия, то можно сформировать транзитивные маршруты. Это можно выразить с помощью следующего критерия взаимосогласованности.

Определение 2.9 (Критерий взаимосогласованности области доверия). Допустимый маршрут транзитивного доверия требует, чтобы область доверия функционального (и, следовательно, последнего) вектора доверия/убеждённости на маршруте находилась на пересечении областей всех предыдущих векторов рекомендуемого доверия на маршруте. □

Проще говоря, каждый вектор доверия может иметь только одну и ту же область доверия. Таким образом, распространение транзитивного доверия возможно на основе векторов функционального и рекомендуемого доверия, которые имеют одну область доверия. Транзитивный путь доверия останавливается на первом появившемся векторе функционального доверия. Конечно, субъект может иметь как функциональное, так и рекомендуемое доверие к другому субъекту, но это должно быть отражено в виде двух отдельных векторов доверия. Наличие обоих векторов функционального и рекомендуемого доверия, например, от Тома к Тиме, и должно интерпретироваться следующим образом: «*Тома доверяет Тиме, не только потому, что он – хороший*

стоматолог, но и потому, что он даёт рекомендации относительно других стоматологов».

2.12.5 Оператор понижения доверия

Доверие можно рассматривать как особый вид веры/убеждённости. И в этом смысле доверие может быть смоделировано как мнение, которое может использоваться в качестве входного аргумента или в качестве выходных результатов в моделях логического анализа, основанных на СЛ. Для обозначения доверия в виде субъективного мнения используется термин *мнение о доверии*.

2.12.5.1 Принцип понижения доверия

Общая идея понижения доверия состоит в том, чтобы отразить степень доверия к источнику информации (субъекту), а затем понизить ценность информации, предоставленной этим источником (субъектом), как функцию доверия к источнику (субъекту). Доверие и предоставляемая информация отображаются в форме субъективных мнений, а затем определяется соответствующая операция относительно таких мнений с целью определения мнения с понижением доверия.

Пусть субъект $\mathcal{A}$ – доверяющая сторона, а субъект $\mathcal{B}$ – источник информации, который может быть субъектом, формирующим мнение о рекомендации, или это объект B – датчик, вырабатывающий данные, которые могут быть преобразованы во мнение. Предположим, что источник $\mathcal{B}(B)$ предоставляет информацию субъекту $\mathcal{A}$ о состоянии переменной X, как субъективное мнение о переменной X. Также предположим, что субъект $\mathcal{A}$ имеет мнение о благонадёжности субъекта $\mathcal{B}$ относительно предоставления информации о переменной X, то есть область доверия заключается в предоставлении информации о X. Основываясь на объединении доверия субъекта $\mathcal{A}$ к субъекту $\mathcal{B}$, а также мнения субъекта $\mathcal{B}$ о переменной X, которое было получено субъектом $\mathcal{A}$, можно определить мнение субъекта $\mathcal{A}$ о переменной X. Эта процедура проиллюстрирована на рисунке 2.16.

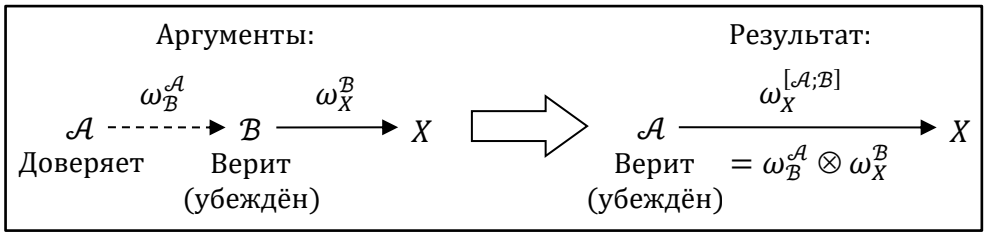

Рисунок 2.16 – Мнение с понижением доверия

Несколько операторов понижения доверия в СЛ описаны в [62,64]. Общее отображение понижения доверия основано на условных выражениях [64], в то время как частные случаи могут быть выражены с помощью конкретных операторов понижения доверия. Ниже будет рассмотрен понижение доверия, зависимого от вероятности, которое приводит к увеличению неопределённости в сформированном мнении субъекта $\mathcal{A}$ о переменной X, в зависимости от прогнозируемого недоверия к рекомендующему субъекту $\mathcal{B}$ или к источнику данных B.

2.12.5.2 Понижение доверия в маршрутах с двумя векторами

Рекомендуемое доверие субъекта $\mathcal{A}$ к субъекту $\mathcal{B}$ можно формально отобразить как двоичное мнение в ОА $\mathbb{T}_{\mathcal{B}} = \{t_{\mathcal{B}}, \bar{t}_{\mathcal{B}}\}$, где величины $t_{\mathcal{B}}$ и $\bar{t}_{\mathcal{B}}$ означают *доверенный* и *не доверенный*, соответственно. Для простоты обозначим это мнение $\omega_{\mathcal{B}}^{\mathcal{A}} = \left(b_{\mathcal{B}}^{\mathcal{A}}, d_{\mathcal{B}}^{\mathcal{A}}, u_{\mathcal{B}}^{\mathcal{A}}, a_{\mathcal{B}}^{\mathcal{A}}\right)$, которое тождественно обозначению (по аналогии с тождеством в §2.12.2.1) данного мнения $\omega_{t_{\mathcal{B}}}^{\mathcal{A}} = (b_{t_{\mathcal{B}}}^{\mathcal{A}}, d_{t_{\mathcal{B}}}^{\mathcal{A}}, u_{t_{\mathcal{B}}}^{\mathcal{A}}, a_{t_{\mathcal{B}}}^{\mathcal{A}})$. Тем не менее будем использовать упрощённое выражение. Параметры $b_{\mathcal{B}}^{\mathcal{A}}$, $d_{\mathcal{B}}^{\mathcal{A}}$ и $u_{\mathcal{B}}^{\mathcal{A}}$ отражают уровни доверия субъекта $\mathcal{A}$, т.е. субъект $\mathcal{A}$ доверяет, не доверяет или не определился относительно благонадёжности субъекта $\mathcal{B}$ на текущий момент, а параметр $a_{\mathcal{B}}^{\mathcal{A}}$ – априорная вероятность, которую субъект $\mathcal{A}$ *априори* присвоил бы благонадёжности субъекта $\mathcal{B}$, т.е. до получения от субъекта $\mathcal{B}$ его мнения $\omega_X^{\mathcal{B}}$.

Определение 2.10 (Понижение зависимого от вероятности доверия для маршрута с двумя векторами). Предположим, что существуют субъекты $\mathcal{A}$ и $\mathcal{B}$, и при этом субъект $\mathcal{A}$ сформировал рекомендуемое доверие к субъекту $\mathcal{B}$ в области доверия, представленной как ОА $\mathbb{X}$. Пусть X – переменная в ОА $\mathbb{X}$, и пусть $\omega_X^{\mathcal{B}} = (\boldsymbol{b}_X^{\mathcal{B}}, u_X^{\mathcal{B}}, \boldsymbol{a}_X^{\mathcal{B}})$ – общее мнение субъекта $\mathcal{B}$ о переменной X, которое рекомендовано субъектом $\mathcal{B}$ субъекту $\mathcal{A}$. Также предположим, что рекомендуемое доверие к субъекту $\mathcal{B}$ относительно рекомендуемого убеждения о переменной X, обозначается как $\omega_{\mathcal{B}}^{\mathcal{A}}$. Тогда понижение доверия отображается с помощью следующего равенства:

$$\omega_X^{[\mathcal{A};\mathcal{B}]} = \omega_{\mathcal{B}}^{\mathcal{A}} \otimes \omega_X^{\mathcal{B}} \ . \tag{2.13}$$

Оператор понижения доверия объединяет мнение субъекта $\mathcal{A}$ о рекомендуемом доверии к субъекту $\mathcal{B}$, обозначаемое как $\omega_{\mathcal{B}}^{\mathcal{A}}$, с пониженным мнением субъекта $\mathcal{B}$ о переменной X, обозначаемым как $\omega_X^{\mathcal{B}}$, с целью определения мнения субъекта $\mathcal{A}$ о переменной X, обозначаемого как $\omega_X^{[\mathcal{A};\mathcal{B}]}$. Параметры результирующего мнения $\omega_X^{[\mathcal{A};\mathcal{B}]}$ определяются следующим образом:

$$\omega_X^{[\mathcal{A};\mathcal{B}]}: \begin{cases} \boldsymbol{b}_X^{[\mathcal{A};\mathcal{B}]}(x) = \mathbf{P}_{\mathcal{B}}^{\mathcal{A}} \boldsymbol{b}_X^{\mathcal{B}}(x) \,, \\ u_X^{[\mathcal{A};\mathcal{B}]} \quad = 1 - \mathbf{P}_{\mathcal{B}}^{\mathcal{A}} \sum_{x \in \mathcal{R}(\mathbb{X})} \boldsymbol{b}_X^{\mathcal{B}}(x) \,, \\ \boldsymbol{a}_X^{[\mathcal{A};\mathcal{B}]}(x) = \boldsymbol{a}_X^{\mathcal{B}}(x) \,. \end{cases} \tag{2.14}$$

□

На рисунке 2.17 проиллюстрирован результат вычисления мнения с использованием оператора понижения доверия. Рассмотренный далее пример анализирует простую сеть доверия:

$$\mathcal{A} \dashrightarrow \mathcal{B} \rightarrow X\,, \tag{2.15}$$

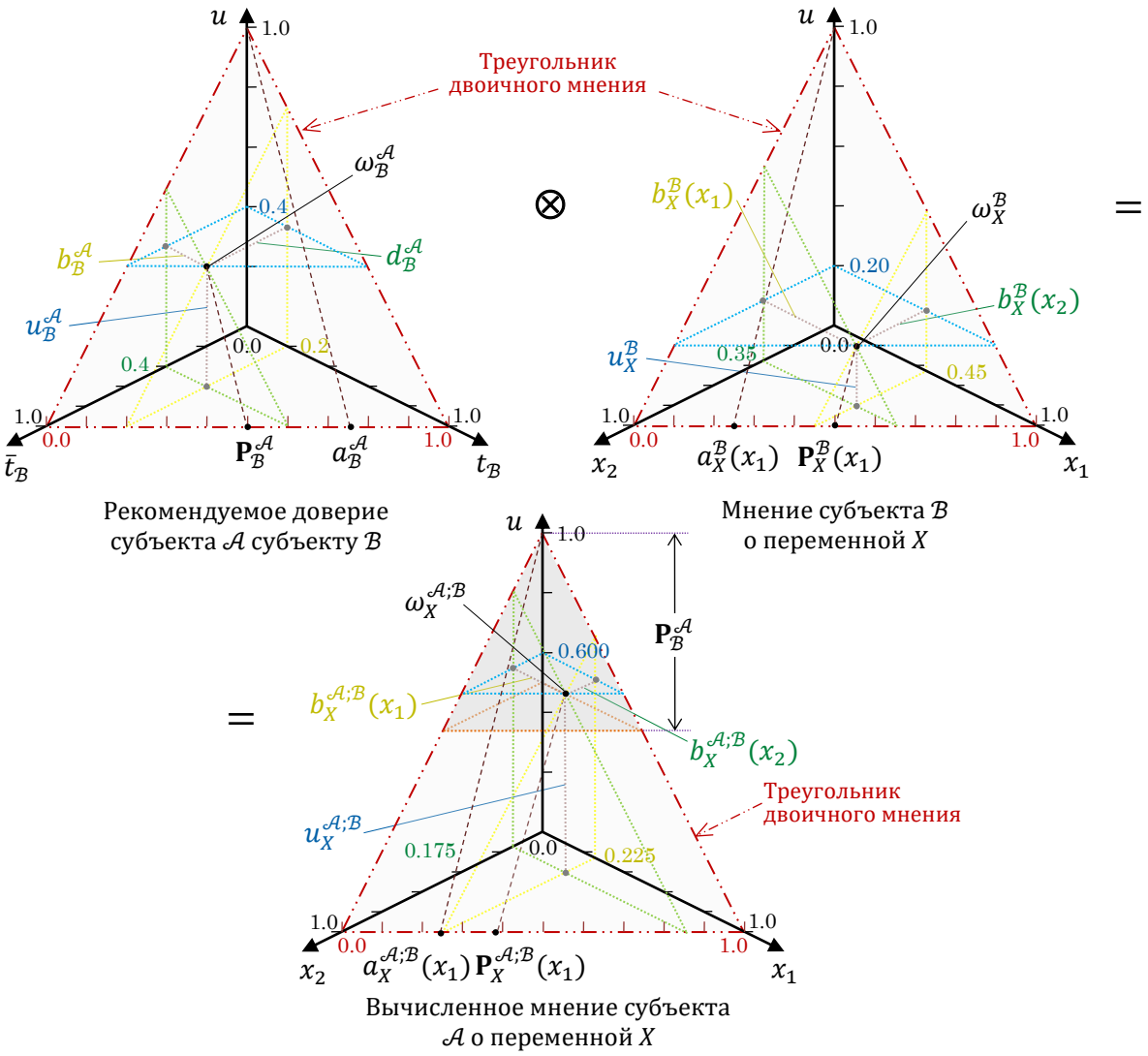

Рисунок 2.17 – Численный пример понижение доверия, зависимого от вероятности

где субъект $\mathcal{A}$ доверяет субъекту $\mathcal{B}$, который отправил субъекту $\mathcal{A}$ своё мнение о переменной X. Обозначим доверие субъекта $\mathcal{A}$ субъекту $\mathcal{B}$ как $\omega_{\mathcal{B}}^{\mathcal{A}}$, а мнение субъекта $\mathcal{B}$ о переменной X как $\omega_X^{\mathcal{B}}$. Используем $\omega_{\mathcal{B}}^{\mathcal{A}}$ и $\omega_X^{\mathcal{B}}$ в качестве входных аргументов для равенства (2.14), чтобы вычислить мнение субъекта $\mathcal{A}$ о переменной X, которое обозначим как $\omega_X^{[\mathcal{A};\mathcal{B}]}$.

Ниже представлены численные значения[21] мнений $\omega_{\mathcal{B}}^{\mathcal{A}}$ и $\omega_X^{\mathcal{B}}$, как входных аргументов, и вычисленное значение мнения субъекта $\mathcal{A}$ о переменной X $\omega_X^{[\mathcal{A};\mathcal{B}]}$ с использованием оператора понижения доверия (равенство 2.14).

$$\omega_{\mathcal{B}}^{\mathcal{A}}:\begin{cases} b_{\mathcal{B}}^{\mathcal{A}} = 0.20\,, \\ d_{\mathcal{B}}^{\mathcal{A}} = 0.40\,, \\ u_{\mathcal{B}}^{\mathcal{A}} = 0.40\,, \\ a_{\mathcal{B}}^{\mathcal{A}} = 0.75\,, \\ \mathrm{P}_{\mathcal{B}}^{\mathcal{A}} = 0.50\,, \end{cases} \quad \omega_X^{\mathcal{B}}:\begin{cases} \boldsymbol{b}_X^{\mathcal{B}}(x_1) = 0.45\,, \\ \boldsymbol{b}_X^{\mathcal{B}}(x_2) = 0.35\,, \\ u_X^{\mathcal{B}} = 0.20\,, \\ \boldsymbol{a}_X^{\mathcal{B}}(x_1) = 0.25\,, \\ \mathbf{P}_X^{\mathcal{B}}(x_1) = 0.50\,, \end{cases} \quad \omega_X^{[\mathcal{A};\mathcal{B}]}:\begin{cases} \boldsymbol{b}_X^{[\mathcal{A};\mathcal{B}]}(x_1) = 0.225\,, \\ \boldsymbol{b}_X^{[\mathcal{A};\mathcal{B}]}(x_2) = 0.175\,, \\ u_X^{[\mathcal{A};\mathcal{B}]} = 0.600\,, \\ \boldsymbol{a}_X^{[\mathcal{A};\mathcal{B}]}(x_1) = 0.250\,, \\ \mathbf{P}_X^{[\mathcal{A};\mathcal{B}]}(x_1) = 0.375\,. \end{cases} \tag{2.16}$$

Вычисление мнения с понижением доверия $\omega_X^{[\mathcal{A};\mathcal{B}]}$ к X, как правило, приводит к увеличению множества неопределённости по сравнению с первоначальным мнением, рекомендованным субъектом $\mathcal{B}$, т.е. увеличение множества неопределённости обусловлено прогнозируемой (апостериорной) вероятностью мнения о рекомендуемом доверии $\omega_{\mathcal{B}}^{\mathcal{A}}$. Понижение доверия основано на принципе: чем меньше прогнозируемая вероятность $\mathrm{P}_{\mathcal{B}}^{\mathcal{A}}$, тем больше множество неопределённости вычисленного мнения $\omega_{\mathcal{B}}^{\mathcal{A}}$.

На рисунке 2.17 показан общий алгоритм вычисления с помощью оператора понижения доверия, зависимого о вероятности, на котором «*итоговое мнение*» ограничено тёмно-серым треугольником в верхней части нижнего (результирующего) треугольника двоичного мнения. Высота тёмно-серого треугольника соответствует прогнозируемой вероятности доверия во мнении о доверии. В результате трёхмерное представление $\omega_X^{\mathcal{B}}$ «*сжимается*» пропорционально $\mathrm{P}_{\mathcal{B}}^{\mathcal{A}}$, и становится трёхмерным представлением мнения (треугольник мнения) внутри тёмно-серого треугольника.

Следует упомянуть некоторые конкретные случаи. В случае, когда прогнозируемая вероятность доверия равна единице, что означает полное доверие к субъекту (источнику данных), доверяющая сторона полностью признаёт полученное мнение о доверии/убеждённости, а это, в свою очередь, означает, что вычисленное мнение равно полученному мнению. В случае, когда прогнозируемая вероятность доверия равна нулю, что означает полное недоверие к субъекту (источнику данных), полученное мнение, с точки зрения доверия к нему, понижено и становится бессмысленным мнением, а это, в свою очередь, означает, что полученное мнение полностью отвергается (игнорируется).

Следует отметить, что описанный выше оператор понижения доверия является частным случаем общего оператора понижения доверия для вычисления мнений для маршрутов доверия произвольной длины.

[21] Численные значения были выбраны случайным образом.

2.12.5.3 Пример практического использования понижения доверия

Следующий пример показывает, как конкретно используется понижение доверия в реальных ситуациях. Предположим, что Маша приехала в длительную командировку в другой город, и что ей для работы в системе ЭДО организации нужно получить пару ассиметричных ключей и $СЕРТ_{ОК}$ в одном из местных ЦС, так как в организации своего ЦС нет. Маша, на основе имеющейся у неё предварительной информации, предполагает, что в городе только половину ЦС можно считать надёжными. Она, конечно, хотела бы найти самый надёжный, с точки зрения сотрудников организации. Во время общения с сотрудником по имени Миша она поинтересовалась относительно ЦС, который порекомендовал ей ЦС «Луч».

Также полагаем, что Маша ранее не была знакома с Мишей, так что априори её доверие к Мише основано на высокой степени неопределённости. Однако Маше достаточно предположить, что другие сотрудники организации дают хорошие рекомендации и это повышает априорную вероятность её доверия к рекомендациям сотрудников. Даже если её доверие к Мише – бессмысленно, то высокая априорная вероятность приведёт к высокой прогнозируемой вероятности доверия. Полагая, что Миша даёт очень положительную рекомендацию о ЦС «Луч», Маша сформирует положительное мнение о ЦС «Луч», основанное на рекомендации Миши.

Данный пример может иметь своё численное отображение. На рисунке 2.18 показано понижение доверия в СЛ, в котором используются аргументы, наиболее подходящие для случая с рекомендацией ЦС.

В результате полученной рекомендации Маша становится совершенно уверенной в том, что ЦС «Луч» – приемлемый ЦС, и собирается на следующий день получить в нём пару ассиметричных ключей и $СЕРТ_{ОК}$. Тем не менее, если Маша получит вторую рекомендацию, которая противоречит первой, то её доверие к ЦС «Луч» может резко упасть, и поэтому она может передумать. Анализ такого варианта развития событий будет рассмотрен ниже.

2.12.5.4 Понижение доверия в многовекторных маршрутах

Теперь рассмотрим способ вычисление транзитивного доверия в случае трёх- или более векторных маршрутов доверия. Рассмотрим граф, который отображает маршрут доверия от узла $\mathcal{A}_1$ до узла X через произвольное число промежуточных узлов $\mathcal{A}_1, \dots, \mathcal{A}_n$:

$$\text{Многовекторный граф доверия: } (\mathcal{A}_1 \to X) \;=\; (\mathcal{A}_1 \dashrightarrow \mathcal{A}_1 \;\dashrightarrow \dots \mathcal{A}_n \to \; X)\,. \qquad (2.17)$$

Вектор вычисленного функционального убеждения $[\mathcal{A}_1, X]$ из равенства (1.17) формально может быть представлен с помощью различных тождественных форм:

$$\text{Полное формальное обозначение: } [\mathcal{A}_1, X] = \; [\mathcal{A}_1; \mathcal{A}_2] : [\mathcal{A}_2; \mathcal{A}_3] : \dots [\mathcal{A}_n, X]\,,$$

Сокращённое обозначение маршрута доверия: $[\mathcal{A}_1, X] = [\mathcal{A}_1; \mathcal{A}_2; \ldots \mathcal{A}_n, X]$,

Разделение рекомендуемого и функционального: $[\mathcal{A}_1, X] = [\mathcal{A}_1; \ldots \mathcal{A}_n] : [\mathcal{A}_n, X]$,

Сокращённое обозначение с разделением: $[\mathcal{A}_1, X] = [\mathcal{A}_1; \mathcal{A}_n] : [\mathcal{A}_n, X]$. (2.18)

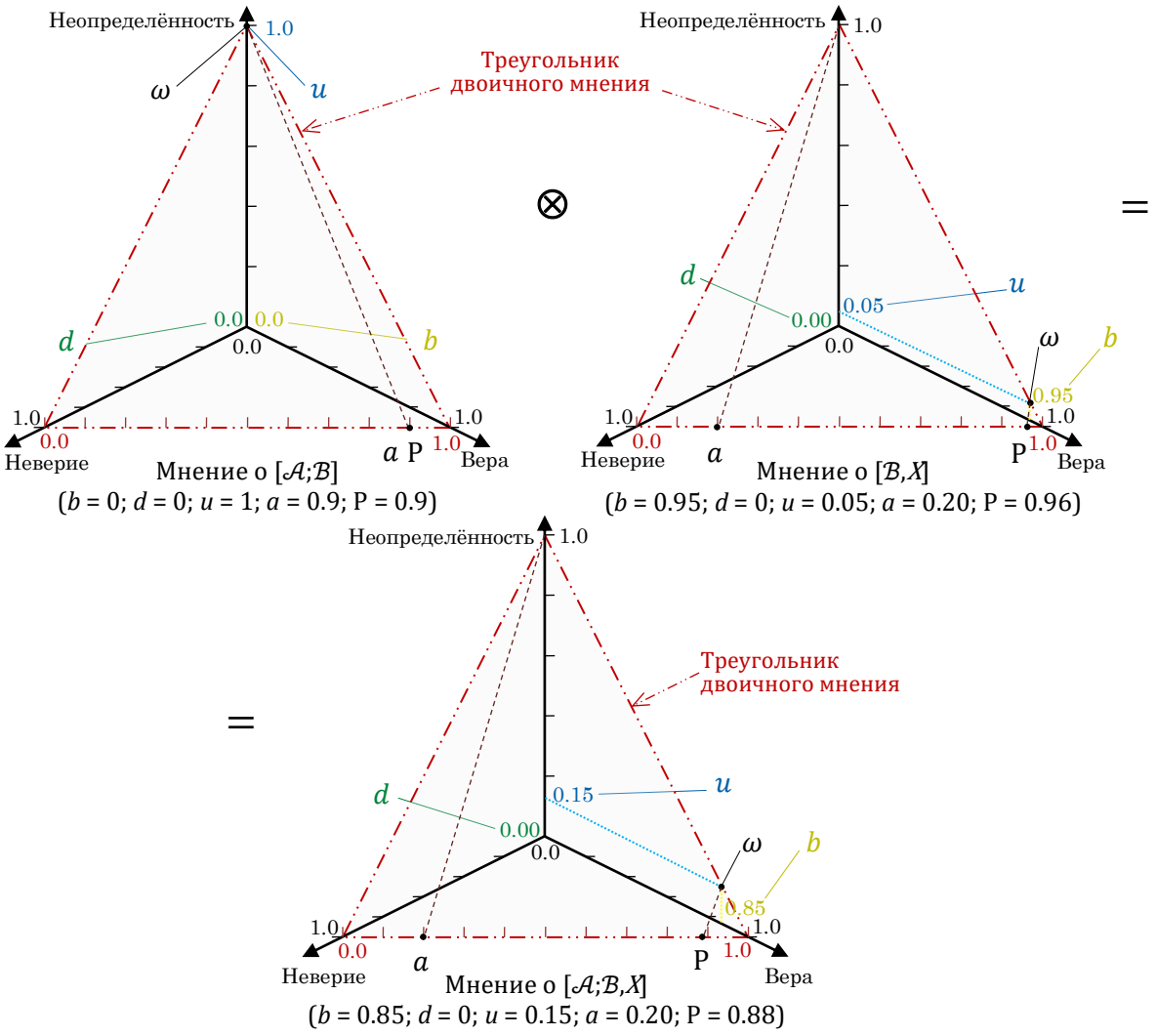

Рисунок 2.18 – Понижение доверия в примере с рекомендацией ЦС «Луч»

Многовекторный маршрут транзитивного доверия, равенство (2.17), состоит из начального субмаршрута рекомендуемого доверия и завершается вектором функционального доверия/убеждения, которые можно отобразить следующим образом:

Субмаршрут рекомендуемого доверия: $[\mathcal{A}_1; \ldots \mathcal{A}_n]$, (2.19)

Вектор функционального доверия/убеждения: $[\mathcal{A}_n, X]$. (2.20)

Если каждому вектору «*присвоено*» мнение, то мнения внутренних субъектов («узлов») о доверии обозначаются как $\omega^{\mathcal{A}_i}_{\mathcal{A}_{(i+1)}}$, а функциональное мнение конечного вектора обозначается как $\omega^{\mathcal{A}_n}_{X}$. Все мнения внутренних субъектов отображают рекомендуемое доверие, а мнение, относящееся к конечному вектору, – функциональное доверие.

Прогнозируемая (апостериорная) вероятность маршрута рекомендуемого доверия $[\mathcal{A}_1; \mathcal{A}_n]$ вычисляется следующим образом:

$$\text{Прогнозируемая вероятность рекомендуемого доверия: } \mathrm{P}_{\mathcal{A}_n}^{\mathcal{A}_1} = \prod_{i=1}^{n-1} \mathrm{P}_{\mathcal{A}_{(i+1)}}^{\mathcal{A}_i} . \quad (2.21)$$

Понижение доверия в маршруте рекомендуемого доверия произвольной длины – функция прогнозируемой вероятности рекомендуемого доверия, вычисляемая в соответствие с равенством (2.21).

Определение 2.11 (Понижение доверия в многовекторных маршрутах). Предположим, что маршрут транзитивного доверия состоит из соединённых векторов доверия между субъектами $\mathcal{A}_1, \ldots, \mathcal{A}_n$, за которым следует завершающий вектор доверия/убеждения между последним субъектом $\mathcal{A}_n$ и целевым узлом X, а цель такого маршрута – вычислить мнение о векторе между первым субъектом $\mathcal{A}_1$ и целевым узлом X. Параметры вычисленного мнения $\omega_X^{\mathcal{A}_1}$ определяются следующим образом:

$$\omega_X^{\mathcal{A}_1}: \begin{cases} \boldsymbol{b}_X^{\mathcal{A}_1}(x) = \mathrm{P}_{\mathcal{A}_n}^{\mathcal{A}_1} \boldsymbol{b}_X^{\mathcal{A}_n}(x) , \\ u_X^{\mathcal{A}_1} \quad = 1 - \mathrm{P}_{\mathcal{A}_n}^{\mathcal{A}_1} \sum_{x \in \mathcal{R}(\mathbb{X})} \boldsymbol{b}_X^{\mathcal{A}_n}(x) , \\ \boldsymbol{a}_X^{\mathcal{A}_1}(x) = \boldsymbol{a}_X^{\mathcal{B}}(x) . \end{cases} \quad (2.22)$$

□

Принцип понижения многовекторного доверия состоит в том, чтобы определить прогнозируемые вероятности части рекомендуемого доверия, в соответствие с (2.22), как оценку надёжности сети доверия. Затем, такая оценка надёжности используется для понижения функционального мнения о рекомендуемом доверии $\omega_X^{\mathcal{A}_n}$ для заключительного вектора веры/убеждения $[\mathcal{A}_n, X]$. Другими словами, оператор понижения доверия использует в качестве одного из входных аргументов последовательное произведение прогнозируемых вероятностей.

В случае, если каждое мнение о рекомендуемом доверии имеет прогнозируемую вероятность $\mathrm{P}_{\mathcal{A}_{(i+1)}}^{\mathcal{A}_i} = 1$, то итоговое произведение прогнозируемых вероятностей рекомендуемого доверия также будет равно 1, т.е. вычисленное мнение $\omega_X^{\mathcal{A}_1}$ равно полученному рекомендуемому мнению $\omega_X^{\mathcal{A}_n}$. В случае, если каждое мнение о рекомендуемом доверии имеет прогнозируемую вероятность $\mathrm{P}_{\mathcal{A}_{(i+1)}}^{\mathcal{A}_i} = 0$, то итоговое произведение прогнозируемых вероятностей рекомендуемого доверия также будет равно 0, следовательно, вычисленное мнение $\omega_X^{\mathcal{A}_1}$ становится бессмысленным.

Следует отметить, что оператор вычисления мнений для маршрутов доверия произвольной длины, рассмотренный выше, – обобщение оператора понижения доверия для двухвекторных маршрутов (§2.12.4.2)

Для примера рассмотрим следующую сеть доверия:

$$\begin{aligned}[\mathcal{A},X] &= [\mathcal{A};\mathcal{B}]:[\mathcal{B};\mathcal{C}]:[\mathcal{C};\mathcal{D}]:[\mathcal{D},X]\\ &= [\mathcal{A};\mathcal{B};\mathcal{C};\mathcal{D},X]\\ &= [\mathcal{A};\mathcal{B};\mathcal{C};\mathcal{D}]:[\mathcal{D},X] = [\mathcal{A};\mathcal{D}]:[\mathcal{D},X].\end{aligned} \tag{2.23}$$

В таблице 2.4 представлен численный пример мнений для маршрута доверия, в соответствие с (2.23), а также показан результат вычисления оператора понижения доверия. Предполагается, что X – бинарная переменная, а ω_X – мнение в двоичной форме.

Несмотря на то, что каждый вектор рекомендуемого доверия имеет высокую прогнозируемую вероятность, их произведение быстро снижается до условно низкого значения $\mathrm{P}_{\mathcal{D}}^{\mathcal{A}} = 0.44$. А мнение с понижением доверия $\omega_X^{[\mathcal{A};\mathcal{D}]}$становится очень неопределённым.

Таблица 2.4 – Пример понижения доверия для многовекторного маршрута

Параметры:		Входные мнения: $\omega_{\mathcal{B}}^{\mathcal{A}}$	$\omega_{\mathcal{C}}^{\mathcal{B}}$	$\omega_{\mathcal{D}}^{\mathcal{C}}$	$\omega_X^{\mathcal{D}}$	Произведение: $\mathrm{P}_{\mathcal{D}}^{\mathcal{A}}$	Вычисленное мнение: $\omega_X^{[\mathcal{A};\mathcal{D}]}$
Вера/убеждённость:	b	0.20	0.20	0.20	0.80		0.35
Неверие:	d	0.10	0.10	0.10	0.20		0.09
Неопределённость:	u	0.70	0.70	0.70	0.00		0.56
Априорная вероятность:	a	0.80	0.80	0.80	0.10		0.10
Прогнозируемая вероятность:	P	0.76	0.76	0.76	0.80	0.44	0.41

Такой результат отражает интуитивное предположение о том, что *длинный маршрут косвенного доверия быстро становится бесполезным*, потому что функциональное доверие, вычисленное для него, становится слишком неопределённым.

Очевиден вопрос, а может ли длинный многовекторный маршрут доверия быть практичным? В повседневной жизни мы редко полагаемся на маршруты доверия, длина которых превышает два вектора. Например, мало кто поверит такой рекомендации: «Один мой коллега сказал мне, что у его сестры есть друг, который знает хорошего стоматолога, так почему бы вам не вылечить зубы в его стоматологическом центре?!»

В реальной жизни люди начинают сомневаться в правдивости информации или рекомендации в тех ситуациях, когда между информацией от первоначального источника и нашей собственной информацией о цели X высокая степень различия, потому что мы нередко видим, как информация искажается если она передаётся от человека к человеку многократно. Это происходит потому, что мы, люди, являемся довольно ненадёжными субъектами относительно правдивого отображения и передачи получаемой нами информации.

Однако, ИТС способны корректно распространять информацию через несколько сетевых узлов с высокой надёжностью. Поэтому транзитивность доверия, основанная на длинных маршрутах, больше подходит для ИТС, чем для социальных сетей.

Узкоспециализированные мобильные и сенсорные сети представляют собой вид ИТС, в которых несколько узлов зависят друг от друга, с точки зрения предоставления услуг. Типичная характеристика таких сетей – неопределённая надёжность каждого узла, а также отсутствие контроля со стороны одного узла других узлов. Поэтому транзитивные вычисления доверия с использованием аппарата СЛ весьма актуальны для узкоспециализированных мобильных и сенсорных сетей, даже в случае длинных маршрутов доверия.

2.12.6 Слияние доверия

Обычно для получения более полной информации, например, в процедурах принятия решений, необходимо получать информацию из нескольких источников. В случае использования мнений, такой процесс можно назвать *слиянием доверия*, которое означает, что мнения, вычисленные для различных маршрутов доверия, сливаются в одно мнение.

Продолжим рассматривать пример из §2.12.3.1, в котором Маше необходимо вылечить зубы. Маша получила рекомендацию Миши о посещении стоматологического центра, к котором работает стоматолог Тима. Теперь предположим, что Маша сомневается в рекомендации Миши, и поэтому она хотела бы получить второе мнение. Поэтому она спрашивает у другой своей коллеги Томы её мнение о Тиме (его стоматологическом центре). Маршрут доверия, включающий обе рекомендации, показан на рисунке 2.19.

Формальное обозначение графа, показанного на рисунке 2.19, представлено ниже. Кроме того, такая сеть доверия использует транзитивность доверия, которое вычисляется с помощью оператора понижения доверия:

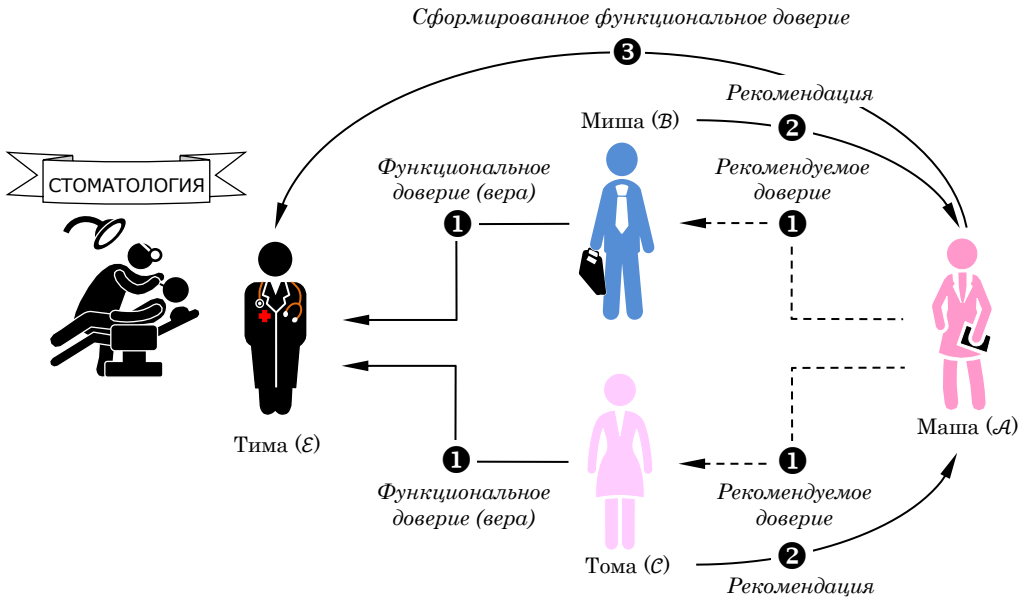

Рисунок 2.19 – Пример слияния доверия

Формальное обозначение слияния доверия: $[\mathcal{A},\mathcal{E}] = ([\mathcal{A};\mathcal{B}]:[\mathcal{B},\mathcal{E}])\diamond([\mathcal{A};\mathcal{C}]:[\mathcal{C},\mathcal{E}])$,

Компактное обозначение: $[\mathcal{A},\mathcal{E}] = [\mathcal{A};\mathcal{B},\mathcal{E}]\diamond[\mathcal{A};\mathcal{C},\mathcal{E}]$. (2.24)

Вычисление слияния доверия основано на двух процедурах понижения доверия и слияние убеждённостей, так как это – фактическое слияние двух мнений с понижением доверия. Двоичная переменная $X = \{"\mathcal{E}-\text{надёжный}","\mathcal{E}-\text{ненадёжный}"\}$ может отображать целевое доверие к $\mathcal{E}$ (рисунок 2.19), так как аналитик $\mathcal{A}$ фактически вычисляет мнение о переменной X. Общий принцип слияния доверия относительно двух мнений о переменной X показано на рисунке 2.20.

В соответствии с **Опред.2.7** для обозначения слияния двух маршрутов доверия $[\mathcal{A};\mathcal{B},X]$ и $[\mathcal{A};\mathcal{C},X]$ (компактная форма) используется символ «◇». Выбор такого символа был обусловлен сходством между его ромбовидной формой и графом типовой сети слияния доверия (левая часть рисунка 2.20). Отображение вычисленного мнения субъекта $\mathcal{A}$ о переменной X, как функции слияния доверия, следующее:

$$\omega_X^{[\mathcal{A};\mathcal{B}]\diamond[\mathcal{A};\mathcal{C}]} = \left(\omega_{\mathcal{B}}^{\mathcal{A}} \otimes \omega_X^{\mathcal{B}}\right)\oplus\left(\omega_{\mathcal{C}}^{\mathcal{A}} \otimes \omega_X^{\mathcal{C}}\right). \quad (2.25)$$

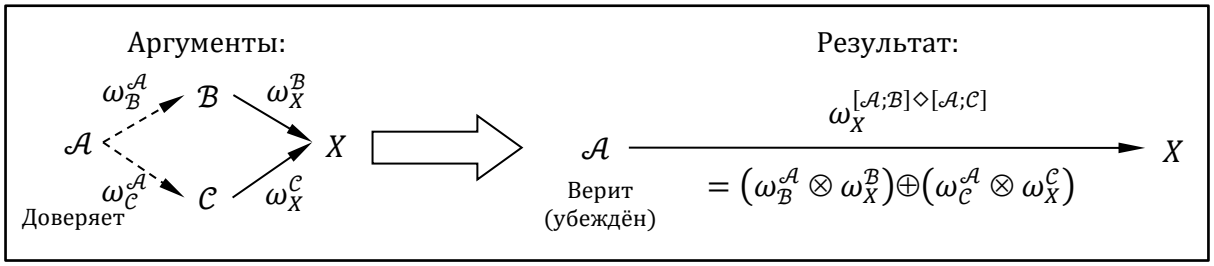

Рисунок 2.20 – Слияние мнений с понижением доверия

Пример на рисунке 2.20 предусматривает, что субъект (аналитик) $\mathcal{A}$ получил мнения о переменной X от субъектов (из источников) $\mathcal{B}$ и $\mathcal{C}$, и что субъект $\mathcal{A}$ обладает рекомендуемыми довериями о субъектах $\mathcal{B}$ и $\mathcal{C}$. В целом, мнения, которые аналитик получает из других источников, – *исходные мнения*.

Теперь конкретизируем, в случае, если источником является (разумный) субъект, то исходное мнение является *рекомендуемым мнением*, поскольку оно представляет собой однозначную рекомендацию субъекта. Рекомендуемое мнение может отображать рекомендуемое доверие к другому исходному субъекту (узлу) или это может быть мнение о вере в целевую переменную.

Оператор слияния нескольких маршрутов доверия должен выбираться из группы операторов слияния убеждений/веры [89], к которым относятся:

- ограниченное слияние убеждений;
- суммарное слияние убеждений;

▪ усреднённое слияние убеждений;

▪ взвешенное слияние убеждений.

В частности, равенство (2.25) содержит символ «⊕», который указывает на оператор суммарного слияния убеждений.

В таблице 2.15 представлен численный пример, который отражает результат суммарного слияния доверия в ситуации, представленной на рисунке 2.19. Вначале, мнение о доверии вычисляется для каждого маршрута с использованием оператора понижения доверия (**Опред.2.10** и **Опред.2.11**). Затем, два вычисленных мнения о доверии сливаются с помощью оператора суммарного слияния (**Опред.2.7**).

В этом примере Миша и Тома предлагают свои достаточно надёжные рекомендации о Тиме, и поэтому первое вычисленное доверие Маши к Тиме возрастает после того, как она обращается к Томе с просьбой о второй рекомендации относительно Тимы.

Таблица 2.5 – Пример слияния доверия к стоматологу в ситуации, изображённой на рисунке 2.19

		Входные мнения:				Промежуточные мнения:		Вычисленное мнение:
Параметры:		ω_B^A	ω_E^B	ω_C^A	ω_E^C	$\omega_E^{[A;B]}$	$\omega_E^{[A;C]}$	$\omega_X^{[A;B]\diamond[A;C]}$
Вера/убеждённость:	b	0.40	0.90	0.50	0.80	0.630	0.600	0.743
Неверие:	d	0.10	0.00	0.00	0.10	0.000	0.075	0.048
Неопределённость:	u	0.50	0.10	0.50	0.10	0.370	0.325	0.209
Априорная вероятность:	a	0.60	0.40	0.50	0.40	0.400	0.400	0.400
Прогнозируемая вероятность:	P	0.70	0.94	0.75	0.84	0.778	0.730	0.826

На рисунке 2.21 представлен пример слияния доверия на основе данных, представленных в таблице 2.5.

Следует отметить, что рисунок 2.21 показывает ту же самую сеть доверия, что и на рисунке 2.19, но в котором треугольник мнения для каждого вектора размещён на векторе. Входные аргументы представлены как четыре треугольника мнений в верхней части рисунка, а вычисленное мнение о доверии представлено как треугольник мнения в нижней части рисунка.

В рассмотренном примере слияния доверия используются совместно операторы понижения и слияния доверия. Путём объединения слияния и понижения доверия, можно моделировать и анализировать сложные сети доверия.

2.12.7 Переоценка доверия

2.12.7.1 Причины переоценки доверия

В случае слияния доверия, когда несколько источников предоставляют крайне противоречивые мнения, что может указывать на то, что один или оба источника ненадёжны, появляется

«усложняющий» элемент. Следовательно, в такой ситуации необходима стратегия преодоления противоречия. При этом сама выбранная стратегия должна соответствовать конкретной ситуации.

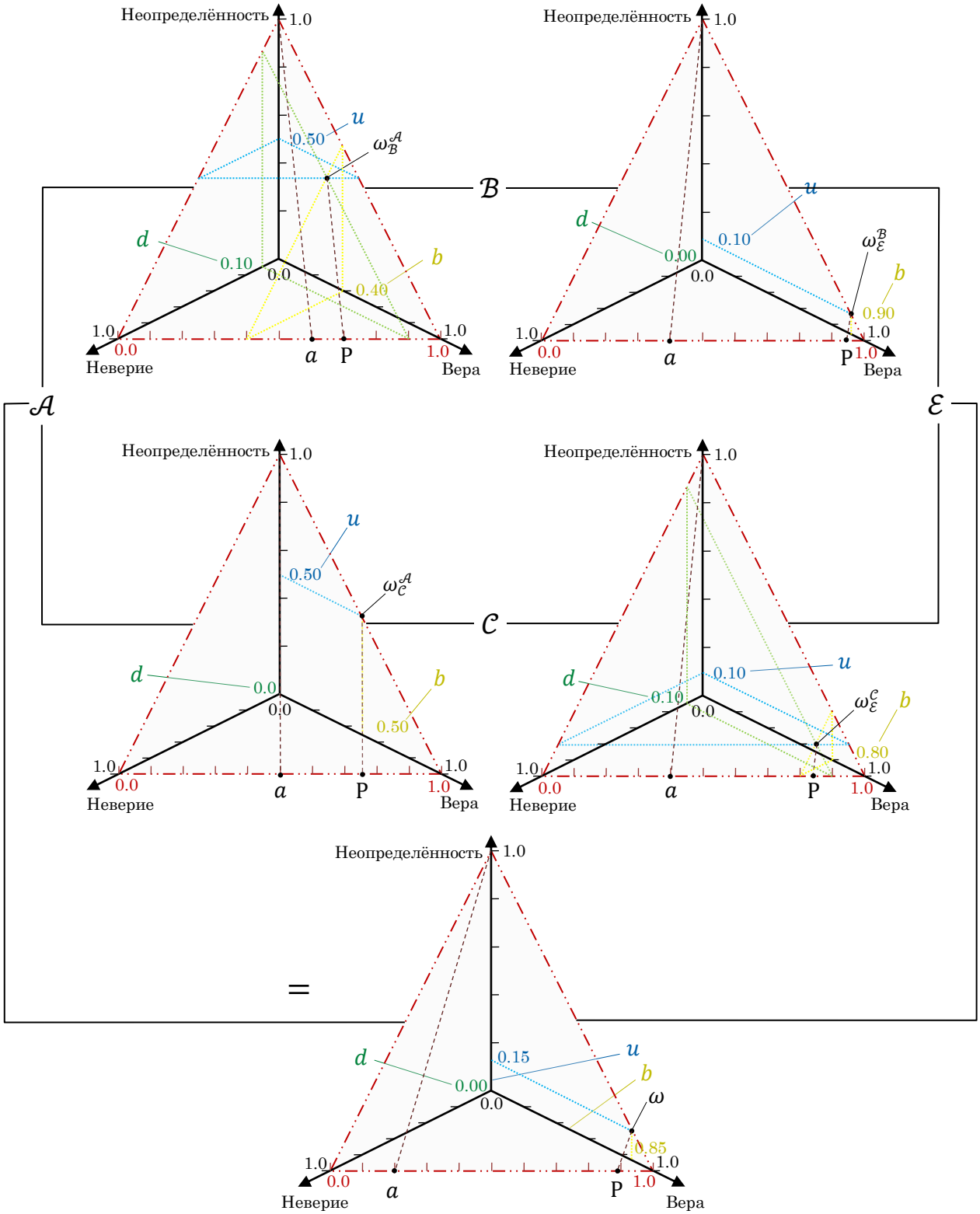

Рисунок 2.21 – Пример слияния доверия на основе данных, представленных в таблице 2.5

Упрощённая стратегия слияния противоречивых мнений состоит в том, чтобы рассматривать мнения о смешанном доверии как статичные, и не пересматривать доверие вообще. В такой стратегии доверяющей стороне необходимо только определить наиболее приемлемый оператор слияния для анализируемой ситуации (см. §2.12.6).

Например, если суммарное слияние приемлемо, тогда простая модель позволяет вычислить мнение субъекта $\mathcal{A}$ о переменной X в соответствие с правилом суммарного слияния доверия (2.24), а именно:

$$\omega_X^{(A;B)\diamond(A;C)} = \left(\omega_B^{\mathcal{A}} \otimes \omega_X^{\mathcal{B}}\right) \oplus \left(\omega_C^{\mathcal{A}} \otimes \omega_X^{\mathcal{C}}\right). \tag{2.26}$$

Таким образом, слияние весьма противоречивых мнений может быть вполне приемлемым, например, в случае коротких выборок процессов, когда различные типы событий могут наблюдаться в разные периоды времени.

Однако, бывают ситуации, когда простое слияние может быть неадекватным, и когда понадобилась бы переоценка одного или нескольких входных аргументов с целью вычисления мнения относительно доверия. Например, может быть ситуация, когда мнения $\omega_X^{\mathcal{B}}$ и $\omega_X^{\mathcal{C}}$ весьма противоречивы с точки зрения их распределений прогнозируемой вероятности относительно переменной X.

Предположим, что субъекты $\mathcal{A}$ и $\mathcal{B}$ наблюдали за одним и тем же параметром процесса или событием, возможно в одно и то же время, но по-прежнему выражают разные мнения, тогда становится очевидным, что один из них или оба являются ненадёжными, т.е. целесообразно провести переоценку (повторную оценку) доверия.

Или другая ситуация, при которой необходимо переоценить доверие, – это когда доверяющая сторона $\mathcal{A}$ узнает, что реальная правда о X радикально отличается от полученных мнений субъектов (данных источников). Следовательно, у аналитика есть веские причины не доверять субъекту (источнику), который выражает совершенно противоположное мнение (предоставляет совершенно иные данные).

Наличие высокой степени противоречия указывает на то, что один или несколько субъектов (источников) могут быть ненадёжными, тогда для получения максимально надёжного убеждения относительно целевого объекта стратегия должна быть направлена на уменьшение влияния ненадёжных субъектов (источников).

Снижение влияния ненадёжных субъектов (источников), как правило, предусматривает использования некоторой формы переоценки доверия, т.е. доверие аналитика к некоторым субъектам (источникам) может быть снижено, если доверие рассматривать как функцию степени противоречия их мнений [90].

2.12.7.2 Метод переоценки доверия

Переоценка доверия основана на определении степени противоречия между мнениями, которая вычисляется с помощью операторов понижения доверия к двум различным маршрутам. Причина в том, что противоречие указывает на ненадёжность одного или обоих источников, поэтому рекомендуемое доверие к субъектам (источникам) следует повторно оценивать в зависимости от степени противоречия.

Степень противоречия (*degree of conflict*, DC) – оценка различия между мнениями, которая может использоваться в стратегиях для решения проблем, связанных с различием мнений об одном и том же целевом объекте.

Пусть субъект $\mathcal{A}$ имеет собственные мнения о рекомендуемом доверии к субъектам (источникам) $\mathcal{B}$ и $\mathcal{C}$ $\omega_X^{[\mathcal{A};\mathcal{B}]}$ и $\omega_X^{[\mathcal{A};\mathcal{C}]}$ относительно одной и той же переменной X. Основной параметр измерения противоречия между мнениями $\omega_X^{[\mathcal{A};\mathcal{B}]}$ и $\omega_X^{[\mathcal{A};\mathcal{C}]}$ – расстояние между прогнозируемыми вероятностями (*projected probability distance*, PD), которое определяется следующим равенством:

$$\mathrm{PD}(\omega_X^{[\mathcal{A};\mathcal{B}]}, \omega_X^{[\mathcal{A};\mathcal{C}]}) = \frac{\sum_{x\in\mathbb{X}}\left|\mathbf{P}_X^{[\mathcal{A};\mathcal{B}]}(x) - \mathbf{P}_X^{[\mathcal{A};\mathcal{C}]}(x)\right|}{2} . \tag{2.27}$$

Свойство, что $\mathrm{PD} \in [0,1]$, можно объяснить следующим образом. Очевидно, что $\mathrm{PD} \geq 0$. Более того, учитывая, что $\sum \mathbf{P}_X^{[\mathcal{A};\mathcal{B}]}(x) + \sum \mathbf{P}_X^{[\mathcal{A};\mathcal{C}]}(x) = 2$, независимо от мощности $\mathbb{X}$, можно заметить, что $\mathrm{PD} \leq 1$. В случае, если $\mathrm{PD} = 0$, то распределения прогнозируемой вероятности равны, что отражает не противоречивость мнений (но возможно различных). В случае, если $\mathrm{PD} = 1$, то имеют место абсолютные мнения с различными прогнозируемыми вероятностями.

Большое значение PD не обязательно указывает на противоречие, так как потенциальное противоречие уменьшается, если одно или оба мнения имеют высокую степень неопределённости. Чем более неопределённым является одно или оба мнения, тем более «терпимо» следует относиться к большому значению PD.

Толерантность к большому значению PD, в случае высокой степени неопределённости, отражает тот факт, что неопределённые мнения имеют небольшое значение в возможной процедуре слияния.

Естественная мера общей достоверности между двумя мнениями $\omega_X^{[\mathcal{A};\mathcal{B}]}$ и $\omega_X^{[\mathcal{A};\mathcal{C}]}$ – их *конъюнктивная достоверность* (*conjunctive certainty*, CC):

$$\mathrm{CC}(\omega_X^{[\mathcal{A};\mathcal{B}]}, \omega_X^{[\mathcal{A};\mathcal{C}]}) = (1 - u_X^{[\mathcal{A};\mathcal{B}]})(1 - u_X^{[\mathcal{A};\mathcal{C}]}) . \tag{2.28}$$

Следует отметить, $\mathrm{CC} \in [0,1]$. Если $\mathrm{CC} = 0$, то одно или оба мнения бессмысленны, а если $\mathrm{CC} = 1$, то оба мнения категоричны, т.е. имеют множество неопределённости равное нулю.

Степень противоречия определяется просто как произведение PD и CC:

$$\mathrm{DC} = \mathrm{PD} \cdot \mathrm{CC}\,. \tag{2.29}$$

Определение 2.12 (степень противоречия). Предположим, что субъект $\mathcal{A}$ имеет собственные мнения о рекомендуемом доверии к субъектам (источникам) $\mathcal{B}$ и $\mathcal{C}$ $\omega_X^{[\mathcal{A};\mathcal{B}]}$ и $\omega_X^{[\mathcal{A};\mathcal{C}]}$ относительно одной и той же переменной X. Тогда, степень противоречия между мнениями $\omega_X^{[\mathcal{A};\mathcal{B}]}$ и $\omega_X^{[\mathcal{A};\mathcal{C}]}$ обозначается как $\mathrm{DC}(\omega_X^{[\mathcal{A};\mathcal{B}]}, \omega_X^{[\mathcal{A};\mathcal{C}]})$ и равно:

$$\mathrm{DC}(\omega_X^{[\mathcal{A};\mathcal{B}]}, \omega_X^{[\mathcal{A};\mathcal{C}]}) = \mathrm{PD}(\omega_X^{[\mathcal{A};\mathcal{B}]}, \omega_X^{[\mathcal{A};\mathcal{C}]}) \cdot \mathrm{CC}(\omega_X^{[\mathcal{A};\mathcal{B}]}, \omega_X^{[\mathcal{A};\mathcal{C}]})\,. \tag{2.30}$$

□

Знание степени противоречия – это только один из параметров, определяющих масштаб переоценки мнений о рекомендуемом доверии $\omega_{\mathcal{B}}^{\mathcal{A}}$ и $\omega_{\mathcal{C}}^{\mathcal{A}}$. Вполне естественно, что масштаб переоценки доверия также определяется относительной степенью неопределённости мнений о рекомендуемом доверии, и поэтому наиболее неопределённое мнение подвергается наибольшей переоценке. Основная причина этому состоит в том, что если аналитик имеет неопределённое рекомендуемое доверие к другому субъекту, то уровень доверия может легко измениться.

Различие неопределённости (*uncertainty differential*, UD) – оценка относительной неопределённости между двумя мнениями о рекомендуемом доверии. Существует одно UD для каждого мнения относительно другого.

$$\text{Раличия неопределённости: } \begin{cases} \mathrm{UD}\left(\omega_{\mathcal{B}}^{\mathcal{A}} | \omega_{\mathcal{C}}^{\mathcal{A}}\right) = \frac{u_{\mathcal{B}}^{\mathcal{A}}}{u_{\mathcal{B}}^{\mathcal{A}} + u_{\mathcal{C}}^{\mathcal{A}}} \\ \mathrm{UD}\left(\omega_{\mathcal{C}}^{\mathcal{A}} | \omega_{\mathcal{B}}^{\mathcal{A}}\right) = \frac{u_{\mathcal{C}}^{\mathcal{A}}}{u_{\mathcal{B}}^{\mathcal{A}} + u_{\mathcal{C}}^{\mathcal{A}}} \end{cases}. \tag{2.31}$$

Очевидно, что $\mathrm{UD} \in [0,1]$, если $\mathrm{UD} = 0.5$, то оба мнения о рекомендуемом доверии имеют одинаковую неопределённость, и более того, они должны быть подвергнуты равной переоценке. Если $\mathrm{UD} = 1$, то первое мнение о рекомендуемом доверии значительно более неопределённое, чем второе, и более того, оно должно быть подвергнуто полной переоценке. Если $\mathrm{UD} = 0$, то второе мнение о рекомендуемом доверии значительно более неопределённое, чем первое, и более того, оно должно быть подвергнуто полной переоценке.

Таким образом, параметры UD определяют относительную долю переоценки доверия для каждого мнения о рекомендуемом доверии. Масштаб переоценки доверия определяется *показателем (причиной) переоценки* (*revision factor*, RF), который представляет собой произведение DC и UD:

$$\text{Показатели переоценки: } \begin{cases} \mathrm{RF}\left(\omega_B^{\mathcal{A}}\right) = \mathrm{UD}\left(\omega_B^{\mathcal{A}} | \omega_C^{\mathcal{A}}\right) \cdot \mathrm{DC}\left(\omega_X^{[\mathcal{A};B]}, \omega_X^{[\mathcal{A};C]}\right), \\ \mathrm{RF}\left(\omega_C^{\mathcal{A}}\right) = \mathrm{UD}\left(\omega_C^{\mathcal{A}} | \omega_B^{\mathcal{A}}\right) \cdot \mathrm{DC}\left(\omega_X^{[\mathcal{A};B]}, \omega_X^{[\mathcal{A};C]}\right). \end{cases} \tag{2.32}$$

Переоценка доверия состоит в изменении мнения о рекомендуемом доверии путём увеличения множества недоверия за счёт множества доверия и множества неопределённости. Идея заключается в том, что субъектам (источникам), признанным ненадёжными, следует доверять меньше. Субъекту (источнику), который оказался совершенно ненадёжным, вообще нельзя доверять.

Если рассмотреть треугольник мнения, то переоценка доверия приведёт к смещению точки (мнения) ближе к углу недоверия (рисунок 2.22).

С учётом входного мнения о рекомендуемом доверии $\omega_B^{\mathcal{A}} = (b_B^{\mathcal{A}}, d_B^{\mathcal{A}}, u_B^{\mathcal{A}}, a_B^{\mathcal{A}})$ повторно оценённое мнение о рекомендуемом доверии, обозначаемое как $\breve{\omega}_B^{\mathcal{A}}$, вычисляется следующим образом:

$$\breve{\omega}_B^{\mathcal{A}}: \begin{cases} \breve{b}_B^{\mathcal{A}} = b_B^{\mathcal{A}} - b_B^{\mathcal{A}} \cdot \mathrm{RF}\left(\omega_B^{\mathcal{A}}\right), \\ \breve{d}_B^{\mathcal{A}} = \breve{d}_B^{\mathcal{A}} + \left(1 - \breve{d}_B^{\mathcal{A}}\right) \cdot \mathrm{RF}\left(\omega_B^{\mathcal{A}}\right), \\ \breve{u}_B^{\mathcal{A}} = u_B^{\mathcal{A}} - u_B^{\mathcal{A}} \cdot \mathrm{RF}\left(\omega_B^{\mathcal{A}}\right), \\ \breve{a}_B^{\mathcal{A}} = a_B^{\mathcal{A}} \ . \end{cases} \tag{2.33}$$

Аналогично, с учётом входного мнения о рекомендуемом доверии $\omega_C^{\mathcal{A}} = (b_C^{\mathcal{A}}, d_C^{\mathcal{A}}, u_C^{\mathcal{A}}, a_C^{\mathcal{A}})$ повторно оценённое мнение о рекомендуемом доверии, обозначаемое как $\breve{\omega}_C^{\mathcal{A}}$, вычисляется следующим образом:

$$\breve{\omega}_C^{\mathcal{A}}: \begin{cases} \breve{b}_C^{\mathcal{A}} = b_C^{\mathcal{A}} - b_C^{\mathcal{A}} \cdot \mathrm{RF}\left(\omega_C^{\mathcal{A}}\right), \\ \breve{d}_C^{\mathcal{A}} = \breve{d}_C^{\mathcal{A}} + \left(1 - \breve{d}_C^{\mathcal{A}}\right) \cdot \mathrm{RF}\left(\omega_C^{\mathcal{A}}\right), \\ \breve{u}_C^{\mathcal{A}} = u_C^{\mathcal{A}} - u_C^{\mathcal{A}} \cdot \mathrm{RF}\left(\omega_C^{\mathcal{A}}\right), \\ \breve{a}_C^{\mathcal{A}} = a_C^{\mathcal{A}} \ . \end{cases} \tag{2.34}$$

На рисунке 2.22 показан результат переоценки доверия для $\omega_B^{\mathcal{A}}$, который указывает на смещение мнения о рекомендуемом доверии к углу недоверия.

После того, как была проведена переоценка доверия и получены повторно оценённые мнения $\breve{\omega}_B^{\mathcal{A}}$ и $\breve{\omega}_C^{\mathcal{A}}$, можно повторить вычисление слияния доверия в соответствии с равенством (2.26) с учётом уменьшения противоречия. Тогда слияние усреднённых и повторно оценённых мнений о доверии можно определить с помощью следующего равенства:

$$\omega_X^{(A;B)\underline{\diamond}(A;C)} = \left(\omega_B^{\mathcal{A}} \otimes \omega_X^{\mathcal{B}}\right) \underline{\oplus} \left(\omega_C^{\mathcal{A}} \otimes \omega_X^{\mathcal{C}}\right). \tag{2.35}$$

Переоценка доверия предлагает стратегию для урегулирования ситуаций, в которых потенциально ненадёжные субъекты (источники) выражают противоречивые мнения, предположительно потому, что один или оба из них выражают мнения, являющиеся неверными или значительно отличающимися от реальной ситуации. Основываясь на степени противоречия и априорной неопределённости мнений о рекомендуемом доверии, переоценка доверия определяет меру, в соответствие с которой мнения о рекомендуемом доверии должны рассматриваться как ненадёжные, и поэтому должны быть повторно оценены с целью уменьшения влияния на вычисленное путём слияния убеждение (веру). Эта процедура даёт более консервативные результаты, которые учитывают, что источники информации (субъекты, предоставляющие информацию) могут быть ненадёжными.

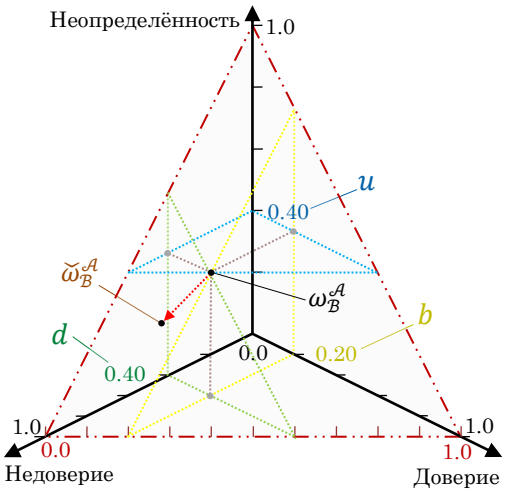

Рисунок 2.22 – Результат переоценки мнения $\omega_B^{\mathcal{A}}$ о рекомендуемом доверии – $\breve{\omega}_B^{\mathcal{A}}$

2.12.7.3 Пример: противоречие рекомендаций о ЦС

Продолжим рассматривать пример из §2.12.4.3 о рекомендуемом ЦС «Луч». Но теперь предположим, что Маша поселилась в городском отеле, а её соседка по номеру Тома, которая также приехала в длительную командировку в ту же самую организацию, сообщила ей, что она уже была в ЦС «Луч» и осталась недовольна уровнем обслуживания клиентов.

Предположим, что Маша разговаривала с Томой несколько раз и считает её высокопрофессиональной сотрудницей, и поэтому у неё, с интуитивной точки зрения, сформировалось относительно высокое доверие к Томе. Таким образом, Маша получила вторую рекомендацию относительно ЦС «Луч». Это даёт ей основание для (является причиной) переоценки её начального доверия к Мише, которое возможно будет преобразовано в недоверие к нему, и которое могло бы вызвать изменение её первоначального убеждения относительно ЦС «Луч».

Это пример можно представить в численном выражении, в котором мнения $\omega_{\mathcal{B}}^{\mathcal{A}}$, $\omega_{X}^{\mathcal{B}}$, $\omega_{\mathcal{C}}^{\mathcal{A}}$ и $\omega_{X}^{\mathcal{C}}$ являются аргументами.

Вначале рассмотрим результат слияния доверия без переоценки доверия, когда вычисленной мнение $\omega_{X}^{[\mathcal{A};\mathcal{B}]\diamond[\mathcal{A};\mathcal{C}]}$ будет определяться как простое слияние доверия:

$$\omega_{X}^{[\mathcal{A};\mathcal{B}]\diamond[\mathcal{A};\mathcal{C}]} = \left(\omega_{\mathcal{B}}^{\mathcal{A}} \otimes \omega_{X}^{\mathcal{B}}\right) \oplus \left(\omega_{\mathcal{C}}^{\mathcal{A}} \otimes \omega_{X}^{\mathcal{C}}\right). \quad (2.36)$$

Будем считать, что X – двоичная переменная, т.е. мнения ω_X – двоичные мнения. Мнения-аргументы и вычисленное мнение представлены в таблице 2.6.

Применение процедуры слияния доверия в ситуации, когда Маша получает рекомендации от Миши и Томы, даёт вычисленное мнение с прогнозируемой вероятностью $\mathrm{P}_{X}^{\mathcal{A}} = 0{,}465$, т.е. вероятность того, что ЦС «Луч» – надёжный, и вероятность того, что ЦС «Луч» – не надёжный, примерно равны. Этот результат кажется нелогичным. Хотя прогнозируемые вероятности $\mathrm{P}_{\mathcal{B}}^{\mathcal{A}} = 0{,}90$ и $\mathrm{P}_{\mathcal{C}}^{\mathcal{A}} = 0{,}99$ достаточно близки, убеждённость Маши в рекомендуемое доверие к Томе равно $b_{\mathcal{C}}^{\mathcal{A}} = 0{,}90$, что намного больше, чем её убеждённость в рекомендуемое доверие к Мише равно $b_{\mathcal{B}}^{\mathcal{A}} = 0{,}00$. Поэтому, казалось бы, вполне логичным присвоить рекомендации Томы значительно больший вес, но в случае простого слияния доверия, как показано в таблице 2.6, это не так.

Таблица 2.6 – Простое слияния доверия при условии противоречивых рекомендаций о ЦС «Луч»

Параметры:		Входные мнения: $\omega_{\mathcal{B}}^{\mathcal{A}}$	$\omega_{X}^{\mathcal{B}}$	$\omega_{\mathcal{C}}^{\mathcal{A}}$	$\omega_{X}^{\mathcal{C}}$	Промежуточные мнения: $\omega_{X}^{[\mathcal{A};\mathcal{B}]}$	$\omega_{X}^{[\mathcal{A};\mathcal{C}]}$	Вычисленное мнение: $\omega_{X}^{[\mathcal{A};\mathcal{B}]\diamond[\mathcal{A};\mathcal{C}]}$
Вера/убеждённость:	b	0.00	0.95	0.90	0.10	0.855	0.099	0.452
Неверие:	d	0.00	0.00	0.00	0.80	0.000	0.792	0.482
Неопределённость:	u	1.00	0.05	0.10	0.10	0.145	0.109	0.066
Априорная вероятность:	a	0.90	0.20	0.90	0.20	0.200	0.200	0.200
Прогнозируемая вероятность:	P	0.90	0.96	0.99	0.12	0.884	0.121	0.465

В такой ситуации, с интуитивной точки зрения, естественной реакцией Маши была бы переоценка своё рекомендуемого доверия к Мише, потому что его рекомендация противоречит рекомендации Томы, которой она доверяет с большей уверенностью, то есть множество веры/убеждённости больше. Естественно, что Маша не будет доверять Мише, так как очевидно – его рекомендация ненадёжна. В результате такой переоценки доверия, рекомендация Томы получит больший вес (значимость).

Применение метода переоценки доверия (§2.12.6.2) позволяет вычислить следующие промежуточные значения:

$$\text{Противоречие:}\begin{cases}\text{PD}\left(\omega_X^{[\mathcal{A};\mathcal{B}]},\omega_X^{[\mathcal{A};\mathcal{C}]}\right)=0.763\,,\\ \text{CC}\left(\omega_X^{[\mathcal{A};\mathcal{B}]},\omega_X^{[\mathcal{A};\mathcal{C}]}\right)=0.762\,,\\ \text{DC}\left(\omega_X^{[\mathcal{A};\mathcal{B}]},\omega_X^{[\mathcal{A};\mathcal{C}]}\right)=0.581\,.\end{cases} \tag{2.37}$$

$$\text{Переоценка:}\begin{cases}\text{UD}\left(\omega_{\mathcal{B}}^{\mathcal{A}}|\omega_{\mathcal{C}}^{\mathcal{A}}\right)=0.909\,,\\ \text{UD}\left(\omega_{\mathcal{C}}^{\mathcal{A}}|\omega_{\mathcal{B}}^{\mathcal{A}}\right)=0.091\,,\\ \text{RF}\left(\omega_{\mathcal{B}}^{\mathcal{A}}\right)=0.529\,,\\ \text{RF}\left(\omega_{\mathcal{C}}^{\mathcal{A}}\right)=0.053\,.\end{cases} \tag{2.38}$$

Эти промежуточные значения (равенства 2.37 и 2.38) определяют мнения $\breve{\omega}_X^{[\mathcal{A};\mathcal{B}]}$ и $\breve{\omega}_X^{[\mathcal{A};\mathcal{C}]}$ о рекомендуемом и повторно оценённом доверии (таблица 2.7.). В таблице 2.7 представлен результат применения слияния доверия на основе мнений о рекомендуемом и повторно оценённом доверии.

Следует отметить, что повторно оценённое рекомендуемое доверие Маши к Мише существенно снизилось, а вот рекомендуемое доверие к Томе практически осталось без изменений. Это отражает вполне естественную реакцию, когда мы находимся в аналогичной ситуации.

Таблица 2.7 – Переоценка доверия при условии противоречивых рекомендаций о ЦС «Луч»

		Входные мнения:				Промежуточные мнения:		Вычисленное мнение:
Параметры:		$\breve{\omega}_{\mathcal{B}}^{\mathcal{A}}$	$\omega_X^{\mathcal{B}}$	$\breve{\omega}_{\mathcal{C}}^{\mathcal{A}}$	$\omega_X^{\mathcal{C}}$	$\breve{\omega}_X^{[\mathcal{A};\mathcal{B}]}$	$\breve{\omega}_X^{[\mathcal{A};\mathcal{C}]}$	$\breve{\omega}_X^{[\mathcal{A};\mathcal{B}]\diamond[\mathcal{A};\mathcal{C}]}$
Вера/убеждённость:	b	0.00	0.95	0.85	0.10	0.403	0.094	0.180
Неверие:	d	0.53	0.00	0.05	0.80	0.000	0.750	0.679
Неопределённость:	u	0.47	0.05	0.10	0.10	0.597	0.156	0.141
Априорная вероятность:	a	0.90	0.20	0.90	0.20	0.200	0.200	0.200
Прогнозируемая вероятность:	P	0.42	0.96	0.94	0.12	0.522	0.125	0.208

Переоценку доверия следует рассматривать как специализированный метод, поскольку в природе не существует параллельных процессов, которые можно было бы объективно наблюдать и анализировать. Выбор конструкции, отражающей интуитивное человеческое мнение (взгляд), существенно влияет на определение причин переоценки RF. Могут быть разные варианты конструкций определения причин переоценки, которые наилучшим образом отражают человеческую интуицию, и которые могут также давать надёжные результаты с точки зрения конкретных критериев.

Выводы по Главе 2

1. Первая часть данной главы посвящена анализу взаимосвязи концепций «доверие» и «безопасность» в ИТС. Эта тема лежит в стыке двух научных направлений теории распределённых вычислений и ИБ. Было проанализировано доверие в условиях ограниченных знаний в области психологии и поведенческой науки.

Рассмотрены основные направления и результаты научных исследований в этой области. Сделан вывод о том, что появление нового научного направления – субъективной логики (СЛ) – послужило прорывом в исследовании доверия в ИТС и, что очень важно, обеспечении ИБ. СЛ – математический аппарат синтеза и анализа систем доверия.

Для описания человеческих качеств использованы характеристики честный, нечестный, надёжный и ненадёжный, которые послужили для определения двух важных словосочетаний честный/надёжный или благонадёжный, и нечестный/ненадёжный или злонамеренный. Именно эти два понятия используются в дальнейшем анализе систем доверия. Показано, что доверие – позитивная концепция (понятие). Оно означает, что мы ожидаем что-нибудь позитивное от надёжного субъекта, или другими словами, мы ожидаем от него, что он будет обладать желаемым нами свойством или вести себя так, как мы этого хотим. Под доверием понимается степень, с которой один субъект готов зависеть от чего-то или кого-то в конкретной ситуации, ощущая при этом относительную безопасность, даже если возможны и негативные последствия. Очевидно, что это определение включает в себя основные составляющие доверия, а именно: *(1)* зависимость от доверенной стороны, *(2)* надёжность доверенной стороны и *(3)* риск в случае, если доверенная сторона не функционирует так, как предполагалось. Смысл этого определения заключается в том, что требования к обеспечению доверия напрямую коррелируют с влиянием риска.

С другой стороны, показано, что доверие, затрагивающее безопасность ИТС, отражает её сопротивляемость (резистивность) по отношению к злонамеренным угрозам.

2. Во второй части данной главы проанализированы концептуальные понятия «доверенная сторона», «доверяющая сторона» и «преступное намерение». В работе определены два класса «доверенных сторон» – «мыслящий субъект» и «логический объект». При этом первым типом доверия называется доверие к мыслящему субъекту (человек, организация), которое представляет собой веру в то (убеждённость в том), что он будет вести себя без злого умысла. А вторым типом доверия называется доверие к логическому объекту (алгоритм, протокол, комплекс технических средств и т.п.), которое представляет собой веру в то (убеждённость/уверенность в том), что он будет противодействовать вредоносным манипуляциям мыслящего субъекта.

Показано, что причина доверия сложна и очень часто основана на неопределяемых объёмах исходной информации, и что она требует от мыслящего субъекта способности доверять.

Кроме того, показано, что только мыслящие субъекты способны сформировать доверие, и что такое доверие имеет смысл только для человека.

Представлен обзор основных типов доверительных взаимосвязей с точки зрения участвующих субъектов (сторон). Доверие в ИТС предусматривает участие трёх сторон: мыслящего доверяющего субъекта, логического доверенного объекта и мыслящего внешнего угрожающего (злонамеренного) субъекта. Впервые показаны новые структурные модели доверительных взаимосвязей: в первой – злонамеренный мыслящий субъект манипулирует доверенным логическим объектом, а мыслящий доверяющий субъект доверяет такому логическому мошенническому объекту (модель взаимодействия с поддельным (мошенническим) *Web*-сайтом); во второй – мыслящий доверяющий субъект управляет доверенным логическим объектом, и одновременно с этим злонамеренный субъект узурпировал (захватил) управление и манипулирует логическим объектом (модель компьютерного шпионажа).

Далее проанализирована концепция «преступное намерение», которое означает злонамеренность, т.е. сочетание нечестности и ненадёжности. То, что конкретно представляет собой злонамеренное поведение, никогда не может быть абсолютным, а может быть определено только на основе политики безопасности, морально-этических норм, контрактов/договоров и законодательства.

3. В третьей части данной главы проанализированы многообразие и взаимозависимость доверия. Далее показано, что доверие можно рассматривать как знания о защищённости (безопасности). В жизни существует иррациональное доверие, которое не основано на знаниях, а основано, например, на вероисповедании, и иногда может продолжать существовать «назло» знаниям. Такой тип доверия может быть весьма полезен во многих ситуациях, но, с точки зрения обеспечения ИБ, он может быть чрезвычайно опасным. Поэтому единственным типом доверия в распределённых ИТС должно быть, насколько это возможно, доверие, основанное на знаниях. Другими словами, доверие отражает знания пользователя о защищённости (безопасности) ИТС. Безопасность отражает идеалистическую сторону, т.е. какой бы мы хотели видеть ИТС с теоретической точки зрения. С другой стороны, доверие отражает реальную сторону ИТС, так как ошибки при разработке ИТС всегда будут иметь место, несмотря на строгое соблюдение всех процедур проектирования и внедрения.

Далее представлен анализ доверия с точки зрения стратегической игры. Анализируя СОИБ ИТС, можно смоделировать угрозу, при которой возможный злонамеренный субъект с целью повышения уровня доверия к нему со стороны других субъектов будет «вести» себя корректно в течение определённого периода времени, а затем внезапно проведёт ложную кредитную транзакцию, предусматривающую привлечение большого объёма финансовых средств, и впо-

следствии исчезнет из сети (это напоминает способ атак типа «маскарад»). Этот пример показывает, что доверием можно манипулировать, а кто в конце концов станет победителем может зависеть от того, кто «умнее». Очевидно, что доверяющий и доверенный субъекты могут оказаться в бесконечном цикле с обратной связью, что напоминает стратегическую игру.

В работе проведено сравнение защищённости (безопасности) и надёжности. Показано, что оба эти понятия вписываются в более общее понятие «функциональная надёжность или благонадёжность».

Далее представлен анализ двух проблем. Во-первых, можно ли рассматривать отсутствие доверия из-за неполных знаний или невежества как энтропию информации, а во-вторых, можно ли моделировать доверие как вероятность. Если используется понятие «энтропия» с целью анализа доверия, то энтропия должна пониматься в более широком смысле, а не только в смысле статистического понятия по Шеннону. В работе рассмотрен пример, который показывает, что доверие не обязательно транзитивно, тогда как вероятность транзитивна. Указанный пример не говорит о том, что теория вероятности не может использоваться при моделировании доверия, он просто говорит о том, что её нельзя применять напрямую и в общем смысле. Её применение возможно, если ввести некоторые ограничения на такое применение. Например, использовать теорию вероятностей только в случае оценки доверия к логическим объектам, когда влияние взаимосвязей между доверяющим субъектом и угрожающей стороной можно проигнорировать.

4. В четвёртой части данной главы рассматривается концепция доверия в ИТС на основе математического аппарата субъективной логики (методы и средства синтеза и анализа систем доверия). Общая идея СЛ заключается в расширении вероятностной логики до формализованного подхода (формализма) за счёт прямого дополнения, т.е. включения (1) неопределённости вероятностей и (2) выразителя субъективной веры (убеждённости).

Аргументы в СЛ называются субъективными мнениями (или просто мнениями). При этом, мнение может содержать множество неопределённости в смысле неопределённости вероятностей. Кроме того, в СЛ рассматриваются два вида мнений: статистическое, которое основано на анализе многократно повторяющихся событий (их результатов/исходов), и эпистемологическое, которое основано на анализе неповторяющихся (одиночных) событий (их результатов/исходов). Модель субъективного мнения расширяет классическую модель функции веры/убеждённости в том смысле, что мнения учитывают априорные вероятности, а функции убеждённости их игнорируют. И в этой связи, преимущество СЛ относительно классической теории вероятностей и двоичной логики состоит в том, что СЛ позволяет получить точное выражение неопределённости и неоднозначности, и поэтому реальные ситуации могут быть смоделированы и проанализированы более точно по сравнению с классическими вероятностными моделями.

Далее в работе рассматриваются основные элементы СЛ. Даны определения области и гипербласти анализа, двоичного и m-ичного мнений. Представлен анализ субъективных мнений, которые отражают веру/убеждённость в истинность предположений в условиях неопределённости, а также могут указывать на выразителя (субъекта) мнения, когда это необходимо. Описаны три основных класса мнений, при этом каждый класс мнений может быть разделён на четыре подкласса в соответствии с уровнями достоверности. Даны выражения для прогнозируемой вероятности и дисперсии мнений, а также представлено новое трёхмерное отображение субъективного мнения, вместо известного двухмерного барицентрического отображения.

Особое место в работе отведено анализу доверия в ИТС, т.е. направленной взаимосвязи между двумя субъектами (взаимодействующими сторонами), которых можно назвать доверяющей и доверенной сторонами. Показано, что доверие имеет две основные интерпретации: доверие к надёжности и доверие при принятии решения. Даны определения этих двух типов доверия, а также представлен их анализ. Также показано, что особенность зависимости доверия заключается в появлении риска, который является функцией возможного ущерба, возникающего в результате возможной неспособности субъекта оправдать оказываемое ему доверие. Вместе с тем, мнения о доверии – это двоичные мнения, так как выражаются относительно двоичных переменных, которые естественно могут принимать только два значения.

В работе проведено сравнение репутации и доверия. Дано определение репутации и показано, что репутацию можно рассматривать как коллективную оценку благонадёжности (в смысле надёжности), основанную на рекомендациях или рейтингах членов сообщества. Субъективное доверие человека может быть получено путём объединения полученных рекомендаций и личного опыта. Такое объединение может быть проведено с помощью оператора суммарного слияния, определение и аналитическое выражение которого даны в работе.

Далее в работе проанализирована транзитивность доверия. Рассмотрены понятия рекомендуемого и функционального доверия. Представлены семантические требования (критерии) транзитивности доверия. Описаны операторы понижения, слияния и переоценки доверия. Для каждого из операторов рассмотрены причины его практического применения, а также пример его конкретного использования и вычисления, на его основе, итогового мнения о доверии.

Глава 3 ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ

3.1 Переход к электронному документообороту

Проблема определения точного соответствия между бумажным (БДО) и электронным документооборотом (ЭДО) была известна достаточно давно. Ещё в 80-х годах XX века велась научная дискуссия по этой проблеме. Основные реализационные и правовые различия между БДО и ЭДО стали очевидными только в 90-годах прошлого века. *Бумажный документ* с собственноручной подписью имеет свойственные ему атрибуты защиты, позволяющие обнаружить любую подделку или искажение бумажного документа: типографская краска, наносимая на целлулоидные волокна бумаги, уникальность процедуры печати (например, фирменный бланк), водяные знаки, биометрические свойства подписи (форма и стиль подписи, нажим на ручку), метки времени [10].

В *электронном документе* таких атрибутов нет. *Электронное сообщение* – последовательность двоичных чисел (единиц и нулей), которые кодируют информацию в определённом формате. При случайном выборе криптографических ключей единицы и нули в сообщении носят случайный характер, так как зависят не только от содержания сообщения и алгоритма электронной подписи (ЭП), но и от ключей. По аналогии с бумажными, электронные документы можно модифицировать, если не использовать специальные средства физической и электронной защиты, обеспечивающие необходимый уровень доверия.

Электронные и бумажные документы способны выполнять абсолютно разные функции в юриспруденции и бизнесе. Такие документы различаются между собой, прежде всего, средой доставки, которая сохраняет их уникальность и подлинность. Вместе с тем, электронные сообщения не являются уникальными, возможно сделать любое количество дубликатов (копий), ничем не отличающихся от оригинала. Данное свойство электронных документов вступает в прямое противоречие со свойством бумажных документов, которые специально защищают от копирования. Значит, специфические различия между бумажными и электронными документами требуют различных способов, средств и процедур обработки для достижения необходимых юридических и коммерческих свойств, и обеспечения правомочных функций. Другими словами, в реальной жизни БДО невозможно полностью отобразить в ЭДО. Тем не менее, это не исключает дальнейшего поиска реальных функциональных аналогов, учитывая уникальные свойства передачи дискретных сообщений.

Исторически, процедуры предоставления услуг, приобретения и доставки товаров основывались на бумажных технологиях (БДО). Однако, глобальная информатизация (в частности создание всемирной Интернет-сети) позволила «*перевести*» указанные процедуры в ИТС, реализующие ЭДО («*на электронные рельсы*»), а ИОК способна их ускорить и упростить. Такие

«*электронные коммерческие системы и системы предоставления услуг*» зависят от целостности и подлинности данных. Эти оба свойства данных могут быть реализованы ИОК на основе привязки ЭП к автору ЭП (физическому лицу, гражданину) и обеспечения гарантий того, что ЭП не может быть подделана (сфальсифицирована). Также, физическое лицо (субъект) может подписать данные с помощью ЭП, а получатель может проверить источник данных, и что данные не были модифицированы без знания автора ЭП. Кроме того, ИОК-технология может обеспечить шифрование данных, чтобы гарантировать их конфиденциальность. Другими словами, система управления криптографической защитой в ИТС может основываться на (инфраструктуре) открытых ключах.

Как и все аспекты информационных технологий, внедрение ИОК, как основы системы управления криптографической защитой в ИТС организаций различных форм собственности, требует тщательного планирования и всестороннего понимания её связи с другими ИТС, использующих системы управления криптографической защитой на основе (инфраструктуры) открытых ключей.

3.2 Услуги по обеспечению безопасности

Практически каждая организация или ведомство рассматривает Интернет-сеть как средство предоставления услуг, коммерческой деятельности и снижения расходов. Государственные органы исполнительной власти Российской Федерации находятся, кроме всего прочего, под «дополнительным прессом» при предоставлении услуг гражданам с использованием Интернет-сети, связанным с удовлетворением требований законодательных и нормативных правовых актов, например, требований по защите персональных данных [91].

При предоставлении услуг и проведении коммерческих транзакций (электронных процедур) должны быть реализованы, как минимум, следующие четыре основные услуги (службы) обеспечения безопасности [92]:

- *обеспечение целостности* (*integrity*) [93];
- *обеспечение конфиденциальности* (*confidentiality*) [94];
- *идентификация и аутентификация* (*identification and authentication*) [95];
- *обеспечение неотказуемости* (*non-repudiation*) [96].

Услуги по (службы) обеспечению(я) *целостности данных* позволяют защитить данные от их неавторизованной или случайной модификации. Такая модификация включает вставку, перестановку, удаление и замену данных. Для обеспечения гарантий целостности данных, система должна быть способна обнаруживать *неавторизованную модификацию данных*. Цель – получатель данных может их проверить, что они не были изменены.

Услуги по (службы) обеспечению(я) *конфиденциальности* ограничивают доступ к содержанию уязвимых данных только теми пользователями, которым предоставлено право просмотра данных. Меры по обеспечению конфиденциальности предотвращают несанкционированное *раскрытие информации* неавторизованными пользователями или процессами.

Услуги по (службы) *идентификации и аутентификации* обеспечивают подтверждение подлинности передачи, сообщения и его источника. Цель – получатель данных определяет их источник и убеждается в его подлинности.

Услуги по (службы) обеспечению(я) *неотказуемости* предотвращают попытку пользователя отказаться от участия в предшествующих действиях (транзакциях). Цель – гарантировать, что получатель данных уверен в надёжности отправителя.

3.3 Инфраструктура обеспечения безопасности

Чтобы воспользоваться широким диапазоном служб обеспечения ИБ, *взаимодействующим субъектам* ($\mathcal{A}$ и $\mathcal{B}$) потребуется использовать несколько классов криптографических способов обеспечения безопасности одновременно. Соответственно, для обеспечения конфиденциальности им понадобится распределять симметричные ключи для зашифрования (расшифрования). Распределение симметричных ключей может быть осуществлено тремя способами:

1. непосредственно между взаимодействующими субъектами с использованием симметричного шифрования;

2. с использованием симметричного шифрования и привлечением ДТС;

3. с использованием системы обеспечения ключами на основе открытых ключей и привлечением ДТС.

Для небольших корпоративных ИТС вполне приемлем первый способ. Если субъект $\mathcal{A}$ устанавливает соединения только с тремя или четырьмя субъектами (пользователями ИТС), то он может провести предварительную *процедуру инициализации* с каждым из них. При расширении корпоративной ИТС это решение – неприемлемо. Что будет, если субъект $\mathcal{A}$ попытается установить соединения с десятком субъектов (пользователей ИТС). В такой ситуации для исключения предварительной процедуры инициализации субъекту $\mathcal{A}$ понадобится ДТС. Второй способ приемлем для широкомасштабных ИТС, но он способен обеспечить только ограниченную поддержку аутентификации и не способен обеспечить неотказуемость.

Для широкомасштабных ИТС также приемлем третий способ, и кроме того он обеспечивает комплексное и всестороннее решение. Если ДТС «*привязывает*» ($bind$) открытый ключ к пользователю или системе (то есть, заверяет *параметр подлинности* (ПП) взаимодействующей стороны, обладающей соответствующим открытым ключом), то можно реализовать весь

диапазон услуг по обеспечению ИБ. Пользователь может подтвердить целостность, аутентифицироваться и обеспечить неотказуемость, используя ЭП. Симметричные ключи могут быть распределены, либо с помощью системы доставки ключей, либо с помощью системы согласования ключей [46,49].

Конечно, зона действия одной ДТС тоже должна расширяться на значительное расстояние. Для предоставления услуг по обеспечению ИБ за пределами автономных ИТС организаций может потребоваться несколько ДТС, которые должны быть связаны между собой. Такая совокупность взаимосвязанных ДТС образует *инфраструктуру обеспечения безопасности* (или инфраструктуру безопасности, *security infrastructure*), на которую могут полагаться пользователи, если ими будут востребованы услуги обеспечения ИБ. Если такая инфраструктура безопасности предназначена для распределения открытых ключей, то её называют *инфраструктурой открытых ключей*. В настоящее время, ИОК является основой системы управления криптографической защитой.

3.4 Организация и компоненты ИОК

ИОК привязывает открытые ключи к субъектам, позволяет другим субъектам проверять привязки открытых ключей и предоставляет услуги, которые необходимы при проведении соответствующих процедур обеспечения ключами в распределённой ИТС.

Наиболее общими целями современных архитектур безопасности являются защита и распределение информации, востребованной в широкомасштабных и глобальных ИТС (например, Интернет-сеть), в которых пользователи, ресурсы и их владельцы могут находиться в самых разных местах (с географической точки зрения) и в разное время. Для удовлетворения потребностей по обеспечению ИБ необходимо использование наращиваемых и распределённых ИОК. Последние позволяют управлять криптографической защитой данных, вести электронный бизнес и предоставлять услуги с уверенностью в том, что:

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

При информационном обмене в рамках стандартного электронного бизнеса покупатели и продавцы полагаются на кредитные и дебетовые карты при решении всех финансовых проблем электронных сделок. Продавец может аутентифицировать покупателя путём сравнения подписи или путём проведения идентификации, например, с помощью паспорта. Продавец полагается на информацию, хранящуюся в кредитной или дебетовой карте, и информацию о состоянии счёта,

полученную от организации, выпустившей кредитную или дебетовую карту, с целью обеспечения гарантий последующего поступления платежа. Аналогично, покупатель осуществляет электронную сделку, заведомо зная, что он может заблокировать платёж (платёжную операцию), если продавец «провалит» поставку товаров или услуг. В данном виде электронной сделки организация, выпустившая кредитную или дебетовую карту, выступает в роли ДТС.

Такая модель «*покупатель-бизнес*» (*consumer-to-business*) очень часто используется в электронной коммерции, и даже в тех случаях, когда покупатель и организация, выпустившая кредитную или дебетовую карту, никогда не встречались. Аналогичная модель «*пользователь-ведомство*» также использует аутентификацию и обеспечение целостности при предоставлении электронных услуг.

При ведении электронного бизнеса или предоставлении электронных услуг покупатель/потребитель и провайдер/ведомство могут находиться друг от друга на расстоянии в тысячи километров. Кредитная или дебетовая карта покупателя и финансовая информация или персональные данные потребителя услуг должны быть защищены при передаче их через Интернет-сеть, и поэтому необходимы иные формы аутентификации. Другими словами, участники коммерческих сделок и клиенты ИТС, предоставляющих услуги через Интернет-сеть, обязаны использовать методы шифрования, позволяющие защитить данные при информационном взаимодействии. Кроме того, они должны быть способны получать криптоключи и соответствующие гарантии, что противоположная сторона информационного обмена легитимна. ИОК предоставляет услуги, которые основаны на способах, позволяющих решить такие задачи.

Инфраструктура открытых ключей представляет собой совокупность программного обеспечения (ПО), технологий шифрования и служб, которые способны в интересах организаций обеспечить защиту линий и каналов связи и электронных коммерческих сделок, осуществляемых с использованием сетей передачи данных. ИОК объединяет цифровые СЕРТ, криптографию с открытыми ключами и центры сертификации в единую сетевую архитектуру безопасности в интересах большого количества ИТС организаций (ведомств). *Типовая ИОК* организации или ведомства включает:

a) выпуск цифровых $СЕРТ_{ОК}$ для индивидуальных пользователей и прикладных серверов ИТС;

b) зарегистрированное ПО оконечного пользователя;

c) интеграцию с каталогами $СЕРТ_{ОК}$;

d) средства обслуживания, восстановления и аннулирования $СЕРТ_{ОК}$;

e) соответствующие службы и системы технологической поддержки.

Термин инфраструктура открытых ключей является производным от криптографии с открытыми ключами. *Криптография с открытыми ключами* представляет собой технологию,

являющуюся основой современных способов формирования ЭП. Она обладает уникальными свойствами, которые делают её «*бесценной*» в качестве основы реализации функций по обеспечению безопасности в распределённых ИТС.

3.4.1 Компоненты ИОК

Функциональными элементами ИОК являются (рисунок 3.1):

- центры сертификации[22] (ЦС);
- центры (пункты) регистрации (ЦР);
- репозитарии;
- архивы.

Пользователи ИОК выступают в двух ипостасях: как держатели (владельцы) СЕРТ, и как взаимодействующие стороны. *Центры атрибутных*[23] СЕРТ ($СЕРТ_{АТ}$) являются дополнительными компонентами ИОК.

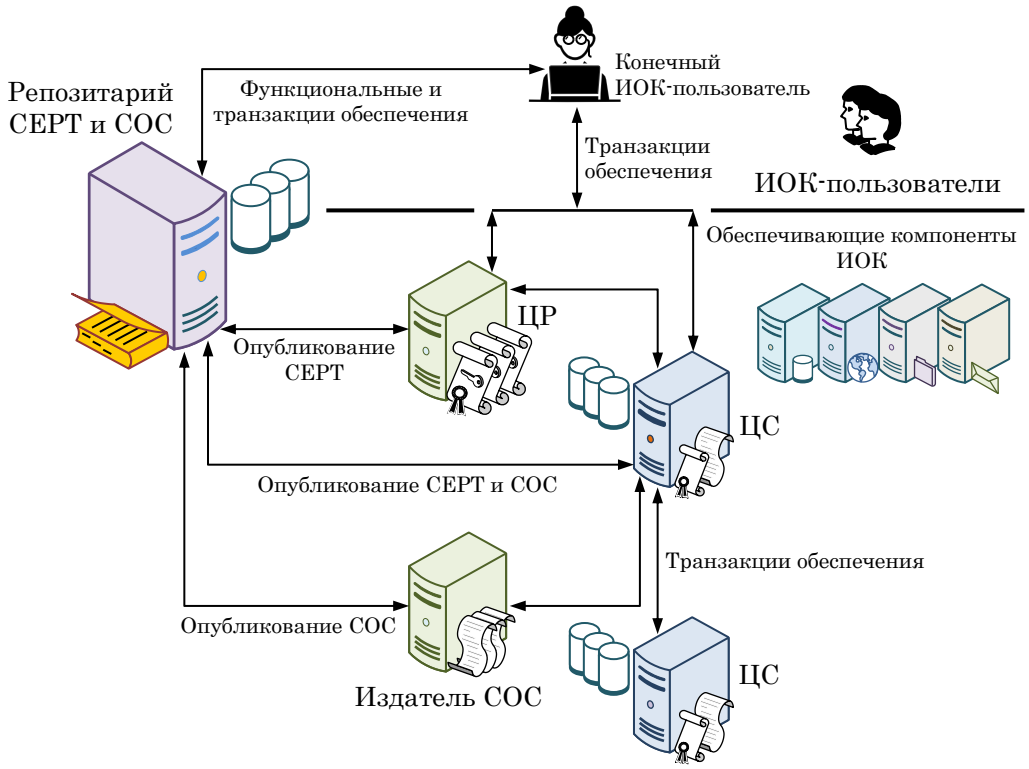

Рисунок 3.1 – Компоненты ИОК

Центры сертификации (*certification authority*). ЦС подобен нотариусу. ЦС подтверждает параметры подлинности взаимодействующих сторон при передаче и приёме электронных

[22] В Российской Федерации они получили наименование *удостоверяющих центров*, так как последние представляют собой объединение центров сертификации и регистрации.
[23] Атрибут – информационный объект, который включает два компонента (поля): наименование параметра/признака и значение этого параметра/признака, например, ФИО: Иванов Пётр Сергеевич.

платежей или при осуществлении иных процедур электронной коммерции. Аутентификация является необходимым элементом многих стандартных процедур установления соединений между взаимодействующими сторонами, включая электронные платёжные процедуры.

Центр (пункт) регистрации (*registration authority*) является доверенным субъектом ЦС для регистрации или подтверждения параметров подлинности клиентов, пользующихся услугами этого ЦС.

Репозитарий (*repository*) представляет собой базу данных (БД), в которой хранятся действующие цифровые СЕРТ системы ЦС. *Главная задача* репозитария – предоставлять данные, которые позволят его пользователям, получившим подписанные ЭП сообщения, согласовать (установить) состояние (статус) цифровых СЕРТ физических лиц и организаций. Такие получатели сообщений именуются как взаимодействующие стороны. ЦС посылают сертификаты и *списки отозванных сертификатов* (СОС, *certificate revocation list* – CRL) в репозитарии.

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, является ли ЭП на «устаревшем» документе заслуживающей доверия.

ЦС выпускает (издаёт) *сертификат открытого ключа*, содержащий ПП, который включает соответствующие зарегистрированные (учётные, персональные) данные владельца $СЕРТ_{ОК}$. Цифровой $СЕРТ_{ОК}$ обычно включает открытый ключ, информацию о ПП взаимодействующей стороны, обладающей закрытым ключом, период действия $СЕРТ_{ОК}$ и собственную ЭП ЦС. Кроме этого, $СЕРТ_{ОК}$ может содержать и другую информацию о взаимодействующей стороне, обладающей правом подписи, или информацию о рекомендуемом порядке использовании открытого ключа. Пользователем, подписывающим электронные сообщения, может быть физическое лицо или организация, которые взаимодействуют с ЦС с целью получения цифрового $СЕРТ_{ОК}$ для проверки ПП в подписанных с помощью ЭП электронных сообщениях.

Вместе с тем, ЦС должны выпускать и обрабатывать СОС, которые представляют собой перечни $СЕРТ_{ОК}$, которые были аннулированы (отозваны). Перечень обычно подписывается тем же самым субъектом, который выпустил $СЕРТ_{ОК}$. $СЕРТ_{ОК}$ могут быть аннулированы, если, например, закрытый ключ владельца $СЕРТ_{ОК}$ был утерян; владелец покинул компанию или ведомство; владелец поменял имя. Кроме того, СОС может задокументировать исторический статус удалённых $СЕРТ_{ОК}$. Другими словами, датированная ЭП может быть проверена на предмет её правомерности (и подлинности), если дата самого подписания (формирования и проставления подписи) относится к периоду действия $СЕРТ_{ОК}$, а текущий СОС, выпущенный ЦС в этот момент времени, не показывал $СЕРТ_{ОК}$ как аннулированный.

Пользователи ИОК (*ИОК-пользователи*) представляют собой организации или физические лица, которые пользуются услугами ИОК, но не выпускают СЕРТ$_{ОК}$. Они относятся к другим компонентам ИОК, которые получают СЕРТ$_{ОК}$ и проверяют СЕРТ$_{ОК}$ других субъектов, с которыми они осуществляют электронные коммерческие сделки или которые предоставляют электронные услуги. К оконечным объектам относятся:

– *взаимодействующая сторона*, которая полностью доверяет СЕРТ$_{ОК}$, содержащему открытый ключ противоположной стороны;

– *держатель (владелец)* СЕРТ$_{ОК}$, который получил СЕРТ$_{ОК}$ и может подписывать электронные цифровые документы.

Следует заметить, что в различных прикладных ИТС физическое лицо или организация могут быть одновременно, и взаимодействующей стороны, и владельцем СЕРТ$_{ОК}$.

3.4.1.1 Центры сертификации

ЦС – это основной «строительный блок» ИОК. ЦС – это комплекс технических средств, специализированного ПО и персонала, эксплуатирующего и обслуживающего ЦС. ЦС обозначается с помощью двух атрибутов: своего имени и своего открытого ключа. ЦС выполняет четыре основные ИОК:

1. выпускает (издаёт) СЕРТ$_{ОК}$ (т.е., формирует их, а затем их подписывает);
2. поддерживает в актуальном состоянии информацию о статусе СЕРТ$_{ОК}$ и выпускает СОС;
3. публикует свои действующие (например, не просроченные) СЕРТ$_{ОК}$ и СОС, причём таким образом, чтобы пользователи могли получать информацию, которая необходима им для реализации услуг по обеспечению ИБ;
4. обслуживает архивы данных о состоянии СЕРТ$_{ОК}$ с просроченным сроком действия, которые этот ЦС выпустил.

Иногда эти требования трудно удовлетворить одновременно. Для выполнения этих требований ЦС может делегировать часть своих функций другим компонентам инфраструктуры.

ЦС могут выпускать СЕРТ$_{ОК}$, либо только для пользователей, либо только для других ЦС, либо те и другие совместно. Когда ЦС выпускает СЕРТ$_{ОК}$, он доказывает, что субъект (владелец сертификата, указанный в нём) имеет закрытый ключ, которому соответствует открытый ключ, содержащийся в СЕРТ$_{ОК}$. Если ЦС включает в СЕРТ$_{ОК}$ дополнительную информацию, то ЦС доказывает, что эта информация также затрагивает субъекта. Такая дополнительная информация может быть контактной информацией (например, адрес электронной почты) или информацией, указывающей на политику обеспечения безопасности (например, типы ИТС, в которых может

использоваться открытый ключ). Когда владельцем $\text{СЕРТ}_{\text{ОК}}$ является другой ЦС, ЦС, выпустивший сертификат, доказывает, что сертификаты, выпускаемые другим ЦС (владельцем сертификата), заслуживают доверия.

ЦС помещает в каждый сформированный им $\text{СЕРТ}_{\text{ОК}}$ (и СОС) своё наименование, а также подписывает их с помощью своего закрытого ключа. После того, как пользователи установят, что они доверяют некоторому ЦС (непосредственно или на основе маршрута сертификации), они могут доверять $\text{СЕРТ}_{\text{ОК}}$, выданным этим ЦС. Пользователи могут легко проверить сертификаты, выданные этим ЦС, путём сравнения его наименования. Для обеспечения гарантий того, что $\text{СЕРТ}_{\text{ОК}}$ является подлинным, они проверяют подпись, используя для этого открытый ключ ЦС. Таким образом, и это очень важно, ЦС обеспечивает адекватную защиту своего закрытого ключа.

3.4.1.2 Центры (пункты) регистрации

ЦР предназначен для проверки содержания $\text{СЕРТ}_{\text{ОК}}$, выпускаемого ЦС. Содержание сертификата может отражать информацию, которая относится к объекту, запросившему $\text{СЕРТ}_{\text{ОК}}$, например, паспорт, социальную карту или другие удостоверяющие личность документы. Кроме того, они могут отражать информацию, предоставляемую ДТС. Например, лимит кредита, указанный в кредитной карте, отражает информацию, которая была получена из бюро кредитных историй. Сертификат может отражать данные кадрового департамента компании или письмо официального представителя компании. Например, $\text{СЕРТ}_{\text{ОК}}$ субъекта $\mathcal{A}$ ($\text{СЕРТ}_{\text{ОК}}^{\mathcal{A}}$) мог бы указывать на то, что он обладает правом подписи небольших контрактов. ЦР обобщает такие входные данные и предоставляет совокупную информацию в ЦС.

Как и ЦС, ЦР представляет собой объединение ПАК и обслуживающего его персонала. Но в отличие от ЦС, ЦР будет обслуживаться, вероятнее всего, одним человеком. Каждый ЦС будет вести список аккредитованных ЦР, т.е. список заслуживающих доверие ЦР. ЦР известен ЦС по его имени и открытому ключу. С помощью проверки подписи ЦР в сообщении ЦС может удостовериться в том, что именно аккредитованный ЦР предоставил ему информацию, а последняя является надёжной. В итоге, и это очень важно, что ЦР обеспечивает адекватную защиту своего собственного закрытого ключа.

3.4.1.3 Репозитарии ИОК

Все ИТС, пользующиеся услугами ИОК, в значительной степени зависят от глобальной *Службы единого каталога* (СЕК, *The Directory* [97,98]), предназначенной для распределения $\text{СЕРТ}_{\text{ОК}}$ и информации о состоянии $\text{СЕРТ}_{\text{ОК}}$. СЕК предоставляет средства для хранения и распределения $\text{СЕРТ}_{\text{ОК}}$ и их обновления. Услуги СЕК являются типовыми услугами, определёнными стандартом X.500, или подмножеством таких услуг.

Стандарт ITU-T X.500 включает серию рекомендаций и технические требования, и кроме того содержит ряд ссылок на несколько стандартов ISO. Он был разработан с целью описания услуг (служб) СЕК, которые могли бы функционировать, невзирая на системные, корпоративные и международные границы. Совокупность разработанных протоколов определяет функциональные процедуры информационного взаимодействия серверов (*server-to-server*), например, формирования маршрутов («*цепочек*») доверия (*chaining*), дублирования (*shadowing*) и перенаправление (*referral*), а также вводит *протокол доступа к СЕК* (*Directory Access Protocol* – DAP) для связи между клиентом и сервером (*client to server*). Немного позже, в качестве альтернативы DAP-протоколу, был разработан протокол упрощённого доступа к СЕК (*Lightweight Directory Access Protocol* – LDAP [99]). Большинство СЕК-серверов и их клиентов используют LDAP-протокол, и не все из них поддерживают DAP-протокол.

Чтобы СЕК-серверы были «*привлекательны*» для ИТС, пользующихся услугами ИОК, они должны быть функционально совместимыми. Без такой совместимости проверяющая сторона информационного взаимодействия не сможет получить необходимые сертификаты и СОС от удалённых источников с целью проверки подписей.

3.4.1.4 Архивы

Архив «несёт» ответственность за долговременное хранение архивных данных от имени ЦС. Архив декларирует, что информация на момент её получения была подлинной и не была модифицирована в период её хранения. Информация, предоставленная ЦС на хранение, должна быть достаточной, чтобы определить, был ли $СЕРТ_{ОК}$ действительно выдан тем ЦС, который указан в сертификате, и был ли $СЕРТ_{ОК}$ действующим на тот момент времени. Архив защищает такую информацию с помощью технических способов и соответствующих процедур в течение её хранения и обслуживания. Если позднее возникнет конфликтная ситуация (спор), то информация может быть использована для проверки того, что закрытый ключ, связанный с $СЕРТ_{ОК}$, использовался для подписания документа. Это позволяет проверить все подписи в старых документах (например, завещания) в более позднее время.

3.4.1.5 ИОК-пользователи

Пользователями ИОК являются организации (любой формы собственности) или физические лица, пользующиеся услугами ИОК, но не выпускающие $СЕРТ_{ОК}$. Они зависят от других компонентов ИОК, предоставляющих им $СЕРТ_{ОК}$ и проверяющих $СЕРТ_{ОК}$ других субъектов, с которыми они заключают интерактивные сделки (проводят электронные транзакции). К конечным субъектам относятся:

▪ *проверяющая сторона*, которая проверяет СЕРТ$_{ОК}$, чтобы с уверенностью знать открытый ключ противоположной стороны;

▪ *держатель сертификата*, который получил СЕРТ$_{ОК}$ и может подписать цифровой документ.

Следует заметить, что в различных прикладных системах физическое лицо или организация могут быть одновременно, и проверяющей стороной, и держателем СЕРТ$_{ОК}$.

3.5 Архитектуры открытых ключей

Держатели СЕРТ$_{ОК}$ получают свои сертификаты в различных ЦС, в зависимости от организации или сообщества, членами которых они являются. ИОК, как правило, состоит из нескольких ЦС, которые связаны между собой надёжными маршрутами доставки данных (информационного взаимодействия). Надёжный маршрут связывает проверяющую сторону с одной или несколькими ДТС, причём так, что проверяющая сторона может быть уверена в подлинности используемого СЕРТ$_{ОК}$. Получатели подписанного сообщения, которые не взаимодействуют с ЦС, выпустившим СЕРТ$_{ОК}$ для отправителя сообщения, могут также проверить подлинность СЕРТ$_{ОК}$ отправителя путём поиска маршрута между ЦС, обслуживающим получателя подписанного сообщения, и ЦС, который выдал СЕРТ$_{ОК}$ отправителю.

Существуют две общепринятые используемые в организациях ИОК, которые обеспечивают необходимое решение указанной проблемы:

- *иерархическая* ИОК организации;
- *сетевая* ИОК организации.

Дальнейшим развитием ИОК является стремление организаций к «*связыванию*» своих собственных ИОК с такими же ИОК своих бизнес-партнёров. Другими словами, формирование единой ИОК «снизу-вверх», т.е. от частных к общей.

3.5.1 Основные типы ИОК в организациях

ЦС могут связываться несколькими способами. Подавляющее большинство организаций, внедряющих и использующих свои собственные ИОК, выбирают «*сетевую*» или «*иерархическую*» архитектуру (рисунок 3.2) [10].

Иерархическая архитектура: ЦС «выстраиваются иерархически» под корневым ЦС, который выпускает СЕРТ$_{ОК}$ для «подчинённых» ЦС. Последние могут выпускать СЕРТ$_{ОК}$ для своих «подчинённых» ЦС или для пользователей. В иерархической ИОК-архитектуре каждая проверяющая сторона знает открытый ключ корневого ЦС. Любой СЕРТ$_{ОК}$ может быть проверен путём проверки маршрута сертификации, состоящего из СЕРТ$_{ОК}$, начиная с сертификата корневого ЦС.

Маша (рисунок 3.2,*а*) проверяет СЕРТ$_{ОК}$ Миши, выпущенный ЦС$_4$, затем – СЕРТ$_{ОК}$ ЦС$_4$, выпущенный ЦС$_2$, а затем – СЕРТ$_{ОК}$ ЦС$_2$, выданный ЦС$_1$ (т.е. корневым), открытый ключ которого она знает.

Сетевая: независимые ЦС взаимно сертифицируются каждый с каждым (т.е. выпускают и доставляют СЕРТ$_{ОК}$ друг другу), в результате чего формируется сеть доверенных связей между «*равноправными*» ЦС (*peers*). На рисунке 3.2,*б* представлена сеть ЦС. Проверяющая сторона знает открытый ключ «*ближайшего*» к ней ЦС, как правило, это тот ЦС, который выпустил для неё СЕРТ$_{ОК}$. Проверяющая сторона проверяет СЕРТ$_{ОК}$ путём проверки маршрута сертификации, который сформирован из сертификатов, начиная с СЕРТ$_{ОК}$ доверенного ЦС. ЦС проводят процедуры взаимной сертификации каждый с каждым, т.е. они издают СЕРТ$_{ОК}$ друг для друга, и объединяются в пары взаимной сертификации.

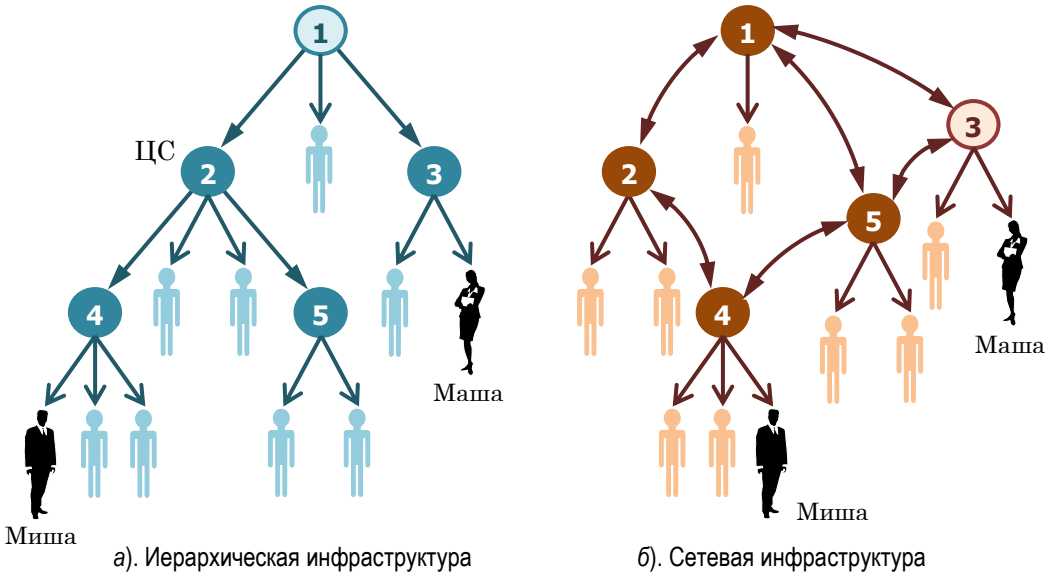

Рисунок 3.2 – Основные ИОК-архитектуры

Так, например, Маша знает открытый ключ ЦС$_3$, в то время как Миша знает открытый ключ ЦС$_4$. Существует несколько маршрутов сертификации, которые начинаются от Миши и заканчиваются у Маши. Кратчайший маршрут требует, чтобы Маша проверила СЕРТ$_{ОК}$ Миши, выданный ЦС$_4$, затем – СЕРТ$_{ОК}$ ЦС$_4$, выданный ЦС$_5$, и в заключении, – СЕРТ$_{ОК}$ ЦС$_5$, выданный ЦС$_3$. ЦС$_3$ является обслуживающим Машу ЦС, она доверяет ЦС$_3$ и знает его открытый ключ.

Существует множество способов реализации ИОК организации. Строго рекомендуется [16], чтобы основные компоненты ИОК располагались в разных системах, т.е. ЦС – в одной системе, ЦР – в другой системе, а СЕК-серверы – в других системах. Так как компоненты ИОК содержат уязвимые данные, они должны размещаться «позади» сетевых экранов организаций, обеспечивающих защиту от внешних атак из Интернет-сети.

Если некоторые организации желают получить доступ к СЕРТ$_{ОК}$ друг друга, то их СЕК-службы должны быть доступны друг другу и возможно другим организациям через Интернет-сеть. Однако, СЕК-сервер может содержать и другие данные, которые считаются уязвимыми, и поэтому информация СЕК-сервера может быть ещё более уязвима, если её сделать открытой для публичного доступа. Типовым решением могло бы стать создание каталога, который содержит только открытые ключи или СЕРТ$_{ОК}$, и размещение его на границе (периметре) организации. Такой каталог именуется как *граничный* СЕК-модуль *(border directory*). Наиболее вероятное размещение СЕК-модуля могло бы быть с внешней стороны сетевой экрана организации, а ещё лучше в защищённой *демилитаризованной зоне* сети организации так, что СЕК-модуль по-прежнему будет доступен для общего пользования, но будет более надёжно защищён от атак. На рисунке 3.3 представлен пример практической реализации ИОК организации.

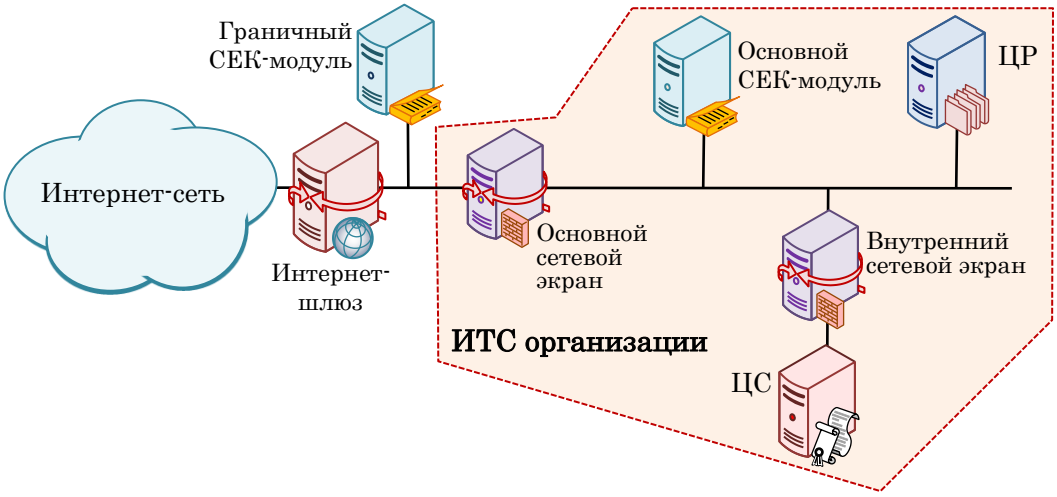

Рисунок 3.3 – Пример практической реализации ИОК на базе ИТС организации

3.5.2 Современные типы ИОК-архитектур

3.5.2.1 Строгая иерархия

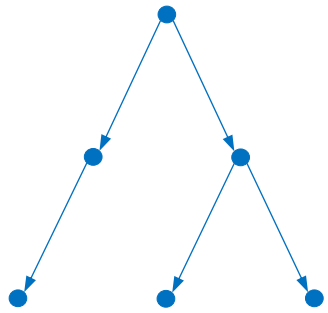

Рисунок 3.4 – Строгая иерархия

Большинство коммерческих ИОК имеют *строгую иерархию* (*strict hierarchy*), которая показана на рисунке 3.4 и, как правило, включает один или два уровня. Маршруты сертификации идут строго от верхнего корневого ЦС, как правило, через промежуточные ЦС, и далее вниз к пользователям, в которых считается, что пользователи сертифицированы дочерними ЦС.

В строгой иерархии все пользователи могут быть легко идентифицированы и найдены вследствие иерархической структуры. Пользователь обязан знать

открытый ключ верхнего корневого ЦС с целью определения цепочек сертификации и формирования маршрута сертификации до любого другого пользователя в иерархии.

3.5.2.2 Общая иерархия

Общая иерархия включает двунаправленную сертификацию между ЦС, как показано на рисунке 3.5. Когда сертификация двунаправленная, каждый пользователь будет нуждаться только в получении подлинной копии открытого ключа ближайшего ЦС, и при этом он по-прежнему способен сформировать маршрут сертификации до каждого другого пользователя в сети. Стандарт ITU-T X.509 [100] предлагает общую иерархию такого типа, но коммерческие ИОК такую топологию не используют.

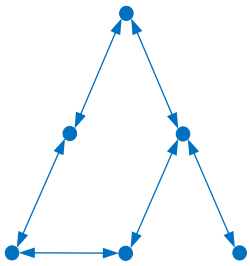

Рисунок 3.5 – Общая иерархия

3.5.2.3 Произвольная структура

Противоположной иерархической структуре является *произвольная структура* (*anarchic*), в которой каждый ЦС (и пользователь) может свободно выбрать другой ЦС (и пользователей) для собственной сертификации (рисунок 3.6).

На основе произвольной структуры функционирует *PGP*-инфраструктура открытых ключей [101…103]. Она состоит из однонаправленной и/или двунаправленной сертификации между произвольными субъектами. В принципе между пользователями и ЦС нет различий. Недостаток анархической сети сертификации по сравнению с иерархической структурой состоит в том, что нет простого алгоритма определения маршрутов сертификации между пользователями сети с произвольной структурой, тогда как в иерархических сетях такие алгоритмы существуют. Пользователь обязан иметь максимально много открытых ключей, чтобы сформировать цепочки сертификации до других пользователей.

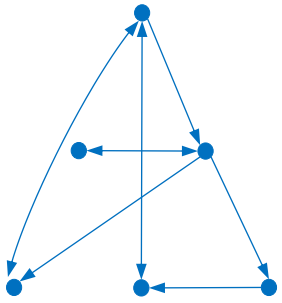

Рисунок 3.6 – Произвольная структура

3.5.2.4 Изолированные иерархии

Многие ИОК могут существовать параллельно без связи друг с другом (рисунок 3.7). Пользователь обязан получить открытый ключ корневого ЦС каждой ИОК с целью проверки сертификатов пользователей во всех иерархиях. Пользователи, входящие в иерархии, в которых корневой ЦС неизвестен, не могут быть идентифицированы.

ИОК, используемые в ГАИС «*World Wide Web*» Интернет-сети, включают *изолированные строгие иерархии*, и, фактически, относятся к этому типу топологии. Открытые ключи корневых ЦС хранятся в закодированном виде в наиболее популярных *Web*-обозревателях (например, КПО «*Microsoft Internet Explorer*» содержит несколько десятков ключей корневых ЦС, среди которых нет ни одного российского).

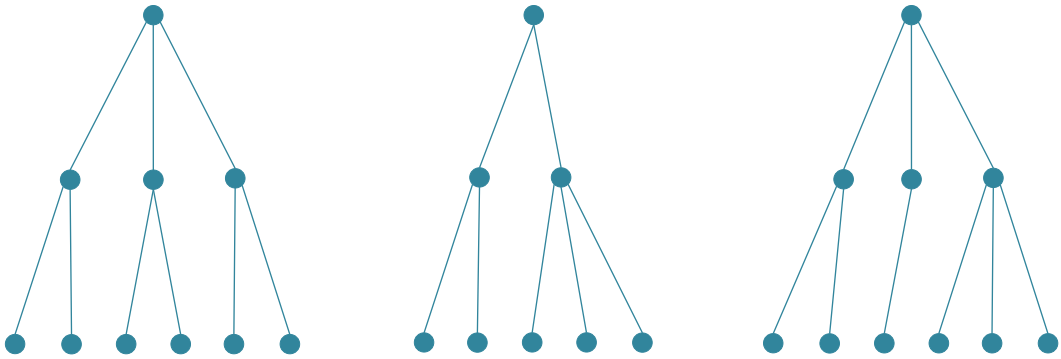

Рисунок 3.7 – Изолированные иерархии сертификации

3.5.2.5 Взаимно-сертифицированные иерархии

Чтобы избежать необходимость обладания пользователями нескольких открытых ключей, сами иерархии могут быть *взаимно сертифицированными* (рисунок 3.8). В случае строгой иерархии достаточно, чтобы пользователь получил подлинную копию открытого ключа своего корневого ЦС, и в то же время, пользователь будет способен сформировать маршрут сертификации до любого пользователя в любой иерархии.

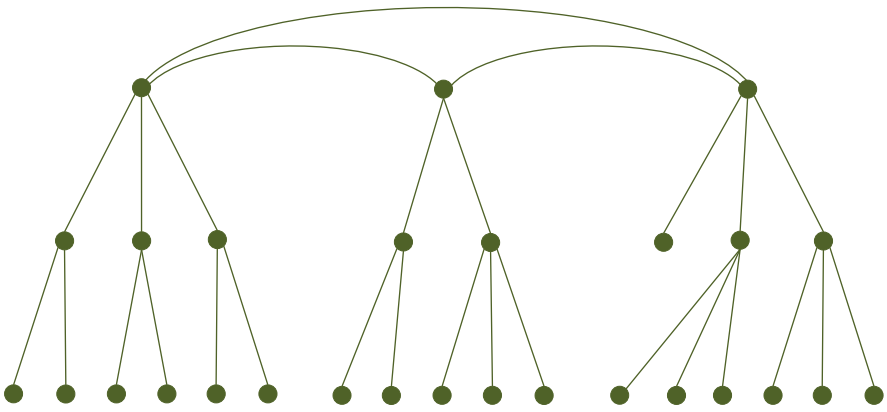

Рисунок 3.8 – Взаимно-сертифицированные иерархии

Взаимная сертификация между ИОК способна упростить распространение открытых ключей корневых ЦС, и сделает ИОК по-настоящему открытыми. *Основная проблема*, препятствующая такому развитию, заключается в том, что ЦС, как правило, имеют несовместимые политики сертификации, в то время как взаимная сертификация требует некоторой согласованности таких

политик. Например, государственные органы исполнительной власти могут применять общую политику и осуществлять взаимную сертификацию между всеми государственными ИОК, но самопроизвольная взаимная сертификация между коммерческими ИОК до сих пор не получила широкого распространения.

3.5.3 Форматы данных, используемые в ИОК

В ИОК используются два основных формата данных:

1. сертификат открытого ключа;
2. списки отозванных (аннулированных) сертификатов (СОС).

Третьим ИОК-форматом данных является $СЕРТ_{АТ}$, который может использоваться в качестве дополнительного сертификата [100].

3.5.3.1 Формат $СЕРТ_{ОК}$

Первая стандартизированная система сертификации была представлена в Рекомендации ITU-T X.509v1 [104], которая предназначена для обеспечения безопасности СЕК [105], а также для функционирования в иерархии ЦС.

Рекомендация X.509v1 в дальнейшем была доработана во второй и третьей версиях X.509v2 и X.509v3, которые исключили слабости первой версии. Более того, третья версия X.509v3 является основой для рабочей группы IETF PKIX (Интернет-сообщества), которая определила основные цели и задачи инфраструктуры открытых ключей для Интернет-сети [17]. Формат сертификатов X.509 представлен на рисунке 3.9.

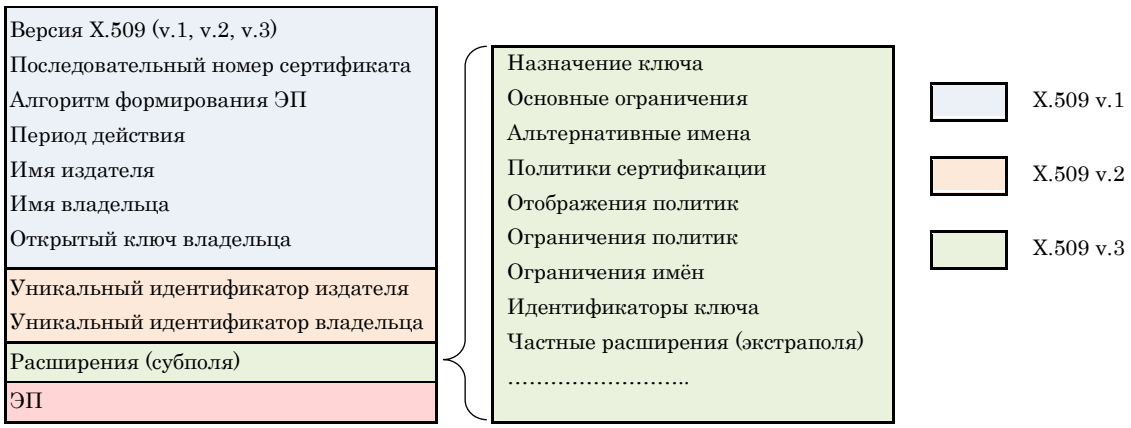

Рисунок 3.9 – Структура $СЕРТ_{ОК}$ с полями расширения

СЕК X.509 никогда не применялась Интернет-сообществом, так как она и соответствующий протокол доступа к СЕК (*Directory Access Protocol* – DAP, [106]) рассматривались как слишком сложные в использовании для простых клиентов Интернет-сети. Вместо него используется

протокол упрощённого доступа к СЕК (*Lightweight Directory Access Protocol* – LDAP, [99]), который считается относительно простым протоколом для поиска и обновления каталогов СЕК, основанные на Интернет-архитектуре.

Формат СЕРТ$_{ОК}$ стандарта X.509 «*превратился*» в адаптивное и «*мощное*» средство доставки самой разнообразной информации. Большая часть такой информации является дополнительной, и кроме этого содержание обязательных полей может варьироваться.

СЕРТ$_{ОК}$ защищён с помощью ЭП ЦС. Пользователи сертификатов знают, что содержание не было подделано с момента сформирования ЭП, если, конечно же, ЭП может быть проверена. СЕРТ$_{ОК}$ содержат набор общих полей, и могут включать дополнительный набор субполей под единым названием «*поле расширения*» (*extensions*).

Существуют десять общих полей, из которых шесть обязательных и четыре дополнительных. К обязательным полям относятся:

1. серийный (последовательный) номер;
2. идентификатор алгоритма формирования ЭП сертификата;
3. наименование издателя сертификата;
4. период действия сертификата;
5. открытый ключ;
6. наименование держателя (владельца) сертификата.

Держатель (владелец) СЕРТ$_{ОК}$ является взаимодействующей стороной, которая контролирует соответствующий закрытый ключ. К дополнительным полям относятся:

1. номер версии;
2. два уникальных идентификатора (УИД);
3. расширения (специализированные дополнительные субполя).

Эти дополнительные субполя используются только во второй, третьей и последующих версиях сертификатов.

Версия. Это поле определяет синтаксис СЕРТ$_{ОК}$. Если это поле не заполнено (пропущено), то СЕРТ$_{ОК}$ закодирован в соответствие с правилами кодирования первой версии. Сертификаты первой версии не включают УИД или субполей расширения. Если сертификат включает УИД, но без расширений, то в поле «Версия» указывается «2». Если же сертификат содержит субполя расширения, как правило, они присутствуют во всех современных СЕРТ$_{ОК}$, то в поле «Версия» указывается «3».

Последовательный номер. Это поле содержит целое число, которое назначается издателем каждому изданному СЕРТ$_{ОК}$. Последовательный номер должен быть уникальным для каждого СЕРТ$_{ОК}$. Сочетание имени издателя и последовательного номера позволяют однозначно идентифицировать СЕРТ$_{ОК}$.

Алгоритм вычисления ЭП. Это поле указывает на используемый алгоритм формирования ЭП, которая защищает $СЕРТ_{ОК}$.

ЦС, выпустивший сертификат. Это поле содержит уникальное наименование ЦС, сформировавшего $СЕРТ_{ОК}$.

Срок действия. Это поле содержит даты начала и окончания действия $СЕРТ_{ОК}$.

Держатель (владелец) сертификата. Это поле содержит уникальное имя владельца закрытого ключа, который соответствует открытому ключу, указанному в $СЕРТ_{ОК}$. Владельцем может быть ЦС, ЦР или конечный пользователь. Конечными пользователями могут физические лица (субъекты), программно-аппаратные комплексы или любые другие объекты, которые способны использовать закрытый ключ по предназначению.

Информация об открытом ключе владельца сертификата. Это поле содержит открытый ключ владельца $СЕРТ_{ОК}$, дополнительные параметры и идентификатор алгоритма. Открытый ключ в этом поле, совместно с дополнительными параметрами алгоритма, используется для проверки ЭП или для проведения некоторой процедуры, связанной с обеспечением ключами. Если держателем $СЕРТ_{ОК}$ является ЦС, то открытый ключ используется для проверки ЭП самого сертификата.

УИД ЦС, выпустившего сертификат, и УИД владельца сертификата. Эти поля содержат УИД, и применяются в $СЕРТ_{ОК}$ только второй или третьей версий. УИД владельца сертификата и издавшего его ЦС предназначены для регулирования многократного использования наименований субъектов или издателей сертификатов по прошествии длительного времени. Однако, этот способ, как выяснилось позже, является «плохим решением». В Интернет-стандартах [17] включение (использование) этих полей не рекомендовано.

Расширения. Это дополнительное поле применяется только в сертификатах третьей и последующих версиях. Если оно имеет место, то оно содержит одно или несколько субполей. Каждое субполе «Расширение» включает подполе «Идентификатор расширения», подполе «Флаг критичности» и подполе «Значение расширения». Общие расширения сертификата отвечают на вопросы, ответы на которые нельзя получить из общих полей.

Тип держателя (владельца) сертификата. Это субполе содержит указатель, является ли держателем сертификата ЦС или конечный пользователь (физическое лицо).

Информация об именах и параметрах подлинности. Это субполе помогает ответить на вопросы, связанные с параметром подлинности пользователя.

Атрибуты ключа. Это субполе описывает важные атрибуты, связанные с открытыми ключами, например, может ли ключ использоваться для доставки ключа или использоваться для проверки ЭП.

Данные о политике применения. Это субполе помогает пользователям определить, если СЕРТ$_{ОК}$ другого пользователя может быть надёжным, то предназначен ли он (СЕРТ$_{ОК}$) для большого числа транзакций, а также иные условия, которые зависят от корпоративной политики той или иной организации.

Субполя расширения сертификата позволяют ЦС включать информацию, которая не входит в основное содержание сертификата. Любая организация может установить частное субполе расширения с целью удовлетворения своих бизнес-требований. Тем не менее, значительное число требований могут быть удовлетворены за счёт использования стандартных субполей расширения. Стандартные субполя расширения широко используются в коммерческих целях. Субполя расширения позволяют наилучшим образом обеспечить функциональную совместимость, а также они значительно эффективнее, с точки зрения затрат, чем частные субполя расширения.

Каждое субполе расширения включает три подполя (компонента): «*идентификатор расширения*», «*флаг критичности*» и «*значение расширения*».

«*Идентификатор расширения*» указывает на формат и семантику субполя «значение расширения». «*Флаг критичности*» указывает на важность данного поля расширения. Когда это подполе содержит единицу, то содержащаяся в подполе «значение расширения» информация является неотъемлемой (обязательной) при использовании сертификата. Более того, если встретилось неизвестное критичное расширение, то СЕРТ$_{ОК}$ не должен использоваться. В противном случае, такое неизвестное критичное расширение может быть проигнорировано.

Держателем СЕРТ$_{ОК}$ может быть конечный пользователь (физическое лицо) или другой ЦС. Обязательные поля сертификата не отличаются для этих типов владельцев. Расширение основных форматов встречается в сертификатах ЦС, что указывает на возможность использования данного СЕРТ$_{ОК}$ для построения маршрутов сертификации.

Субполе расширения «*предназначение (применимость) ключа*» указывает на виды служб обеспечения безопасности, в которых открытый ключ может использоваться (применяться).

Субполе расширения «*альтернативное наименование держателя сертификата*» используется для указания иных форм имён владельца закрытого ключа, например, DNS-имена[24] или адреса электронной почты.

ЦС могут иметь несколько пар ключей. Субполе расширения «*идентификатор ключа ЦС*» помогает пользователям выбрать правильный открытый ключ для проверки ЭП в данном

[24] *Domain Name System* – система именования сетевых сегментов/областей в Интернет-сети (RFC-1034 и -1035).

СЕРТ$_{ОК}$. Тоже предназначение имеет субполе расширения «*идентификатор ключа владельца сертификата*», которое используется для определения соответствующего открытого ключа владельца СЕРТ$_{ОК}$.

Субполе расширения «*политики сертификации*» включает глобальный УИД, который указывает на политику сертификации, применённую по отношению к данному СЕРТ$_{ОК}$. Различные организации (например, различные компании или правительственные учреждения) используют различные политики сертификации. Пользователи могут не определить политики других организаций. В этой связи, субполе расширения «*отображения политик*» преобразует информацию о политике других организаций в локально используемые политики. Это расширение используется только в сертификатах ЦС.

Субполе расширения «*узлы распространения СОС*» включает указатель на СОС, в котором может быть найдена информация о состоянии (статусе) данного СЕРТ$_{ОК}$.

Когда ЦС выпускает СЕРТ$_{ОК}$ для другого ЦС, первый декларирует, что сертификаты другого ЦС надёжны. Иногда издатель желает продекларировать, что определённая группа сертификатов надёжна. Для решения такой задачи существует три способа, а именно:

1. субполе расширения «*основные форматы*» имеет и второе значение, т.е. указывает, является ли данный ЦС надёжным при издании, либо СЕРТ$_{ОК}$ для других ЦС, либо только СЕРТ$_{ОК}$ пользователей;

2. субполе расширения «*форматы имён (наименований)*» может использоваться для описания совокупности СЕРТ$_{ОК}$ на основе имён, содержащихся, либо в поле «*держатель (владелец) сертификата*», либо в поле «*альтернативное имя держателя (владельца) сертификата*». Это поле расширения может использоваться для определения совокупности доступных или неприемлемых наименований;

3. субполе расширения «*форматы политик*» может использоваться для описания совокупности СЕРТ$_{ОК}$, которые основаны на содержании поля расширения «*политика сертификации*». Если форматы политик внедрены и используются, то пользователи будут уничтожать те СЕРТ$_{ОК}$, которые не содержат поля расширения «*политика сертификации*», или, когда соответствующие политики не определены.

3.5.3.2 Формат списка отозванных сертификатов

Сертификаты содержат дату окончания срока своего действия. К сожалению, указанные в СЕРТ$_{ОК}$ данные могут стать недействительными ещё до того, как истечёт срок действия сертификата. Издателям сертификатам необходим способ для непрерывного обновления данных о состоянии сертификатов, которые они выпустили. Одним из таких способов является СОС, представленный в стандарте X.509 [17].

СОС является ИОК-аналогом «*рабочего*» списка кредитных или дебетовых карт, который хранится специально для его просмотра продавцами ещё до их согласия на проведение крупной электронной сделки с помощью кредитных или дебетовых карт. СОС защищён с помощью ЭП выпустившего его ЦС. Если ЭП может быть проверена, то пользователи этого СОС знают, что его содержание не было модифицировано с момента формирования подписи. СОС содержат совокупность общих полей и могут включать дополнительные субполя расширений. СОС содержит следующие поля.

Версия. Это дополнительное поле определяет синтаксис СОС. (В настоящее время это поле будет содержать вторую или последующую версии.)

Алгоритм вычисления ЭП. Это поле указывает на используемый издателем СОС алгоритм формирования ЭП для подписания СОС.

Держатель (владелец) СОС. Это поле содержит УИД издателя СОС.

Дата выпуска СОС. Это поле указывает на дату выпуска (издания) данного СОС.

Дата выпуска очередного СОС. Это поле указывает на дату выпуска (издания) следующего СОС.

Отозванные (аннулированные) сертификаты. В этом поле перечислены аннулированные сертификаты. Запись о каждом отозванном $СЕРТ_{ОК}$ содержит последовательный номер сертификата, время аннулирования и дополнительные записи в СОС.

Субполе расширения «*запись в СОС*» используется для предоставления дополнительной информации о данном аннулированном $СЕРТ_{ОК}$. Это субполе может использоваться только во второй и всех последующих версиях СОС.

Субполя расширения СОС. Эти субполя используются для предоставления дополнительной информации о всём СОС. Эти субполя могут использоваться только во второй и всех последующих версиях СОС.

К наиболее общим субполям расширения, используемым в СОС, относятся следующие.

Номер СОС. По сути, это субполе содержит значение счётчика. В целом, это субполе расширения «предоставляет» пользователям информацию о том, что данный СОС был издан в качестве вспомогательного (например, при чрезвычайных обстоятельствах).

Как отмечено в предшествующем параграфе, ЦС могут иметь несколько пар ключей. Если в СОС имеет место субполе расширения «*идентификатор ключа ЦС*», то оно помогает пользователям правильно выбрать открытый ключ для проверки ЭП этого СОС.

Субполе «*ЦС, выпустивший сертификат*» содержит наименование СЕК-сегмента, но оно может не содержать тип наименования, который используется соответствующей прикладной системой. Субполе расширения «*альтернативное имя ЦС, выпустившего сертификат*»

используется для описания других форм наименований, используемых владельцем закрытого ключа, например, DNS-имена или адреса электронной почтовой службы.

Субполе расширения «*подтверждение узлов распространения*» используется в сочетании с субполем расширения «*узлы распространения СОС*», содержащимся в СЕРТ$_{ОК}$. Это субполе используется для подтверждения того, что данный СОС является одним из тех, которые были указаны в субполе расширения «*узлы распространения СОС*», и содержит запрашиваемую информацию о состоянии сертификата. Данное субполе расширения будет востребовано тогда, когда СОС не охватывает все сертификаты, изданные ЦС, после того как СОС мог быть доставлен в небезопасную сеть.

Субполя расширения, представленные далее, затрагивают сам СОС в целом. Кроме того, существуют субполя расширения, которые применяются в самом аннулированном сертификате.

Сертификаты могут отзываться по многим различным причинам. Например, криптомодуль пользователя мог быть просто украден или взломан. Субполе расширения «*код причины*» устанавливает причину отзыва (аннулирования) соответствующего СЕРТ$_{ОК}$. Взаимодействующая сторона может использовать эту информацию для принятия решения, могла ли быть допустимой ранее сформированная ЭП.

Иногда ЦС отказывается самостоятельно издавать свои собственные СОС. Он может делегировать эту функцию другому ЦС. ЦС, выпускающий СОС, может добавлять информацию о состоянии сертификатов, изданных другими ЦС, в один и тот же СОС. Субполе расширения «*издатель сертификата*» позволяет определить, какой ЦС выпустил соответствующий СЕРТ$_{ОК}$, или группу сертификатов, представленных в СОС.

3.5.3.3 Формат СЕРТ$_{АТ}$

СЕРТ$_{ОК}$, рассмотренные в §3.5.3.1, обеспечивают «криптосвязку» между держателем (владельцем) сертификата и открытым ключом. Связь между держателем сертификата и открытым ключом рассматривается как долговременная связь. Большинство с СЕРТ$_{ОК}$ конечных пользователей включают срок своего действия, как правило, в течение от одного года до двух лет.

Большинство организаций, различных форм собственности, стремятся улучшить систему управления доступом (УД) [107]. СЕРТ$_{ОК}$ могут использоваться для аутентификации ПП пользователя, а сам ПП может использоваться в качестве входных данных для функции принятия решения в рамках системы УД. Однако, в большинстве случаев ПП не является признаком, используемым при принятии решений в системах УД. Решение относительно доступа в системах УД может зависеть от функциональной роли участника информационного взаимодействия, категории допуска, членства в группе или способности оплачивать товары или услуги.

Информация для авторизации (проверки полномочий или прав доступа), например, членство в группе, как правило, имеет непродолжительный срок действия, по сравнению со связкой ПП и открытого ключа. В принципе, данные для авторизации могли быть размещены в поле расширения $СЕРТ_{ОК}$. Однако, это неприемлемо по следующим двум причинам. *Во-первых*, сертификат, вероятнее всего, будет аннулирован вследствие необходимости обновления данных для авторизации. Аннулирование и переиздание $СЕРТ_{ОК}$ с обновлённой информацией для авторизации – весьма затратная процедура. *Во-вторых*, ЦС, выпускающий $СЕРТ_{ОК}$, вероятнее всего, не будет правомочен для выпуска данных для авторизации. А это повлечёт за собой проведение со стороны ЦС дополнительных процедур информационного обмена с правомочным источником информации для авторизации.

$СЕРТ_{АТ}$ «*привязывает*» атрибуты к владельцу атрибутного сертификата [100,108]. $СЕРТ_{АТ}$ ориентирован на использование в прикладных ИТС (включая гипертекстовые ИТС). Так как $СЕРТ_{АТ}$ не содержит открытого ключа, $СЕРТ_{АТ}$ используется в сочетании с $СЕРТ_{ОК}$. Функциональные модули системы контроля и УД (СКУД) могут использовать атрибуты, предоставляемые в $СЕРТ_{АТ}$, но они не могут быть заменой при аутентификации. $СЕРТ_{ОК}$ должен использоваться, в первую очередь, при проведении аутентификации, а затем используется $СЕРТ_{АТ}$ с целью демонстрации связи атрибутов с аутентифицированным ПП.

Кроме того, $СЕРТ_{АТ}$ может использоваться при предоставлении услуг аутентификации источника данных [95] и обеспечения неотказуемости [96]. С точки зрения прикладной значимости, атрибуты, содержащиеся в $СЕРТ_{АТ}$, предоставляют дополнительную информацию об авторе ЭП (например, его полномочия или права (и объекты) доступа). Такая информация может использоваться для обеспечения гарантий того, что автор ЭП правомочен относительно подписания конкретных данных. Такой вариант проверки зависит, либо от ситуации, в которой осуществляется обмен данными, либо от самих данных, которые были подписаны с помощью ЭП.

Любой сертификат безопасности представляет собой маркер безопасности [109,110], и, в частности, $СЕРТ_{АТ}$ реализуют способ защищённой доставки данных для авторизации, например, в интересах модуля принятия решений в СКУД. $СЕРТ_{АТ}$ похож на $СЕРТ_{ОК}$ и подписывается издателем. $СЕРТ_{АТ}$ содержит девять полей: версия, держатель, издатель, идентификатор алгоритма подписи, последовательный номер, период действия, атрибуты, УИД издателя и субполя расширения.

Поле «*держатель сертификата*» аналогичен полю в $СЕРТ_{ОК}$, но в этом поле владелец может указываться с помощью имени, издателя и последовательного номера $СЕРТ_{ОК}$ или результата вычисления хэш-функции по последовательности данных сертификата или открытого ключа.

Атрибуты содержат информацию для авторизации, связанную с держателем $СЕРТ_{АТ}$. Субполя расширения содержат дополнительную информацию о самом $СЕРТ_{АТ}$ и порядке его использования.

3.5.4 Дополнительные ИОК-услуги

Помимо услуг по обеспечению безопасности, рассмотренных ранее (идентификация и аутентификация, обеспечение неотказуемости, конфиденциальности и целостности), ИОК могут предлагать (предоставлять) и другие услуги. К наиболее важным дополнительным ИОК-услугам относятся восстановление ключа и авторизация.

Восстановление ключа. Если ключ пользователя потерян, то федеральные ведомства и коммерческие организации, тем не менее, обязаны быть способными восстановить данные, которые зашифровал один из их сотрудников, и которые могут быть расшифрованы только в случае восстановления ключа для зашифрования. К причинам восстановления ключа могут относиться:

- сотрудник забыл пароль для разблокировки зашифрованного файла;
- смерть сотрудника, который зашифровал некоторую информацию;
- некто попытался скрыть свою криминальную деятельность от правоохранительных органов.

Для обеспечения гарантий относительно возможности восстановления зашифрованных данных должны создаваться копии ключей для зашифрования, а сами копии должны храниться в защищённом виде.

Тем не менее, следует отметить, что ключи подписи, т.е. ключи, используемые для формирования ЭП, не должны иметь резервных копий, так как это помешает ИОК надёжно предоставлять услугу по обеспечению неотказуемости. Если кто-либо другой, а не соответствующий пользователь, обладает копией ключа для формирования ЭП, то в последствие такой пользователь сможет утверждать, что кто-то ещё поставил подпись на оспариваемом документе. Если пользователь потерял ключ для формирования подписи, то на смену утраченного ключа могут быть достаточно легко сформированы новый ключ и связанный с ним сертификат. ИОК обязана хранить запись о владельце (пользователе) ключа, но не сам ключ.

Права доступа/авторизация. Сертификаты могут использоваться для подтверждения ПП пользователя и особых привилегий (прав доступа), которые были предоставлены пользователю. Привилегии могут включать исключительное право на просмотр секретной информации или разрешение на модификацию данных на сервере прикладной (гипертекстовой) АИС (среди прочих привилегий).

3.6 Североамериканская модель организации ИОК

Создание и развитие *национальной ИОК в США* (или североамериканской модели ИОК) было обусловлено принятием двух важнейших государственных законодательных актов:

1. *Закон о мобильности и подотчётности в здравоохранении,* принятый в 1996 году [111], требовавший в том числе создания национальных стандартов для ЭДО в здравоохранении и общих идентификаторов для поставщиков услуг медицинского страхования и работодателей;
2. *Закон о прекращении БДО в правительстве*, принятый в 1998 году [112]. Он требовал, чтобы за 5 лет система предоставления информации (услуг) гражданам федеральными органами исполнительной власти и службами, а также все процедуры были переведены в электронный формат (ЭДО). Так же он устанавливал юридический статус ЭП, и обязывал ведомства внедрить процедуры электронной аутентификации.

3.6.1 Состав участников национальной ИОК США

3.6.1.1 Органы управления национальной ИОК США

Федеральный совет IT-директоров (ФСД). В состав ФСД входят IT-директора всех министерств уровня кабинета министров и других независимых ведомств [16,113]. ФСД сформировал структуру взаимодействия федеральных ИОК и контролирует работу четырёх организаций, которые являются ответственными за управление такой инфраструктурой и её развитие, и совершенствование. В частности, действующая федеральная политика сертификации (ФПС) была разработана под руководством и с одобрения ФСД.

Федеральный центр разработки и реализации политики развития национальной ИОК США (ФЦРП). ФЦРП – группа ведомств федерального правительства США (включая ведомства на уровне кабинета министров), утверждённых ФСД. ФПС регулируется и реализуется ФЦРП и отражает интересы ФСД.

ФЦРП отвечает за:

• реализацию ФПС;

• утверждение Отчётов о своей текущей деятельности по сертификации (ОДС, *certificate practice statement*) каждого ЦС, который издаёт $СЕРТ_{ОК}$ в соответствие с ФПС;

• утверждение Отчёта по результатам аудиторской проверки на предмет соответствия каждого ЦС, который издаёт $СЕРТ_{ОК}$ в соответствие с ФПС;

• обеспечение гарантий непрерывного соответствия каждого ЦС, который издаёт $СЕРТ_{ОК}$ в соответствие с ФПС и выполняет соответствующие требования, что является условием приемлемого непрерывного функционирования.

Федеральный центр обеспечения и регулирования национальной ИОК США (ФЦОР). ФЦОР – организация, которая эксплуатирует и обслуживает корневые ЦС, реализующие единую политику от имени правительства США в соответствии с указаниями ФЦРП.

Руководитель программ ФЦОР. Руководитель программ – представитель ФЦРП, главное ответственной лицо, которое осуществляет надзор за корректным функционированием корневых ЦС, реализующих единую политику, включая соответствующий репозитарий, и подбор сотрудников ФЦОР. Руководитель программ выбирается ФЦОР и отчитывается перед ФЦРП. Руководитель программ ФЦОР обязан иметь форму допуска к секретной информации не ниже «*Top Secret*».

Центр реализации политики сертификации (ЦРПС). Каждая организация, которая предоставляет ИОК-услуги в соответствии с ФПС, должна определить субъект или группу субъектов, которые будут отвечать формирование ОДС провайдера (сервера) электронных услуг (ПЭУ, *shared service provider*) и за обеспечение гарантий того, чтобы все компоненты ИОК провайдера (сервера) электронных услуг (например, ЦС, серверы, предоставляющие информацию о состоянии сертификатов (ССС, *certificate status server*), системы обслуживания смарт-карт (*card management system*), ЦР) функционировали в соответствие с ОДС ПЭУ и действующей ФПС. С точки зрения ФПС, этот центр называется ЦРПС ПЭУ.

Ведомства, которые заключили контракты на предоставление услуг с ЦС, и которые выполняют требования ФПС, обязаны сформировать у себя структурные подразделения, обслуживающие любые функциональные компоненты ведомства (например, ЦР или репозитарии) и предотвращающие возникновение нештатных ситуаций, связанных с некорректным использованием пространством имён (наименований). Этот центр называется ЦРПС ведомства.

ЦРПС ПЭУ несёт ответственность за оповещение своего обсуживаемого ЦРПС ведомства и ФЦРП о любых изменениях инфраструктуры (как минимум за две недели изменения), которые могут негативно повлиять на федеральный ИОК-сегмент национальной ИОК США.

Все новые электронные документы (СЕРТ$_{ОК}$ ЦС, узлы распространения СЕРТ$_{ОК}$, универсальные идентификаторы ресурсов (*universal resource identificator* – URI) для доступа к информации ЦС и/или соответствующего субъекта и т.п.), сформированные в результате произошедших изменений, должны быть предоставлены в ФЦРП в течении последующих 24 часов с момента изменения инфраструктуры.

ЦРПС ведомства несёт ответственность за обеспечение гарантий того, что все функциональные ИОК-компоненты ведомства (например, ЦС, ССС и ЦР) функционируют в соответствие с ФПС и соответствующим ОДС и будут служить связующим звеном между этим ведомства с ФЦРП и ЦРПС ПЭУ.

Центр Сертификации. ЦС – это объединение комплекса технических, программно-аппаратных средств и обслуживающего персонала, которое формирует, подписывает и издаёт $СЕРТ_{ОК}$ для своих пользователей.

ЦС несёт ответственность за выпуск и обслуживание $СЕРТ_{ОК}$, включая:

- процесс изготовления $СЕРТ_{ОК}$;
- опубликование $СЕРТ_{ОК}$;
- отзыв (аннулирование) $СЕРТ_{ОК}$;
- формирование и уничтожение ключей подписи ЦС;
- обеспечение гарантий того, что службы, функции и инфраструктура ЦС, связанные с $СЕРТ_{ОК}$, издаваемыми таким ЦС, реализуются в соответствие с требованиями, форматами данных и гарантиями ФПС.

Серверы, предоставляющие информацию о состоянии сертификатов. ИОК могут дополнительно включать центры, которые предоставляют информацию о состоянии $СЕРТ_{ОК}$ от имени ЦС с помощью интерактивных транзакций. В частности, ИОК могут включать серверы, реализующие протокол интерактивной проверки состояния $СЕРТ_{ОК}$ (*on-line certificate status protocol,* OCSP [114]), и которые предоставляют информацию о состояния $СЕРТ_{ОК}$ в интерактивном режиме. Такие центры именуются ССС.

Если ССС указан в $СЕРТ_{ОК}$ как официальный источник информации об отзыве, функции такого ССС представлены в ФПС. ССС должен указывать объектные идентификаторы (*object identificator,* OID) всех политик, которые он реализует в статусе официального. Например, ССС могут быть указаны в субполе «*authority information access*» поля «*расширения*» $СЕРТ_{ОК}$. OCSP-серверы, которые являются локально доверенными [114], не подпадают под действие ФПС.

3.6.1.2 Центры регистрации

ЦР собирают и проверяют ПП каждого субъекта (будущего ИОК-пользователя) и информацию, которая должна быть включена в $СЕРТ_{ОК}$ его владельца. ЦР реализуют эту функцию в соответствии с ОДС, утверждённым ФЦРП.

ЦР несёт ответственность за:

- контроль и управление процессами регистрации;
- процессами идентификации и аутентификации.

3.6.1.3 Доверенные субъекты

Доверенный субъект – физическое лицо, которое удовлетворяет всем требованиям благонадёжности ЦР, и которое обеспечивает защиту параметра подлинности в качестве уполномоченного субъекта ЦР. Доверенный субъект регистрирует информацию и проверяет биометрические данные (например, фотографии) в предоставленных учётных документах кандидатов, которые не могут лично явиться на ЦР.

ОДС устанавливает субъекты, которые отвечают за предоставление таких услуг, а также способы определения их благонадёжности.

3.6.1.4 Пользователи

Пользователь – субъект/объект, имя/наименование которого указано в СЕРТ$_{ОК}$ в качестве его владельца. Пользователь «заявляет», что он или она использует ключ и СЕРТ$_{ОК}$ в соответствии с политикой сертификации, указанной в СЕРТ$_{ОК}$, и не выпускает СЕРТ$_{ОК}$. В соответствие с ФПС, ИОК-пользователями могут быть только федеральные служащие, подрядные организации, персонал дочерних организаций и комплексы технических и программно-аппаратных средств, обслуживаемые федеральными ведомствами или по их поручению. Термин «пользователь» указывает только на тех, кто запрашивает СЕРТ$_{ОК}$ для использования, а не на тех, кто подписывает и выпускает СЕРТ$_{ОК}$ или публикует информацию о состоянии СЕРТ$_{ОК}$.

Некоторой части пользователей могут выдаваться СЕРТ$_{ОК}$ в соответствие с их функциональными должностями (зонами ответственности). Такие СЕРТ$_{ОК}$ определяют функциональную должность (зону ответственности), в соответствие с которой пользователь осуществляет соответствующие полномочия, а не имя пользователя, и выдаются в интересах поддержки принятия решений в сфере бизнеса. СЕРТ$_{ОК}$, определяющий функциональную должность (зону ответственности) может использоваться в тех случаях, когда предусматривается обеспечение неотказуемости. В СЕРТ$_{ОК}$, выпущенных для нескольких пользователей, может быть указана одна и та же конкретная функциональная должность (зона ответственности), тем не менее, пара криптоключей будет уникальна для каждого индивидуального СЕРТ$_{ОК}$, определяющего такую функциональную должность (зону ответственности). Например, может быть четыре пользователя, получивших СЕРТ$_{ОК}$, выданный для функциональной должности «министр торговли», однако, каждый из четырёх индивидуальных СЕРТ$_{ОК}$ будет содержать уникальный открытый ключ (который соответствует конкретной паре (открытый/закрытый) криптоключей) и идентификаторы самого сертификата. Функциональные должности (зоны ответственности), для которых могут быть вы-

пущены $СЕРТ_{ОК}$, определяющие такие функциональные должности (зоны ответственности), ограничены теми должностями, которые установлены руководством (должностным регламентом) организации.

3.6.1.5 Доверяющие стороны

Доверяющая сторона – субъект, который доверяет подлинности криптографической привязки имени пользователя к открытому ключу.

Доверяющая сторона:

- несёт персональную ответственность за принятие решения о том, следует ли доверять и как подтвердить подлинность сертификата путём проверки соответствующей информации о его состоянии;
- может использовать $СЕРТ_{ОК}$ для:
  - проверки целостности подписанного с помощью ЭП сообщения;
  - определения автора сообщения;
  - формирования защищённого (с точки зрения обеспечения конфиденциальности) виртуального соединения с владельцем $СЕРТ_{ОК}$;
- может использовать информацию в $СЕРТ_{ОК}$ (например, идентификаторы политики сертификации) с целью определения его пригодности в прикладных процессах и процедурах.

С точки зрения ФПС, доверяющей стороной может быть любой субъект, который желает подтвердить подлинность криптографической привязки открытого ключа к имени (функциональной должности) федерального служащего, контрагента или иного сотрудника компании-партнёра.

3.6.1.6 Другие участники

ЦС и ЦР, функционирующим в соответствие с ФПС, могут потребоваться услуги других центров обеспечения безопасности, объединений и прикладных АИС, например, объединения аудиторов и центры, издающие $СЕРТ_{АТ}$. В ОДС будут указаны взаимодействующие стороны, которые отвечают за предоставление таких услуг, а также способы их предоставления.

3.6.2 Обязанности федеральных ведомств США

Все федеральные ведомства США обязаны использовать *федеральный сегмент национальной ИОК США* с целью:

– доступа к объектам, обеспечения сетевой аутентификации, а также аутентификации некоторых прикладных ИТС, предусматривающих оценку рисков;

– совместного использования документов и ЭП;

– обмена подписанными и зашифрованными сообщениями электронной почты между федеральными ведомствами.

Федеральный сегмент национальной ИОК США решает следующие основные технологические задачи (рисунок 3.10):

1) устанавливает доверие между федеральными ведомствами и промышленностью;
2) обеспечение технической неотказуемости;
3) проведение процедур аутентификации и шифрования;
4) формирование и проверку ЭП.

Рисунок 3.10 – Основные технологические задачи, решаемые федеральным сегментом национальной ИОК США

Возможность решения этих четырёх технологических задач обусловлено использованием цифровых сертификатов, политик сертификации, стандартов и процессов выпуска сертификатов, а также критически важной инфраструктуры доверия.

3.6.3 Модель доверия национальной ИОК США

Североамериканская модель ИОК представляет собой архитектуру на основе *связующего ЦС* (СЦС) и предназначена для взаимодействия ИОК организаций и ведомств, невзирая на их архитектуры [113]. Единственное *целевое предназначение СЦС* – формирование взаимосвязей

между ИОК организаций и ведомств. На рисунке 3.11 представлен принцип функционирования СЦС.

В отличие от сетевого ЦС, СЦС не выпускает СЕРТ$_{ОК}$ непосредственно пользователям. В отличие от корневого ЦС в иерархической ИОК, СЦС не предназначен для использования в качестве «узла доверия». Все ИОК-пользователи полагают, что СЦС является промежуточной точкой. СЦС устанавливает равноправные взаимоотношения между ИОК различных организаций и ведомств. Такие взаимосвязи могут быть объединены с целью формирования «*моста доверия*» (*bridge of trust*), соединяющего ИОК-пользователей различных организаций.

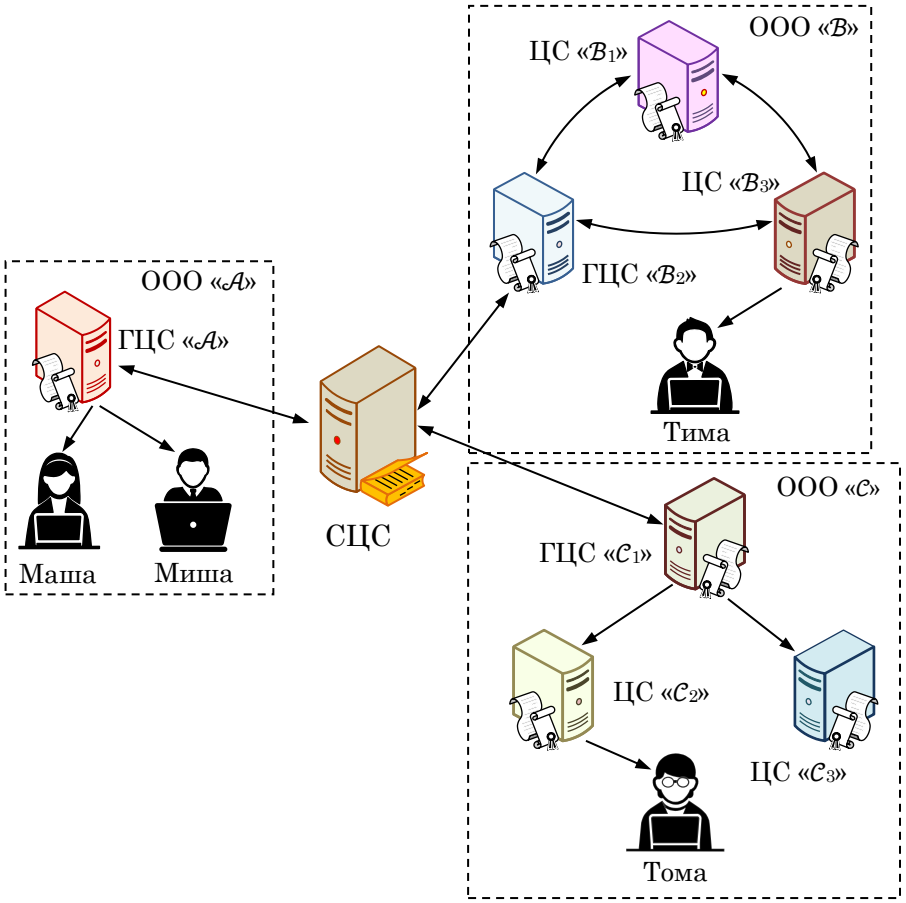

Рисунок 3.11 – Пример СЦС и ИОК организаций

Если доверенный сетевой сегмент представляет собой иерархическую ИОК, то СЦС формирует взаимосвязь с корневым ЦС. Если же доверенный сетевой сегмент представляет собой сетевую ИОК, то СЦС формирует взаимосвязь только с одним ЦС из всей совокупности ЦС (рисунок 3.11). В обоих случаях, ЦС, который устанавливает доверенную взаимосвязь с СЦС, именуется как главный ЦС (ГЦС).

На рисунке 3.11 представлен СЦС, который взаимодействует с тремя ИОК организаций ($\mathcal{A}$, $\mathcal{B}$ и $\mathcal{C}$). В первой расположен ГЦС Миши и Маши, во второй, иерархической ИОК – ЦС Томы, а в третьей, сетевой ИОК – ЦС Тимы. Ни один из пользователей не доверяет СЦС напрямую.

Маша и Миша доверяют ГЦС «$\mathcal{A}$», который выпустил для них СЕРТ$_{ОК}$. Они доверяют и СЦС, так как их ГЦС «$\mathcal{A}$» выпустил СЕРТ$_{ОК}$ и для него. Точкой доверия Томы является корневой ГЦС «$\mathcal{C}_1$». Она также доверяет СЦС, так как корневой ЦС «$\mathcal{C}_1$» выпустил для него сертификат. Тима доверяет сетевому ЦС «$\mathcal{B}_3$», который выпустил для него СЕРТ$_{ОК}$. Он также доверяет СЦС, так как существует маршрут доверенной сертификации от ЦС «$\mathcal{B}_3$», который выпустил для него сертификат, до СЦС. Маша (или Миша) может использовать «мост доверия», который реализуется СЦС, для установления доверенных взаимосвязей с Томой и Тимой.

На рисунке 3.12 представлена модель доверия национальной ИОК США, включающая федеральный СЦС (ФСЦС). Основной его задачей является создание цепочки сертификации как между федеральными ведомствами, объединяя их в одну государственную сеть доверия, так и создание связи с негосударственной сетью доверия [113]. Очевидно, что как ЦС федеральных ведомств, так и частные ЦС должны удовлетворять определённым требованиям для того, чтобы провести взаимную сертификацию с ФСЦС (рисунок 3.12).

ФСЦС представляет собой объединяющий элемент, предназначенный, в частности, для объединения несвязанных между собой ЦС ведомств в единый федеральный сегмент национальной ИОК. Необходимо заметить, что СЦС не является корневым УЦ, но он является «мостом доверия». Он не является началом маршрутов сертификации, но соединяет доверенные сегменты посредством взаимной сертификации между ФСЦС и выделенными ГЦС. Такие доверенные сегменты могут быть, как в рамках федеральных органов исполнительной власти (правительства) США, так и за его пределами.

Федеральные (или не федеральные) ЦС, которые функционируют в доверенных сегментах, удовлетворяющих требованиям, разработанным ФЦРП, имеют возможность и способны взаимно сертифицироваться с ФСЦС. ФСЦС объединяет их в федеральный доверенный сетевой сегмент (или сеть) национальной ИОК. Это позволяет взаимодействующим сторонам и владельцам СЕРТ$_{ОК}$ (в их доверенных сегментах) связываться с укрупнённым федеральным ИОК-сегментом. Это гораздо проще и значительно эффективнее, чем попытка управления совокупностью множества взаимно сертифицированных между собой ЦС из различных доверенных сегментов.

С целью обеспечения максимальной гибкости федеральных ведомств и не вмешательства в их прерогативы, ведомствам не требуется адаптироваться к политикам ФСЦС. Ведомства в качестве дополнительной функции используют другие политики, разработанные их собственными внутренними (ведомственными) центрами реализации политики сертификации. Ведомствам не нужно обращаться в ФСЦС для обеспечения функционального взаимодействия с другими федеральными ведомствами или организациями, расположенными вне федерального правительства. В качестве альтернативы, федеральные ведомства могут напрямую взаимодействовать с ведомствами/организациями в целях формирования требований к их функциональной совместимости.

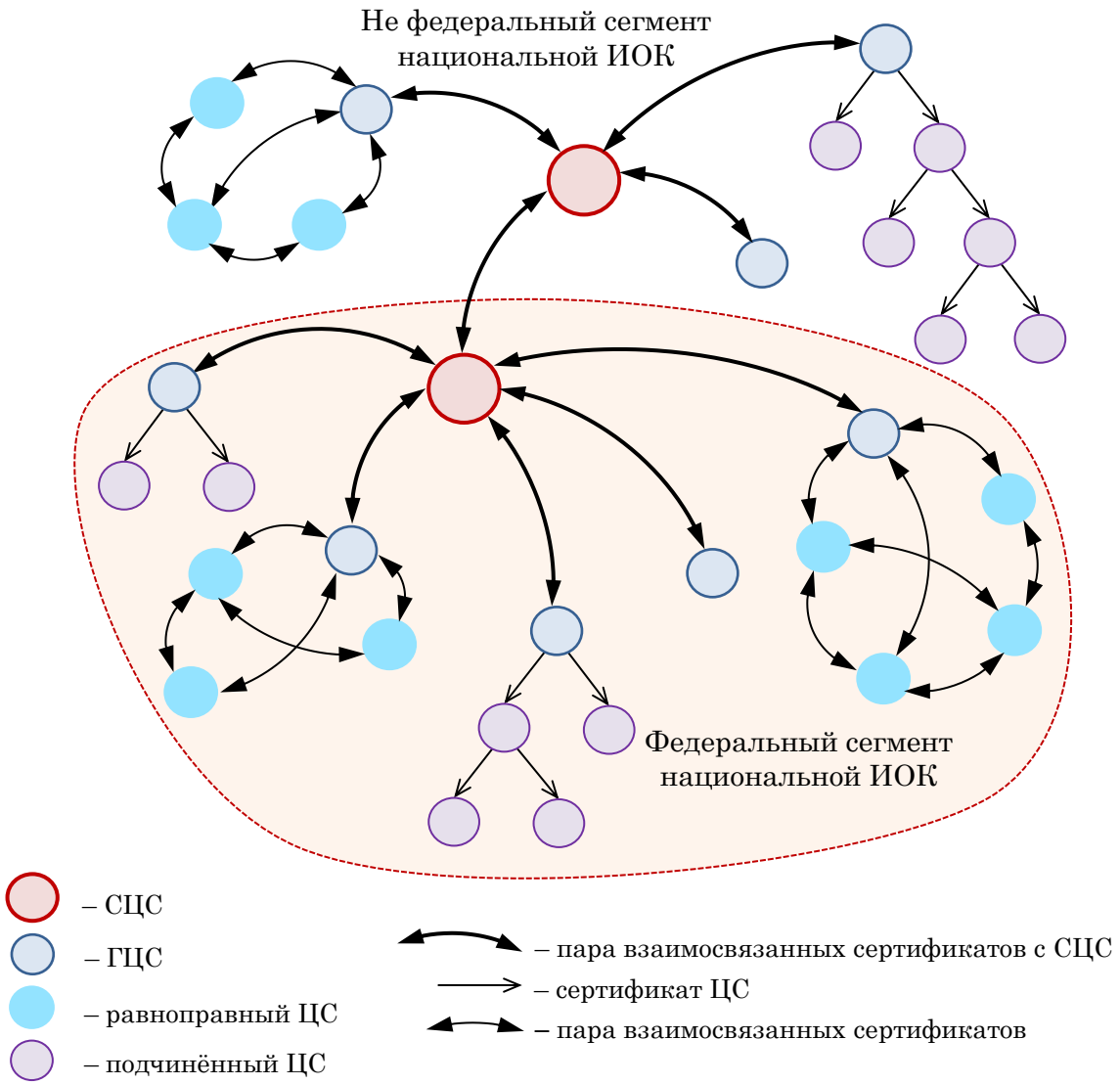

Рисунок 3.12 – Функциональное взаимодействие между федеральным и не федеральным сегментами национальной ИОК США через ФСЦС

По данным на 25 октября 2021 года высшую иерархию национальной ИОК США[25] составляют десять центров сертификации во главе с ФЦРП, а именно (рисунок 3.13):

1. ФЦРП (*Federal Common Policy CA*). Атрибуты $СЕРТ_{ОК}$: идентификатор (*id*): «*CN=Federal Common Policy CA,OU=FPKI,O=U.S. Government,C=US*».

Входные маршруты доверия: от самого ФЦРП и ФСЦС «*G4*».

Выходные маршруты доверия: до самого ФЦРП, ФСЦС «*G4*», ЦС «*DigiCert Federal SSP Intermediate CA – G5*», ЦС «*ORC SSP 4*», ЦС «*Symantec SSP Intermediate CA – G4*», корневого ЦС государственного департамента США («*U.S. Department of State AD Root CA*»), ЦС

[25] URI: https://fpki.idmanagement.gov/tools/fpkigraph/.

«*Verizon SSP CA A2*», корневого ЦС «*Entrust Managed Services Root CA*», ЦС «*WidePoint ORC SSP 5*» и корневого ЦС министерства финансов США («*US Treasury Root CA*»).

2. ФСЦС «*G4*» (*Federal Bridge CA G4*);

3. Корневой ЦС государственного департамента США (*U.S. Department of State AD Root CA*);

4. Корневой ЦС министерства финансов США (*U.S. Treasury Root CA*);

5. ЦС провайдера (сервера) электронных услуг, принадлежащего телекоммуникационной компании «*Verizon*» США, «*A2*» (*Verizon SSP CA A2*);

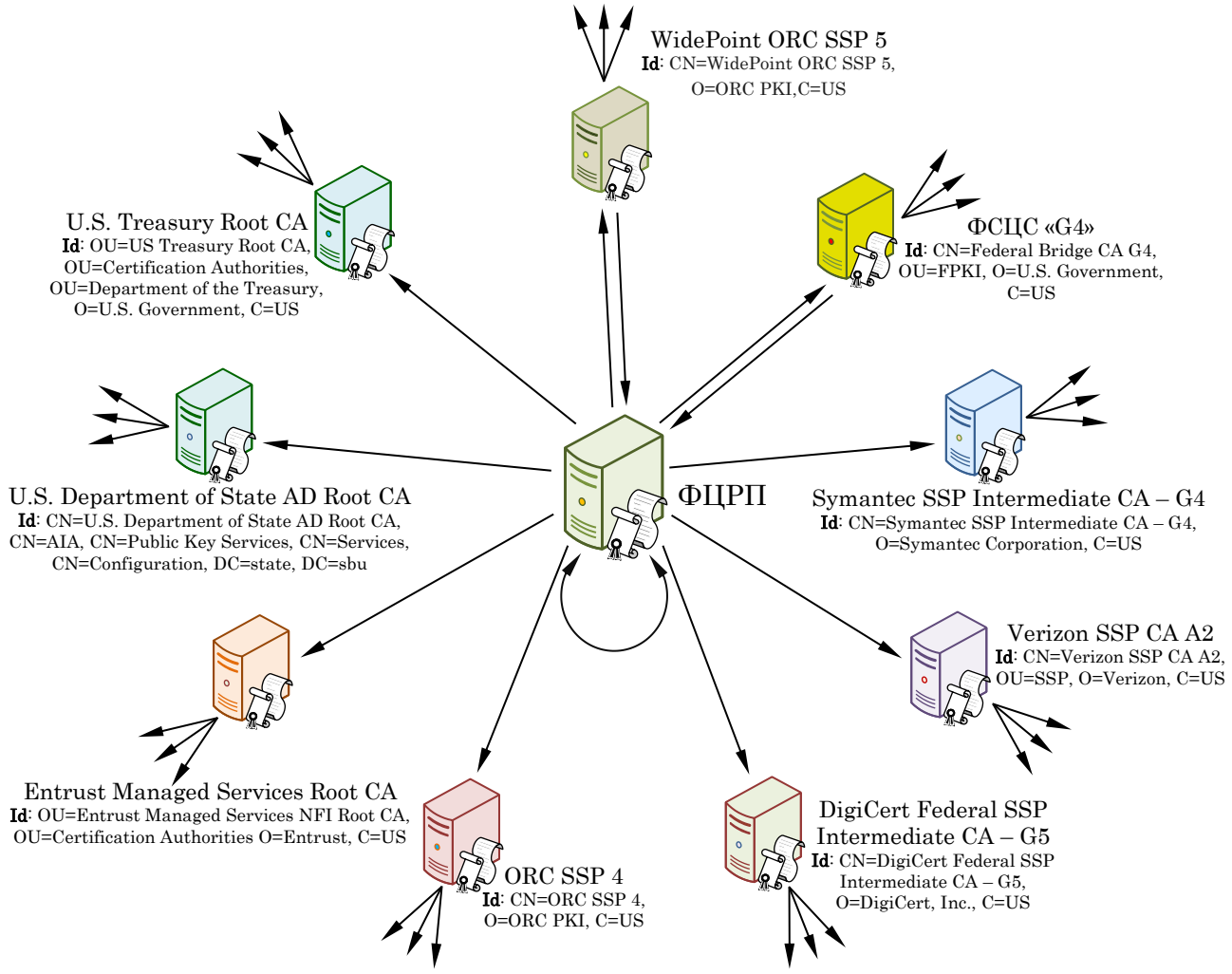

Рисунок 3.13 – Структура высшей иерархии национальной ИОК США

6. Корневой ЦС службы (сервера) предоставления электронных услуг американской компании «*Entrust Datacard*» (*Entrust Managed Services Root CA*);

7. Промежуточный ЦС провайдера (сервера) электронных услуг федерального уровня, принадлежащего технологической компании «*DigiCert*»[26] США, «*G5*» (*DigiCert Federal SSP Intermediate CA – G5*);

8. Промежуточный ЦС провайдера (сервера) электронных услуг, принадлежащего технологической компании «*Symantec» США, «G4*» (*Symantec SSP Intermediate CA – G4*);

9. Промежуточный ЦС провайдера (сервера) электронных услуг, принадлежащего компании «*ORC (Operational Research Consultants)*» США, «*4*» (*ORC SSP 4*);

10. Промежуточный ЦС провайдера (сервера) электронных услуг, принадлежащего компании «*WidePoint Corporation*» США, «*5*» (*WidePoint ORC SSP 5*), и который обслуживает министерство обороны и другие федеральные ведомства США

В рамках национальной ИОК США определено понятие «*присоединённого*» ЦС. Это такой ЦС, СЕРТ$_{ОК}$ которого могут участвовать в формировании маршрута доверия до ФЦРП или другого присоединённого ЦС через ФСЦС.

3.7 Западноевропейская модель организации ИОК

3.7.1 Основные концепции и иерархическая структура ИОК Евросоюза

В Европейском союзе (ЕС) был принят основополагающий нормативный акт: «Директива Европейского парламента и Европейского совета от 13 декабря 1999 года об Основах объединения электронных подписей» [15]. Документ лёг в основу создания ИОК Западной Европы, которую в ЕС оценивают, как основу создания *электронного правительства* и *электронного бизнеса* и т.п.

Необходимость издания документа вызвана тем, что национальные ИОК европейских стран создавались и совершенствовались по образцу северо-американской модели ИОК (§3.6). Однако наличие в ЕС более 20 государственных языков[27] потребовало от Еврокомиссии формирования новых концепций при создании и развитии единой (федеративной) модели ИОК. Такими концепциями являются: *Центр подтверждения подлинности* (ЦПП, *validation authority*) и *Реестр состояния доверенных служб* (РСДС, *trust-service status list*). Функциональная структура ЦПП представлена на рисунке 3.14.

[26] Услугами этого ЦС пользуется Сбербанк РФ (пара асимметричных ключей и СЕРТ$_{ОК}$).
[27] Английский, болгарский, венгерский, голландский, греческий, датский, ирландский, испанский, итальянский, латвийский, литовский, мальтийский, немецкий, польский, португальский, румынский, словацкий, словенский, финский, французский, хорватский, чешский, шведский, эстонский.

Одной из основных услуг ЦПП, которая предоставляется его пользователям, является проверка подлинности СЕРТ$_{ОК}$ в режиме «*одного окна*» («*one-stop-shop*»). Сложность *системы обслуживания ЭП* (ИТСЭП[28]), с точки зрения установления взаимосвязей с каждым ЦС на территории ЕС, связана с трудно реализуемым процессом контроля и проверки состава и содержания СЕРТ$_{ОК}$, выдаваемых европейцам техническими ЦС (в частности многообразие национальных языков), которых в Европе насчитывается несколько сотен.

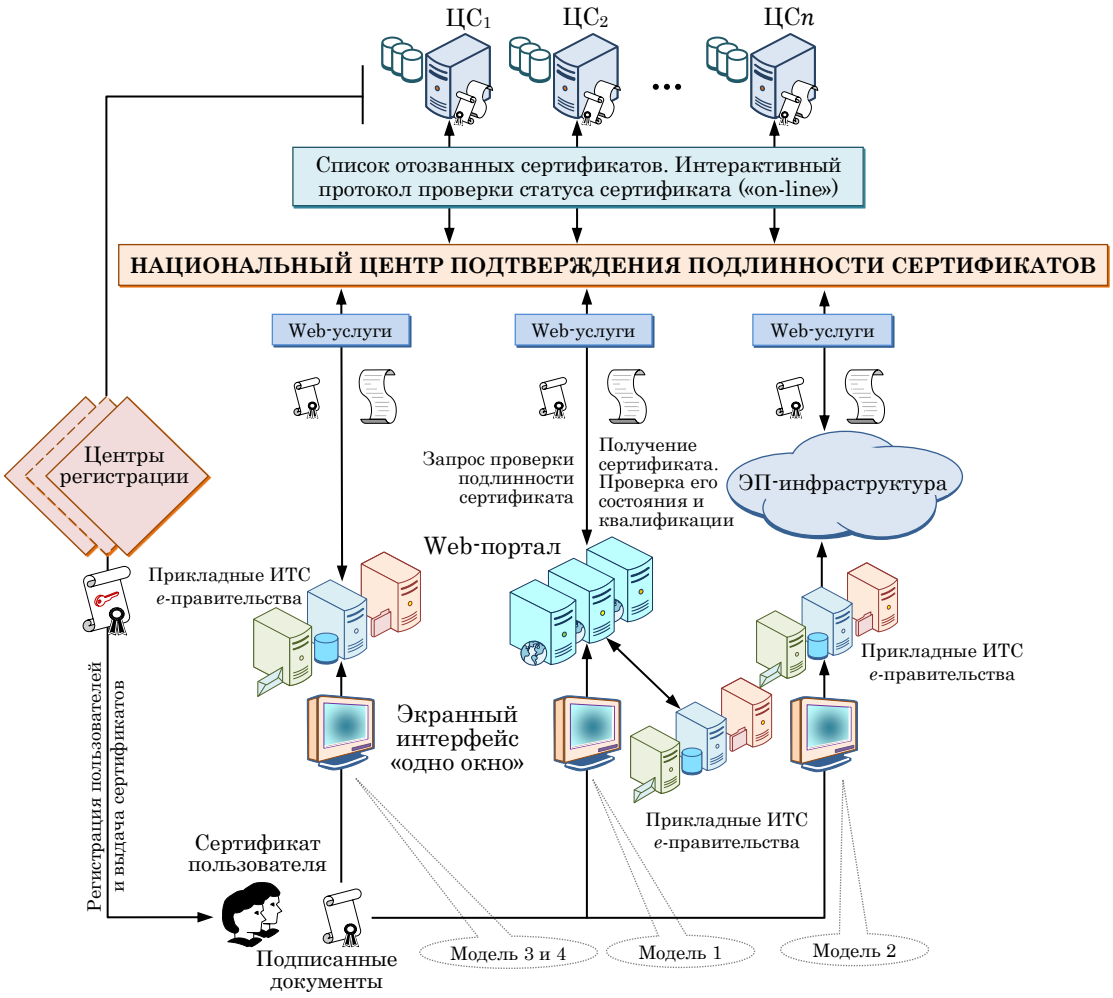

Рисунок 3.14 – Функционально-структурная модель ЦПП в ИОК ЕС

Следовательно, любая ИТСЭП должна обеспечивать:

1. проверку подлинности СЕРТ$_{ОК}$ напрямую с выдавшим его ЦС, если последний известен, но в том случае, когда ЦПП не нужен;

2. нахождение адреса ЦПП, способного и доступного для обработки СЕРТ$_{ОК}$, выданных указанным в сертификате УЦ;

[28] В данном случае под ИТСЭП понимается любая ИТС (например, ЭДО, платёжная, финансовая, система электронной коммерции (бизнеса) и т.п.), которая обрабатывает, хранит и транслирует или использует электронные сообщения (документы), содержащие ЭП.

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 коммерческий или государственный ЦПП национального или европейского уровня.

Представленная на рисунке 3.14 иерархическая структура распределения функций по обслуживанию ЭП основывается на концепции использования национальных ЦПП. В зависимости от соответствующей модели самой ИТСЭП, структура может:

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

– передавать запросы на *Web*-портал, соединяющий с ЦПП (модель 1);

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

Для формирования федеративной системы ЦПП ЕС было 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 ИТСЭП;

▪ построение жизнеспособной модели управления на европейском уровне.

Второй важнейшей услугой, предоставляемой ЦПП, является проверка подлинности ЭП: грамматико-синтаксический анализ и математическая проверка ЭП.

Делегирование этой процедуры ЦПП требует доставки всего документа в ЦПП (включая ЭП и возможно существующую электронную метку времени). Это может противоречить требованию нераскрытия документа при обработке конфиденциальных данных. Данную проблему можно преодолеть с помощью локального вычисления значений хэш-функции подписанного документа и последующей доставки только результата вычисления хэш-функции вместо всего документа. При таком подходе процедуру проверки подлинности $СЕРТ_{ОК}$ можно рассматривать как частный процесс процедуры проверки подлинности ЭП. Если в ЭП присутствует электронная метка времени, то последняя должна обязательно подтверждаться.

На ЦПП могут возлагаться дополнительные функции, среди них:

– извлечение информации о владельцах $СЕРТ_{ОК}$ X.509v3 и проведение их семантической обработки с целью обеспечения *трансграничной функциональной совместимости* ЭП;

– проведение проверки на предмет *исторической подлинности* $СЕРТ_{ОК}$ и ЭП. В идеальном варианте эта услуга должна быть основной для ЦПП, так как конечному пользователю, как правило, не интересно, является ли ЭП подлинной в настоящий момент, ему более интересно знать, была ли подпись подлинна в момент подписания документа (эта более поздняя проблема

определяет значение подписи). Эта процедура позволит ИТСЭП проверить подлинность $СЕРТ_{ОК}$ или ЭП в указанный в прошлом момент времени.

3.7.2 Модель федеративной ИОК ЕС

В широком смысле модель федеративной ИОК ЕС включает следующих участников:

1. ЦС, которые выдают $СЕРТ_{ОК}$. Их основная роль заключается в:

– создании базовой инфраструктуры, предназначенной для формирования ЭП «руками» пользователей этой инфраструктуры;

– обеспечении базовых «строительных» компонентов для проверки подлинности $СЕРТ_{ОК}$ (ЦПП), которые выдают эти ЦС;

– соблюдении стандартных общеевропейских правил в соответствие с требованиями Европейской директивы по ЭП;

2. ЦПП, которые несут ответственность за проверку ЭП (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, и который будет предоставлять доступ к общим надёжным ресурсам, включая обзор ЦПП, способных установить соединение с определёнными ЦС (то есть РСДС). Не допускается, чтобы оператор действовал сам в качестве ЦПП, это может скомпрометировать его нейтральный (независимый) статус.

Функционально-структурная схема модели федеративной ИОК ЕС представлена на рисунке 3.15.

В данной модели, с функциональной точки зрения, владелец ИТСЭП мог бы отказаться от работы со всеми ЦПП и просто внедрить у себя прикладные программные модули для прямого взаимодействия с некоторыми ЦС, с которыми, как он полагает, его система будет взаимодействовать более эффективно и надёжно. Однако, владелец ИТСЭП, в конечном счёте, выберет взаимодействие с ЦПП с целью:

– либо упрощения работы по внедрению необходимого ПО (так как ему бы понадобилось обеспечить только соединение с одним ЦПП, а не с несколькими (возможно большим количеством) ЦС);

– либо увеличения числа взаимодействующих с ним ЦС (т.е. с целью увеличения числа своих потенциальных клиентов и сферы своего бизнеса);

– либо перехода на использование каких-либо дополнительных услуг, предоставляемых ЦПП (таких как семантическая совместимость или подтверждение исторической подлинности).

И решающим фактором в данной ситуации является то, что ЦПП функционируют на единой основе, позволяющей владельцам ИТСЭП использовать одиночный интерфейс («*одно окно*») для установления соединения с любым ЦПП, и позволяющей ЦПП соединяться с любым другим ЦПП, входящим в федеративную модель. На общеевропейском уровне было рекомендовано создание одной (единой) федерации, т.е. объединение национальных ЦПП и ЦС, так как одновременное существование нескольких федераций могло бы повлечь за собой риск, связанный с разделением рынка.

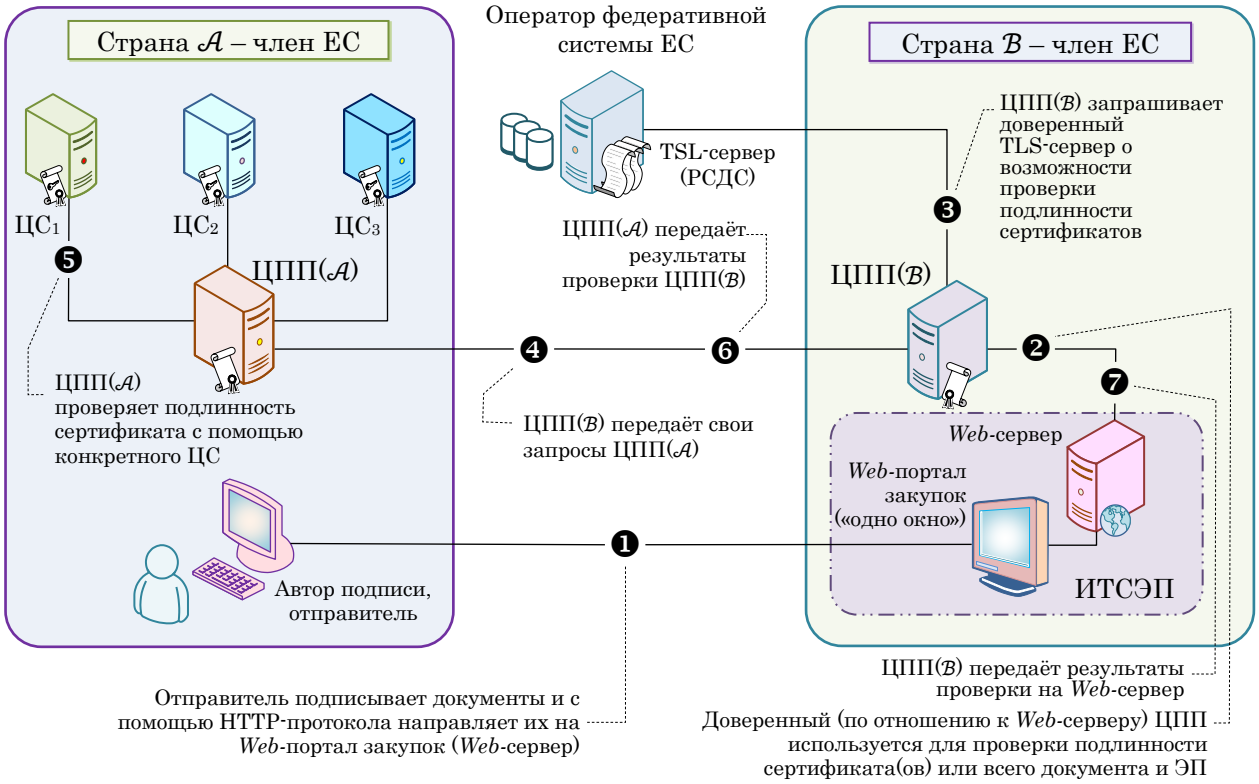

Рисунок 3.15 – Функционально-структурная схема модели федеративной ИОК Евросоюза

Таким образом, модель федеративной системы ИОК ЕС определила следующие основные требования: возможность объединённой проверки подлинности СЕРТ$_{ОК}$ и проверки ЭП с помощью ЦПП, основываясь на единых стандартах подтверждения подлинности, на согласованном внедрении этих стандартов, единых требованиях к качеству СЕРТ$_{ОК}$ и ЭП и на централизованной службе поиска доверенных ЦС и ЦПП с помощью оператора федеративной системы.

В внутри ЕС предполагается, что законодательные и правовые аспекты модели федеративной системы проверки подлинности СЕРТ$_{ОК}$ и ЭП должны отражать следующие виды взаимоотношений между:

- ЦПП и их потребителями (является краеугольным камнем, определяющим жизнеспособность ЦПП-бизнеса);

• ЦПП и ЦС (является ключевым с точки зрения организации бизнеса, он обеспечивает жизнеспособность ЦПП и надёжность для пользователей ЦПП);

• самими ЦПП в рамках федеративной ИОК ЕС (цель регулирование деятельности этого объединения, а также определения прав и обязанностей его участников).

3.7.3 Реестр состояния доверенных служб (услуг)

В 2016 году Европейским институтом по стандартизации в области электросвязи (*European Telecommunications Standards Institute*) был принят стандарт, устанавливающий формат и содержание РСДС [115]. Кроме того, в этом стандарте определены способы создания, определения местоположения, доступа и аутентификации РСДС, который предоставляет информацию о состоянии доверенных служб (услуг) с целью определения заинтересованными субъектами статуса доверенной службы (услуги), указанной в РСДС, в данный момент времени. Этот стандарт подлежит исполнению странами, являющимися членами ЕС.

Операторы систем подтверждения подлинности (СПП, *scheme operator*) других стран (не членов ЕС) или международных организаций с целью упрощения процедур взаимного признания ЭП могут выпускать РСДС в соответствии с указанным стандартом. Также, данный стандарт устанавливает требования в доверяющим субъектам при использовании ими РСДС и содержащейся в них информации о состоянии доверенных служб (услуг).

На рисунке 3.16 представлен общий формат и содержание РСДС.

3.7.3.1 Формат РСДС

РСДС должен издаваться только в XML-формате. Если оператор СПП или какой-либо другой субъект предоставляет средства для отображения одного РСДС в различных форматах, то одним из таких форматов обязательно должен быть XML-формат, который будет использоваться для отображения РСДС.

Во многих полях РСДС содержаться URI-идентификаторы [116], которые позволяют определить точное значение того или иного поля РСДС. Все поля, содержащие значения текущей даты и времени, должны удовлетворять следующим требованиям: (1) значения даты и времени должны иметь формат последовательности символов в соответствие с [117]; (2) значение даты и времени должно отображать *всеобщее скоординированное время* (*coordinated universal time*, UTC[29]). Это значение должно содержать год (четыре цифры), месяц, день, час, минуту, секунды (только целое число) и UTC-определитель «Z». Шкала UTC-времени представляет собой систему

[29] International Telecommunications Union, ITU-R TF.460 Standard-frequency and time-signal emissions, February 2002.

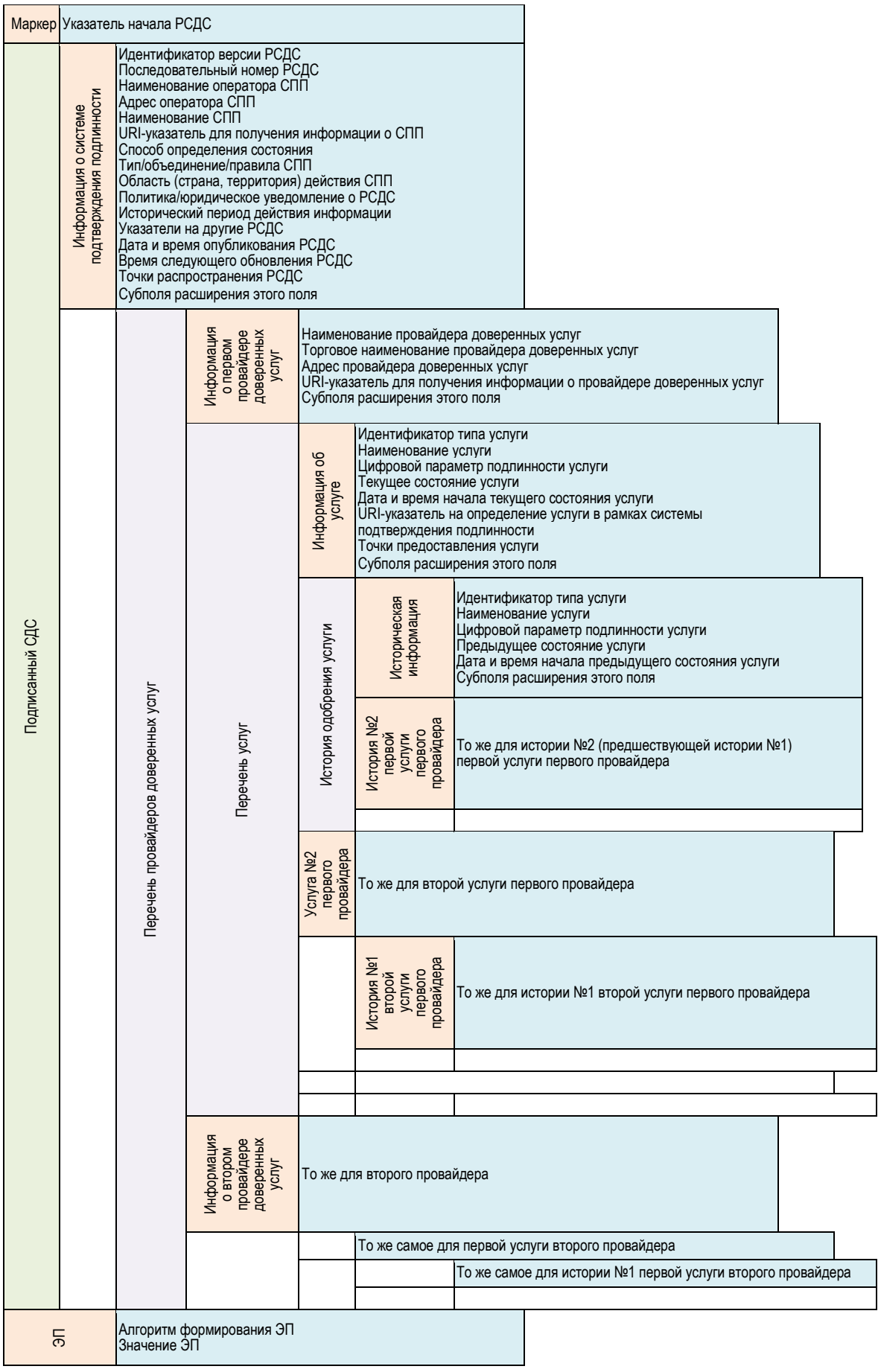

Рисунок 3.16 – Формат и содержание РСДС

отсчёта эталонного источника, в которой время выражается с помощью монотонно возрастающего значения бинарного счётчика с бесконечным числом битов.

Все РСДС должны издаваться, как минимум, на английском языке в соответствие с [118], а также могут издаваться на других (национальных) языках в кодировке UTF-8 [119].

3.7.3.2 Пример модели использования РСДС

Рассмотрим пример модели использования РСДС. Данная модель не вводит каких-либо ограничений на конкретную реализацию системы, использующей РСДС, но определяет основные функции, которые будут реализованы в системах, использующих такие РСДС. На рисунке 3.17 представлена модель использования РСДС с точки зрения подтверждения подлинности ЭП. Информация, содержащаяся в РСДС, может использоваться в процедуре (процессе) подтверждения подлинности маршрута сертификации следующим образом:

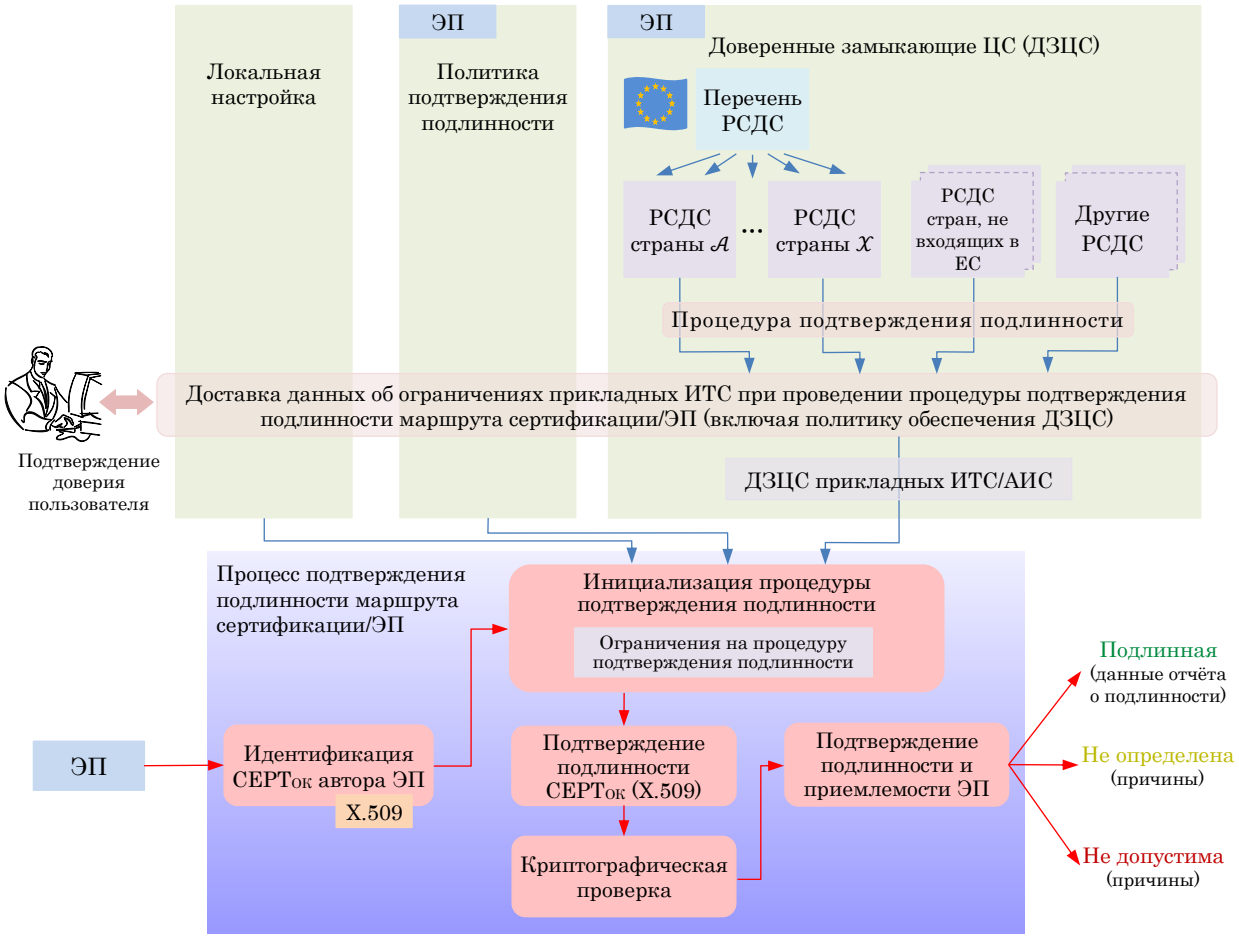

Рисунок 3.17 – Пример модели использования РСДС (перечня РСДС) с целью подтверждения подлинности ЭП

– подтверждение подлинности маршрута сертификации, основанном на проверке ЭП в соответствие с [15,17,120], требует информацию о СЕРТОК ЦС, которые могут быть использованы

прикладными ИТС/АИС, основанными на соответствующей доверенной службе, в качестве доверенных замыкающих ЦС (ДЗЦС, *trust anchor*);

– если в качестве ДЗЦС, с точки зрения проверки ЭП, для которой СЕРТ$_{ОК}$ подписывающего субъекта должен быть проверен на соответствие информации в РСДС, используются «цифровые идентификаторы службы», то в качестве информации о ДЗЦС необходимы только открытый ключ и связанное с ним имя субъекта. Если несколько СЕРТ$_{ОК}$ содержат открытый ключ, идентифицирующий службу, то они рассматриваются как СЕРТ$_{ОК}$ ДЗЦС, содержащие точно такую же информацию, которая необходима для определения ДЗЦС.

Необходимая информация может быть получена из одного или нескольких РСДС при выполнении следующих требований:

a) подлинность источника РСДС должна быть подтверждена с целью обеспечения гарантий того, что информация поступает от надёжного издателя (например, использование ЭП, подтверждение подлинности которой проводилось с помощью СЕРТ$_{ОК}$, полученного из известного ЦС);

b) данные (записи) о ЦС выбираются из РСДС на основе правил, установленных соответствующей политикой обеспечения доверия;

c) СЕРТ$_{ОК}$ ЦС из выбранных записей, к которым прикреплены дополнительные метаданные, хранятся вместе с ДЗЦС;

d) РСДС проверятся на регулярной основе с целью определения изменений состояния предоставляющих услуги ЦС, которые были ранее загружены из РСДС в репозитарий ДЗЦС. Кроме того, РСДС должен проверятся на регулярной основе с целью обнаружения новых записей;

e) перед тем как в репозитарий ДЗЦС будет загружена новая запись, у пользователя или оператора должна быть запрошена необходимая информация с целью подтверждения изменений (обновлений);

f) информация о ЦС из нескольких РСДС должна быть загружена в репозитарий ДЗЦС.

Информация о ЦС из РСДС может быть объединена с информацией о ЦС, хранящейся в репозитарии ДЗЦС или в любой другом хранилище СЕРТ$_{ОК}$ надёжных ЦС, с помощью различных способов, включая ручные или автоматизированные.

3.8 Проблемы и риски функционирования ИОК

Прежде чем издать цифровые СЕРТ$_{ОК}$ любой ЦС, относящийся к ИОК, обязан:

– проверить параметры подлинности пользователей ЦС;

– установить соответствующий (приемлемый) контент (содержание и структуру) цифровых СЕРТ$_{ОК}$;

– сформировать и распределить цифровые $СЕРТ_{ОК}$, а также гарантировать их доступность;

– гарантировать свою собственную внутреннюю безопасность.

Каждая из этих процедур повышает некоторые риски для привлекаемых участников информационного взаимодействия. Далее рассматриваются отдельные возможные уязвимости и риски, а также контрмеры, которые способствуют снижению или предотвращают распространение таких рисков.

ИОК могут характеризоваться, в первую очередь, как открытые или закрытые. Полностью закрытые инфраструктуры заключают контракты, которые содержат права и обязанности всех участников информационного взаимодействия при аутентификации сообщений (соединений) или электронных торговых операций (транзакций). Такой тип систем обеспечивает операторам ЦС значительное снижение рисков, так как, с точки зрения принятых обязательств, отсутствует какая-либо существенная неопределённость.

Соответственно, полностью открытые ИОК не заключают контракты, которые содержат права и обязанности всех участников информационного взаимодействия в конкретной системе. И в такой инфраструктуре, организации, которые реализуют основные направления деятельности и функции ЦС, могли бы иметь уязвимости и продемонстрировать весьма высокий уровень риска для каждого аутентифицированного сообщения (соединения) или каждой электронной торговой операции. Это подобно тому, когда на ранних стадиях своего развития большинство ИОК не были полностью открытыми или полностью закрытыми, контракты, определяющие права и обязанности пользователей инфраструктуры, заключались, по крайней мере, с некоторыми из них, а не со всеми.

3.8.1 Проверка параметров подлинности

Для подтверждения ПП конечного пользователя, ЦС анализирует, либо его полномочия в рамках самого ЦС, либо контракты с ЦР. Решение о передаче части своих функций и выборе ЦР вынуждает ЦС рисковать. Если ЦС или ЦР установил, что параметр подлинности является фальшивым или не совсем точным, то ЦС может понести ущерб от потери бизнеса или даже к нему могут быть применены меры юридического воздействия.

Более того, выпущенные в обращение этим ЦС сертификаты вообще могут стать сомнительными, если существует подозрение на недостаточный контроль при проверке параметров подлинности при издании сертификатов. Уровень риска, связанного с некачественной идентификацией конечного пользователя, может быть снижен тогда, когда ЦС издаёт цифровые сертификаты, которые будут использоваться только в рамках закрытой системы, так как существуют контракты между некоторыми или всеми пользователями системы.

Однако, некоторые ЦС «*перешли к другой крайности*», т.е. с целью предотвращения риска, связанного с выбором ЦР и взаимодействием с ним, они создали модель *удостоверяющего центра* (УЦ), состоящего из двух частей: ЦР и ЦС (модель «ЦР+ЦС» – это типичная ситуация для ИОК Российской Федерации). УЦ самостоятельно устанавливает и контролирует содержание $СЕРТ_{ОК}$, включая удалённый контроль ЦР по защищённому каналу связи. Другими словами, это резко снижает доверие к УЦ, так как он может осуществлять мошенническую сертификацию для достижения своих корыстных целей или в условиях давления криминальных структур. В такой ситуации уязвимым становиться пользователь этого УЦ (ИОК).

Модель «ЦР+ЦС» обладает намного более низким уровнем безопасности по сравнению с системой, в которой ЦС находится под контролем государственного ведомства. Модель «ЦР+ЦС» позволяет некоторому УЦ формировать содержание $СЕРТ_{ОК}$, фальсифицировать контент и издавать мошеннический $СЕРТ_{ОК}$.

Конечно, ЦС может подписать контракт, пообещав, что он не будет этого делать, тем не менее, это не исключает вероятности нарушения. Например, в Российской Федерации были вскрыты факты противоправной деятельности отдельных УЦ, от которой пострадали ни в чём неповинные граждане [3,41,143…146].

3.8.2 Содержание и структура сертификатов

Содержание и структура $СЕРТ_{ОК}$ варьируются в зависимости от конкретной ИОК. Содержание и структура, а также ограничения в $СЕРТ_{ОК}$ являются источником стратегического риска для ЦС, выпускающего $СЕРТ_{ОК}$. Стандартные $СЕРТ_{ОК}$ идентифицируют владельца сертификата и ЦС, выпустивший сертификат. Другим важным элементом стандартного $СЕРТ_{ОК}$ является срок его действия. Рекомендация ITU-T X.509 устанавливает жёсткие требования к содержанию и структуре $СЕРТ_{ОК}$. В частности, цифровые $СЕРТ_{ОК}$ должны содержать:

– уникальное имя ЦС, выпустившего (подписавшего) $СЕРТ_{ОК}$;

– последовательный номер, являющийся специфическим для ЦС, выпустившего (подписавшего) $СЕРТ_{ОК}$;

– идентификатор алгоритма формирования ЭП, используемого ЦС при подписании сертификата;

– срок действия $СЕРТ_{ОК}$.

С точки зрения безопасности $СЕРТ_{ОК}$ обладает физической и логической уязвимостями, которые являются следствием использования КПО, предназначенного для формирования ЭП. Чем дольше такое ПО используется, тем больше вероятность того, что, либо оно станет непригодным, либо нарушитель получит несанкционированный доступ.

Поле расширений СЕРТ$_{ОК}$ содержит дополнительную информацию, помимо параметра подлинности держателя сертификата и выпустившего сертификат ЦС. Такая дополнительная информация может включать предполагаемые ограничения при использовании СЕРТ$_{ОК}$, например, номер и тип транзакций или сообщений, которые имеют право подписывать конечные пользователи. Любое такое ограничение снижает риски, связанные с качеством осуществляемых транзакций и ухудшением репутации (снижением доверия) выпускающего сертификаты ЦС. Кроме того, ЦС может использовать поле расширения для определения классов цифровых СЕРТ$_{ОК}$, используемых в финансовых транзакциях или при доставке конфиденциальной информации. Такие СЕРТ$_{ОК}$ могут использоваться для одного сообщения или одной транзакции, или только при взаимодействии с конкретной стороной информационного обмена, или в условиях ограничения максимальных финансовых затрат.

3.8.3 Формирование и распределение сертификатов и их доступность

Процедуры формирования, распределения и документирования факта получения с СЕРТ$_{ОК}$ их владельцами «*преподносят*» ЦС дополнительные стратегические риски, связанные с проведением соответствующих транзакций и ухудшением репутации (понижением доверия). При формировании СЕРТ$_{ОК}$ причиной появления таких рисков является наличие возможных ошибок, возникающих в системах, что накладывает соответствующие ограничения на сертификацию, связанные с уникальными возможностями формирования ЭП каждым держателем СЕРТ$_{ОК}$. Появление рисков также зависит от политики и процедур контроля и управления процессом.

Распределение СЕРТ$_{ОК}$ и обеспечение их доступности очень часто не является сферой ответственности только лишь одного ЦС. Конечному пользователю также будет предоставляться технология формирования ЭП, либо поставщиком КПО, либо иной IT-компанией. Однако СЕРТ$_{ОК}$ не будет полностью сформирован, пока ЦС не удостоверится в способности пользователя осуществлять процедуру формирования своей собственной ЭП, чтобы внести соответствующую запись в СЕРТ$_{ОК}$. В закрытой системе ЦС, риски ЦС могут быть снижены за счёт заключения договоров, в которых будут указаны точные функции и обязанности взаимодействующих сторон. Некоторые риски, связанные с осуществлением транзакций, могут быть перенесены в головную организацию, на индивидуальных пользователей и взаимодействующие стороны, либо в другой субъект, обслуживающий базу данных, предназначенную для хранения СЕРТ$_{ОК}$. Тем не менее, ЦС по-прежнему могут иметь риски, связанные с ухудшением репутации (понижением доверия), если технологические проблемы присущи ЦС.

Как правило, цифровой СЕРТ$_{ОК}$ не будет «*дееспособным*» до тех пор, пока конечный пользователь не примет подписанный СЕРТ$_{ОК}$. Доступность СЕРТ$_{ОК}$ предполагает, что конечный пользователь соглашается с терминами и условиями, установленными ЦС, а также с любыми

специфическими условиями, которые затрагивают самого конечного пользователя. Ошибки, возникающие в процессе установления и поддержания соединения с конечными пользователями и влияющие на доступность, являются следствием, либо неадекватных политик и процедур, либо технических проблем. Такие ошибки являются причиной появления рисков, связанных с проведением ЦС соответствующих транзакций и ухудшением репутации самого ЦС.

3.8.4 Обеспечение цифровыми сертификатами

Когда ЦС издаёт СЕРТ$_{ОК}$, предназначенные для формирования ЭП конечными пользователями, как правило, он взаимодействует только с конечным пользователем, либо с его представителем, либо с посредником, действующими от имени пользователей. Однако, если ЦС, помимо основных функций, реализует функции репозитария (т.е. обеспечивает выпущенными в обращение СЕРТ$_{ОК}$), то ЦС будет взаимодействовать со сторонами информационного обмена, которые получили сообщения. Далее, с общих позиций, рассматриваются риски, связанные с предоставлением репозитарием услуг конечным пользователям и взаимодействующим сторонам. Существуют четыре основных аспекта обеспечения цифровыми СЕРТ$_{ОК}$:

– раскрытие информации о клиенте;

– поддержка и обслуживание конечных пользователей;

– приостановление действия и аннулирование СЕРТ$_{ОК}$;

– обработка запросов взаимодействующих сторон.

3.8.4.1 Раскрытие информации о клиенте

В настоящее время, ЦС, в условиях конкуренции, необходимо публиковать некоторую информацию об основных предоставляемых им услугах, а также правах и обязанностях конечных пользователей и взаимодействующих сторон. Природа раскрытия информации будет существенно влиять на уровень рисков, связанных с проведением ЦС соответствующих транзакций и ухудшением репутации самого ЦС. Например, если раскрытие информации явно предписывает ЦС на процедуры разрешения ошибок и политику конфиденциальности, то у части конечных пользователей может быть снижено число возможных не штатных ситуаций. Более того, если ЦС предоставляет техническую документацию по использованию КПО, связанного с сертификатами, то у конечных пользователей появляется возможность обнаружения своих внутренних проблем, вызванных не штатной работой КПО, а не штатным функционированием ЦС, которое приводит к возникновению рисков, приводящих, в свою очередь, к ухудшению репутации самого ЦС.

3.8.4.2 Поддержка и обслуживание конечных пользователей

С появлением большого числа новых информационных технологий, а также реализующих их КПО и услуг, от ЦС требуется соответствующая поддержка пользователей, что, в свою очередь, является источником рисков, которые ухудшают репутацию ЦС. ЦС может организовать «*службу технической поддержки*» или какую-либо иную форму непосредственного информационного обмена с конечными пользователями и взаимодействующими сторонами. Политики, процедуры и функционирование самой службы технической поддержки являются потенциальными источниками стратегических рисков, связанных с проведением ЦС соответствующих транзакций. Решение проблем или устранение ошибок, с которыми столкнулись конечные пользователи и взаимодействующие стороны вследствие «неграмотного» использования ими основных технологий, потребует от ЦС или поставщика клиентских услуг значительных ресурсов. Несмотря на то, что ЦС, как правило, не поддерживает КПО, предназначенный для формирования ЭП, могут возникнуть определённые обстоятельства, при которых конечные пользователи будут указывать ЦС на то, что все трудности связаны использованием информационных технологий.

У конечных пользователей могут возникнуть проблемы, вызванные некорректными настройками КПО в их компьютерных системах, и которые возможно не сразу «проявят себя», а проявятся лишь тогда, когда пользователи попытаются подписать сообщение или совокупность сообщений, переданных в период транзакции. Так как организация предоставляет услуги ЦС, то, в конце концов, можно запросить услугу по обеспечению взаимосвязи с клиентами. Предоставление такой услуги на практике может быть обеспечено клиентской службой, либо на основе внутренней экспертизы, либо на основе договора с внешней организацией, которая проведёт соответствующую экспертизу. В настоящее время, некоторые IT-компании предоставляют извлекаемые электронные накопители для хранения $СЕРТ_{ОК}$ конечных пользователей. Вместо загрузки КПО на жёсткий диск клиентского компьютера, последний может иметь USB-интерфейс для подключения извлекаемых электронных накопителей с целью загрузки данных о $СЕРТ_{ОК}$ конечного пользователя. Некоторые из рисков службы поддержки и обеспечения пользователей, связанные с проведением соответствующих транзакций и ухудшением репутации самой службы, могут быть существенно снижены за счёт простоты использования соответствующего программно-аппаратного комплекса (извлекаемого электронного накопителя), а не за счёт требования к владельцам компьютеров загрузить КПО из другого источника.

3.8.4.3 Приостановка действия и аннулирование сертификатов

Так как конечный пользователь несёт ответственность за обеспечение безопасности функции формирования ЭП, то существует реальная возможность того, что система будет скомпрометирована и появится реальная угроза несанкционированного доступа к ней. Таким образом, от ЦС может потребоваться приостановление действия или аннулирование $СЕРТ_{ОК}$. Если в ИОК не предусмотрен контроль и не предпринимаются какие-либо действия на регулярной основе, то ЦС может аутентифицировать поступающие сообщения или транзакции, использующие просроченные ЭП. Следовательно, ЦС, которые не осуществляют проверку подлинности (срока действия) цифровых $СЕРТ_{ОК}$ конечных пользователей, потенциально подвержены значительным стратегическим рискам, связанным с проведением соответствующих транзакций и ухудшением репутации (снижением доверия). Плохо проработанные политики и процедуры являются источником стратегического риска, а если они будут ещё и неправильно реализованы, то ЦС будет подвержен рискам, связанным с проведением соответствующих транзакций и ухудшением репутации (снижением доверия). Сроки необходимого обновления данных репозитария могут отличаться в зависимости от типа хранящихся $СЕРТ_{ОК}$. Задержка в приостановлении действия $СЕРТ_{ОК}$ используется в случае передачи уязвимых сообщений или проведении уязвимых транзакций, которые могут «*преподнести*» относительно высокие риски.

Цифровой $СЕРТ_{ОК}$ может проверяться на предмет его подлинности (срока действия) одним из двух способов. ЦС может аннулировать $СЕРТ_{ОК}$, если станет известно, что конечный пользователь скомпрометировал своё средство формирования ЭП. Наиболее вероятной причиной компрометации является то, что конечный пользователь не хранил свой закрытый ключ надлежащим образом, т.е. в защищённом виде. Если закрытый ключ пользователя стал известным, то нарушители (неавторизованные пользователи) могли бы подписывать передаваемые сообщения и последовательности сообщений в рамках осуществляемых транзакций. Если возник какой-либо вопрос о состоянии $СЕРТ_{ОК}$, то ЦС может приостановить действие $СЕРТ_{ОК}$ до тех пор, пока не будет установлен его статус. Риски, связанные с проведением соответствующих транзакций и ухудшением репутации (снижением доверия), могут быть следствием ошибок при обработке запросов относительно аннулирования и приостановления действия $СЕРТ_{ОК}$. Например, если конечный пользователь, чей $СЕРТ_{ОК}$ был ошибочно признан недействительным, лишился бы, таким образом, возможности подписывать сообщения, то он мог бы понести значительные материально-финансовые потери и возбудить судебный иск к ЦС, что неминуемо привело бы к потере репутации ЦС, как надёжного. И наоборот, репутация (доверие к) ЦС может пострадать, если взаимодействующая сторона признала бы сообщение или последовательность сообщений, переданных в период проведения транзакции, которые были подписаны конечным

пользователем, чей $СЕРТ_{ОК}$ должен быть аннулирован, или действие $СЕРТ_{ОК}$ должно быть приостановлено.

3.8.4.4 Обработка запросов взаимодействующих сторон

Появление значительных стратегических рисков, связанных с проведением определённых транзакций и ухудшением репутации (снижением доверия), вызвано обработкой запросов, поступающих от взаимодействующих сторон и касающихся состояния индивидуальных сертификатов. Несмотря на то, что взаимосвязи между ЦС и конечными пользователями, установленные на основе соответствующих договоров, могут определять обязанности конечных пользователей и других субъектов, такая «договорная защита» может быть совершенно бессильной при осуществлении транзакций между взаимодействующими сторонами в соответствующих открытых системах. Например, если ЦС предоставляет взаимодействующей стороне аннулированные $СЕРТ_{ОК}$ в качестве действующих, то ЦС может сразу потерять репутацию надёжного ЦС, либо «навлечёт на себя» судебный иск, что также приведёт к потере репутации (доверия). В открытых системах существуют и дополнительные риски, вызванные тем, что некоторые конечные пользователи или их группы меняются в течение срока действия используемых $СЕРТ_{ОК}$. Любые задержки в процессе обработки запросов на аннулирование $СЕРТ_{ОК}$, как правило, являются результатом применения неадекватных политик и процедур или технической обработки, которая последовала из-за наличия ошибок в политиках и процедурах. Если репозитарий осуществляет обработку запросов в пакетном режиме, являющимся альтернативой режиму реального времени, то уровень риска увеличивается ещё больше. Кроме того, число рисков может возрасти вследствие увеличения числа проводимых транзакций и $СЕРТ_{ОК}$, находящихся в обращении и имеющих различные ограничения и сроки действия.

3.8.4.5 Отзыв (аннулирование) сертификатов

Существуют два известных способа отправки ответов на запросы подлинности (сроке действия, состоянии) $СЕРТ_{ОК}$ конечного пользователя. Наиболее известный способ требует, чтобы репозитарий извлекал из памяти длинный список действующих сертификатов и СОС для проверки состояния одиночного $СЕРТ_{ОК}$. Неточности в СОС являются источником рисков, связанных с проведением определённых транзакций, для всей ИОК. Кроме того, установленная периодичность формирования СОС также влияет на степень риска самого репозитария. Более частое проведение процедуры обновления СОС приводит к снижению рисков, связанных с проведением ЦС определённых транзакций и ухудшением репутации самого ЦС. Также существует спорный вопрос относительно того, что предпочтительнее:

1. Данные о состоянии сертификата «*предоставляются*» (*push out*) самим репозитарием ЦС в интересах взаимодействующих сторон;

2. Данные о состоянии сертификата будут «*извлекаются*» *(pull from*) из репозитария этими взаимодействующими сторонами самостоятельно.

Каждому из способов присущи свои риски, связанные с проведением определённых транзакций и ухудшением репутации (снижением доверия). Второй способ позволяет репозитарию ЦС успешно «перекладывать» риски, связанные с ухудшением репутации (снижением доверия), на взаимодействующую сторону, что касается обеспечения доступа к действующему $СЕРТ_{ОК}$. С другой стороны, первый способ, и это очевидно, «перекладывает» всю ответственность на ЦС, особенно если СОС не точен или распространяется не своевременно. По причине наличия большего числа рисков и неэффективности затрат при реализации первого способа, IT-индустрия предпочитает второй способ. Некоторые IT-компании разработали КПО, который позволяет репозитарию в масштабе реального времени находить собственные записи для подтверждения подлинности одиночного $СЕРТ_{ОК}$. Другим источником рисков для репозитария, связанных с проведением определённых транзакций, является неспособность взаимодействующей стороны понимать поле расширений $СЕРТ_{ОК}$.

3.9 Проблемы и риски пользователей ИОК

Теперь рассмотрим проблемы и риски пользователей ИОК. Действительно, бизнес-модель на основе $СЕРТ_{ОК}$ – весьма привлекательна. Сами $СЕРТ_{ОК}$ – не дороги, и если ЦС способен убедить клиента купить годовой сертификат, то клиент, используя $СЕРТ_{ОК}$ в Интернет-сообществе, может получить достаточно большую годовую прибыль. А если разработчик КПО для ЦС способен убедить предпринимателя приобрести частный ЦС и платить ему процент от стоимости каждого проданного $СЕРТ_{ОК}$, то такая компания разработчик ПО также будет иметь хорошую прибыль. И поэтому неудивительно, что так много компаний пытаются заработать на этом перспективном рынке. Учитывая, что на карту поставлены огромные прибыли, неудивительно, что поставщики ИОК-компонентов активно проводят рекламные и иные мероприятия по продвижению своих изделий на мировом рынке (и Российская Федерация здесь не исключение). Однако, реклама оставляет некоторые довольно простые вопросы без ответа.

Безопасность бизнеса – это цепь, а её прочность определяется самым слабым звеном. Безопасность любой ИТС, использующей ИОК (систему ЦС), основана на множестве каналов/линий связи, и не все из них имеют криптографическую защиту. А это имеет прямое отношение к пользователям ИОК.

Помогает ли система управления криптографической защитой на основе ИОК таким людям или попросту их игнорирует? Обосновано ли она полагается на честность или корректность

людей? Имеет ли это отношение к ИТС? А такие ИТС безопасны? Все они работают вместе в общем процессе? Процесс предназначен для обеспечения максимальной безопасности или просто для получения прибыли?

Каждый из этих вопросов может указывать на наличие рисков безопасности, которые необходимо нейтрализовать или понизить до приемлемого уровня. Очевиден и самый первый вопрос: «Нужна ли ИОК для электронной коммерции и систем предоставления электронных услуг?» С одной стороны, многие специалисты утверждают, что нужна. Но с другой стороны, все мы являемся свидетелями, что электронная коммерция и системы предоставления электронных услуг уже процветают, и никаких ИОК нет. Интернет-магазины (*Web*-сайты) принимают заказы у клиентов независимо есть или нет у них сертификаты.

Рассмотрим два противоречивых примера. В первом примере, покупатель может заказать много товаров Интернет-магазине, предварительно не оплачивая эти товары, а также их доставку. Интернет-магазин самостоятельно или через коммерческую службу доставки отправляет заказанные товары покупателю в надежде, что покупатель оплатит товары. Но по прибытии курьера Интернет-магазина или коммерческой службы доставки к покупателю (по указанному адресу) последний отказывается от приобретения товаров и даёт курьеру «*от ворот поворот*». В результате, Интернет-магазин понесёт убытки, связанные с получением товаров на складе, их доставкой по адресу покупателю и возврату их на склад. На лицо – классический пример отказа от *принципа неотказуемости*. Интернет-магазин не сможет сформировать необходимые доказательства ущерба, принесённого недобросовестным покупателем, либо затраты на формирование такого доказательства значительно превысят понесённый ущерб.

Во втором примере, Интернет-магазин после заказа товаров покупателем желает проверить его платёжеспособность и запрашивает данные его кредитной или дебетовой карты. Очевидно, что покупатель не знает реальный уровень защищённости сквозного виртуального соединения между его компьютером и *Web*-сайтом Интернет-магазина, и поэтому возникает риск утечки его персональных данных, включая номер и срок действия кредитной или дебетовой карты покупателя. А с другой стороны, если угроза кражи денег с кредитной или дебетовой карты покупателя будет реализована злоумышленником, то репутация Интернет-магазина может резко снизится, вплоть до потери бизнеса.

Таким образом, правы те, кто утверждает, что системы электронной коммерции и предоставления электронных услуг нуждаются в ИОК. Но использование ИОК должно быть тщательно продуманным и учитывать все возможные риски, с которыми могут столкнуться системы электронной коммерции и предоставления электронных услуг (включая государственные).

На рисунке 3.18 представлен пример взаимодействия двух субъектов с использованием ассиметричной криптографической системы, на котором буквами обозначены возможные атаки

(часть атак) злоумышленников, связанные с нарушением процедур аутентификации, обеспечения целостности и раскрытием информации, а именно:

A. Кто-то мог провести атаку, используя компьютер Томы;

B. Кто-то мог показать ей один документ, чтобы получить её согласие на ЭП, а затем отправить другой документ для подписания;

C. Кто-то мог украсть ключи Томы из её компьютера или украсть пароль для доступа к её ключам;

D. Кто-то мог попытаться атаковать криптографически защищённый канал (но, скорее всего, так атаковать не стоит, потому что есть много других способов);

E. Кто-то мог заменить ключ Томы на свой собственный. Если ключ Томы защищён сертификатом, то злоумышленник может заменить ключ в корневом сертификате и выпустить новые сертификаты для своего собственного ключа;

F. Кто-то мог солгать Мише о том, что ЭП была проверена.

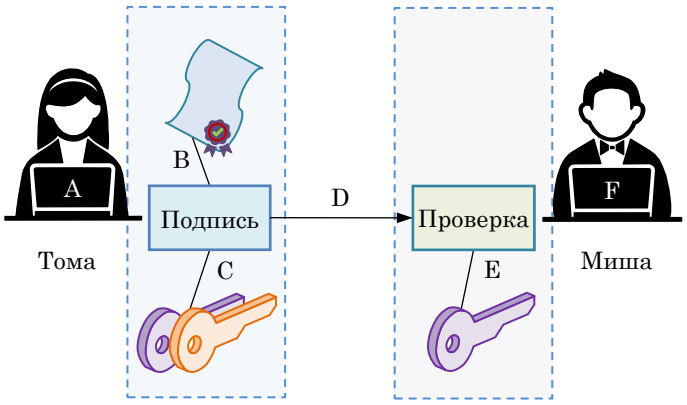

Рисунок 3.18 – Пример информационного взаимодействия на основе асимметричной криптографической системы

Следует заметить, что маршрут доставки сообщений включает несколько каналов связи (виртуальных соединений), которые не защищены с помощью криптографии. Такие каналы связи могут контролироваться злоумышленником с целью заставить Мишу признать ложное сообщение, которое на самом деле было отправлено не Томой, или, по крайней мере, не то сообщение, что она намеревалась отправить.

3.9.1 Кому или чему доверяют пользователи ИОК?

Существует проблема неточного использования слова «доверие». Очень часто, ЦС считают «*доверенным*». С точки зрения криптографии, это всего лишь означает, что ЦС корректно

использует свои закрытые ключи. И это вовсе не означает, что пользователю необходимо доверять СЕРТ$_{ОК}$ этого ЦС в некотором конкретном случае, например, при проведении микроплатёжной операции или подписании платёжного чека на сумму 10 млн. руб.

ЦС могут написать обстоятельные и качественные ОДС, в которых ЦС, фактически, отказываются от какой-либо ответственности за СЕРТ$_{ОК}$, используемые в какой-либо сфере. После выпуска таких ОДС они функционируют штатно, но это вовсе не означает, что СЕРТ$_{ОК}$, выпущенному ЦС для ИТС, можно доверять.

3.9.2 Кто использует ключ пользователя ИОК?

Один из значительных рисков в ИОК связан с собственным предназначенным для формирования ЭП закрытым ключом владельца СЕРТ$_{ОК}$. Как он его защищает? Пользователь ИОК почти наверняка не владеет защищённой вычислительной системой со средствами СКУД, средствами защиты от побочных электромагнитных излучений и наводок (ПЭМИН) и от распространения акустических сигналов, а также иными средствами технической защиты. Он, как правило, хранит свой закрытый ключ на обычном (домашнем или офисном) компьютере. Так вот, компьютер подвергается атакам нарушителей, которые пытаются внедрить в него вирусные и другие вредоносные программы. Даже если закрытый ключ храниться в его компьютере пользователя ИОК в защищённом режиме (формате), то возникает следующий вопрос, а находится ли его компьютер в охраняемой комнате с системой видеонаблюдения, чтобы он знал, что никто иной, кроме него, никогда не пользуется его закрытым ключом? Если доступ в компьютер защищён паролем, то насколько сложно вскрыть такой пароль? Если закрытый ключ пользователя ИОК храниться в извлекаемом электронном устройстве памяти (накопителе), то насколько оно устойчиво к атакам или кражам? [Большинство – очень уязвимо.] Если ключ хранится в надёжно защищённом от атак устройстве, то может ли заражённый компьютер заставить надёжное устройство подписать то, что пользователь ИОК не собирался подписывать?

Это имеет важное значение при использовании термина «неотказуемость». Как и «доверенный», этот термин относится к криптографии и теории обеспечения ИБ. В данном случае он имеет вполне конкретное значение, т.е. алгоритм цифровой подписи надёжен и его невозможно «взломать», и поэтому злоумышленник не может подделать ЭП владельца СЕРТ$_{ОК}$. С юридической точки зрения, если закрытый ключ владельца СЕРТ$_{ОК}$, предназначенный для формирования ЭП, был сертифицирован аккредитованным ЦС, то владелец СЕРТ$_{ОК}$ несёт ответственность за всё, что сформировано с помощью этого закрытого ключа. Неважно, кто был за клавиатурой компьютера или какой вирус сформировал ЭП – владелец СЕРТ$_{ОК}$ несёт юридическую ответственность.

Известно, что цель обеспечения неотказуемости заключается в сборе, обработке, обеспечении доступности и признании неопровержимости доказательства[30] (свидетельства) относительно заявленного события или действия с целью урегулирования споров о произошедшем или не произошедшем событии или действии [96]. В данном случае, речь идёт об ЭП, как доказательстве соответствующего события или действия. И поэтому, например, многомиллионная электронная торговая сделка (транзакция) с использованием ЭП взаимодействующих сторон должна быть подписана (заверена) ДТС, т.е. третьей стороной, которой доверяют оба участника транзакции.

Очевидно, что ИОК напрямую не обеспечивает неотказуемость, но она необходима при формировании доказательства (свидетельства) относительно заявленного события или действия (транзакции).

3.9.3 Каков уровень защищённости проверяющего компьютера?

В §3.9.2 было показано, что компьютер, в котором хранится или обрабатывается закрытый ключ владельца $СЕРТ_{ОК}$, должен быть защищён. Длинные ключи не повышают уровень защищённости системы, потому что общая защищённость системы ниже, чем самый незащищённый компонент системы. Тоже самое относится и к проверяющему компьютеру – компьютеру, который использует $СЕРТ_{ОК}$.

При проверке $СЕРТ_{ОК}$ не используется закрытый ключ, а используются открытые ключи. Таким образом, нет никаких конфиденциальных данных, подлежащих защите. Тем не менее, при такой проверке используется один или несколько «корневых» открытых ключей. Если злоумышленник может добавить свой собственный ключ в указанный перечень, то он сможет выпускать свои собственные $СЕРТ_{ОК}$, которые будут восприниматься точно также, как и законные $СЕРТ_{ОК}$. Они могут даже совпадать с законными $СЕРТ_{ОК}$ во всех полях, за исключением одного, они будут содержать открытый ключ злоумышленника вместо законного владельца $СЕРТ_{ОК}$.

Не поможет и хранение таких корневых ключей в «корневых сертификатах». Такие владельца $СЕРТ_{ОК}$ являются самоподписанными и не повышают уровень защищённости. Единственный ответ – проводить полную проверку владельца $СЕРТ_{ОК}$ в компьютерной системе, которая способна парировать попытки внедрения вредоносного программного обеспечения (ВПО) или физического вмешательства.

[30] Доказательство (свидетельство) представляет собой информацию, которая, либо самостоятельно, либо в сочетании с другой информацией может использоваться для урегулирования (разрешения) спора.

3.9.4 Кто такой Иван Иванович Иванов?

Как правило, $СЕРТ_{ОК}$ связывают открытый ключ и именем его владельца, но мало кто говорит насколько полезна такая криптосвязка. Представим себе, что субъект $\mathcal{A}$ (пользователь ИОК) получил $СЕРТ_{ОК}$ Ивана Ивановича Иванова. Субъект $\mathcal{A}$ может знать только одного Ивана Ивановича Иванова, но сколько Иванов Ивановичей Ивановых знает ЦС? Как установить, что если получен соответствующий $СЕРТ_{ОК}$ Ивана Ивановича Иванова, то – это $СЕРТ_{ОК}$ друга субъекта $\mathcal{A}$. Субъект $\mathcal{A}$ мог получить его открытый ключ лично или проверить его лично (например, *PGP*-инфраструктура позволяет это [101…103]), но, скорее всего, он получил $СЕРТ_{ОК}$ по электронной почте и просто полагает, что это реальный Иван Иванович Иванов. Общее имя (поле «*commonName*») $СЕРТ_{ОК}$, вероятнее всего, будет расширено за счёт некоторой другой информации, чтобы оно стало уникальным среди имён, указанных в $СЕРТ_{ОК}$, выпущенных ЦС друга субъекта $\mathcal{A}$. А субъект $\mathcal{A}$ знает какую-либо иную информацию о своём друге? А субъект $\mathcal{A}$ знает какой ЦС должен издать $СЕРТ_{ОК}$ для его друга?

Криптография с открытым ключом предусматривает, в том числе, использование СЕК, в которой можно найти $СЕРТ_{ОК}$. Если бы субъект $\mathcal{A}$ захотел найти $СЕРТ_{ОК}$ Ивана Ивановича Иванова, то он мог бы его найти в СЕК-сервере, а затем, получив его открытый ключ, отправить ему зашифрованное с помощью открытого ключа сообщение.

Очевидно, что при поиске $СЕРТ_{ОК}$ в СЕК-службе глобальной Интернет-сети [99] могут возникнуть риски, связанные с получением $СЕРТ_{ОК}$ не того субъекта, с которым необходимо провести транзакцию. Поэтому решение такой проблемы – предварительный обмен $СЕРТ_{ОК}$ с последующей проверкой их подлинности взаимодействующими сторонами.

Выводы по Главе 3

1. В первой части данной главы рассмотрены основные различия между бумажным и электронным документооборотом. Показано, что электронные и бумажные документы способны выполнять абсолютно разные функции в юриспруденции и бизнесе. Электронные сообщения не являются уникальными, так как можно сделать любое количество дубликатов (копий), ничем не отличающихся от оригинала. Данное свойство электронных документов вступает в прямое противоречие со свойством бумажных документов, которые специально защищают от копирования. Другими словами, в реальной жизни БДО невозможно полностью отобразить в ЭДО. Тем не менее, это не исключает дальнейшего поиска реальных функциональных аналогов, учитывая уникальные свойства передачи дискретных сообщений.

Также показано, что глобальная информатизация позволила «перевести» БДО в ИТС, реализующие ЭДО («на электронные рельсы»), а инфраструктура открытых ключей способна их ускорить и упростить. Современные «электронные коммерческие системы и системы предоставления услуг» зависят от целостности и подлинности данных. Эти оба свойства данных могут быть реализованы ИОК на основе привязки ЭП к автору ЭП (физическому лицу, гражданину) и обеспечения гарантий того, что ЭП не может быть подделана (сфальсифицирована). Вместе с тем, ИОК-технология может обеспечить шифрование данных, чтобы гарантировать их конфиденциальность. Необходимо отметить, что при предоставлении услуг и проведении коммерческих транзакций (электронных процедур) должны быть реализованы, как минимум, следующие четыре основные услуги (службы) обеспечения безопасности: обеспечение целостности, конфиденциальности, неотказуемости, а также процедуры идентификации и аутентификации. Кроме того, к наиболее важным дополнительным ИОК-услугам относятся восстановление ключа и авторизация (определение прав доступа).

Далее рассмотрены организация и компоненты ИОК. Под инфраструктурой открытых ключей понимается совокупность КПО, технологий шифрования и служб, которые способны в интересах организаций обеспечить защиту линий и каналов связи и электронных коммерческих сделок, осуществляемых с использованием сетей передачи данных. ИОК привязывает открытые криптографические ключи к субъектам, позволяет другим субъектам проверять привязки открытых ключей и предоставляет услуги, которые необходимы при проведении соответствующих процедур обеспечения ключами в распределённой ИТС.

Функциональными элементами ИОК являются: центры сертификации (включая центры атрибутных сертификатов), центры (пункты) регистрации, репозитарии и архивы. Далее описаны основные задачи, решаемые этими элементами ИОК.

2. Во второй части данной главы рассмотрены основные архитектуры ИОК, а также форматы данных, используемых в ИОК. Показано, что владельцы $СЕРТ_{ОК}$ получают свои сертификаты в различных ЦС, в зависимости от организации или сообщества, членами которых они являются. Современные ИОК, как правило, состоит из нескольких ЦС, которые связаны между собой надёжными маршрутами доставки данных (информационного взаимодействия). Получатели подписанного сообщения, которые не взаимодействуют с ЦС, выпустившим $СЕРТ_{ОК}$ для отправителя сообщения, могут также проверить (подтвердить) подлинность $СЕРТ_{ОК}$ отправителя путём поиска маршрута между ЦС, обслуживающим получателя подписанного сообщения, и ЦС, который выдал $СЕРТ_{ОК}$ отправителю. Существуют две общепринятые используемые в организациях ИОК-архитектуры, которые обеспечивают такую проверку (подтверждение) подлинности $СЕРТ_{ОК}$: иерархическая и сетевая.

В случае иерархической архитектуры, ЦС «выстраиваются иерархически» под корневым ЦС, который выпускает $СЕРТ_{ОК}$ для «подчинённых» ЦС. Последние могут выпускать $СЕРТ_{ОК}$ для своих «подчинённых» ЦС или для пользователей. В иерархической ИОК-архитектуре каждая проверяющая сторона знает открытый ключ корневого ЦС. Любой $СЕРТ_{ОК}$ может быть проверен путём проверки маршрута сертификации, состоящего из $СЕРТ_{ОК}$, начиная с сертификата корневого ЦС. В случае сетевой архитектуры, независимые ЦС взаимно сертифицируются каждый с каждым (т.е. выпускают и доставляют $СЕРТ_{ОК}$ друг другу), в результате чего формируется сеть доверенных связей между «равноправными» ЦС.

Далее рассматриваются современные типы ИОК-архитектур, к которым относятся «строгая иерархия», «общая иерархия», «произвольная структура», «изолированные иерархии» и «взаимно-сертифицированные иерархии».

Далее проанализированы форматы данных, используемые в ИОК, а именно сертификат открытого ключа ($СЕРТ_{ОК}$), список отозванных (аннулированных) сертификатов (СОС) и атрибутный сертификат $СЕРТ_{АТ}$, который может использоваться в качестве дополнительного сертификата.

3. В третьей части данной главы рассмотрены североамериканская и западноевропейская модели организации ИОК.

Создание и развитие национальной ИОК в США было обусловлено принятием двух важнейших государственных законодательных актов: «Закон о мобильности и подотчётности в здравоохранении», принятый в 1996 году, и который требовал, в том числе, создания национальных стандартов для ЭДО в здравоохранении и общих идентификаторов для поставщиков услуг медицинского страхования и работодателей; «Закон о прекращении БДО в правительстве», принятый в 1998 году, и который требовал, чтобы за 5 лет система предоставления информации (услуг) гражданам федеральными органами исполнительной власти и службами, а также все процедуры были переведены в электронный формат (ЭДО), кроме того он устанавливал юридический статус ЭП, и обязывал ведомства внедрить процедуры электронной аутентификации.

Далее рассмотрен состав участников национальной ИОК США. К органам управления национальной ИОК США относятся: федеральный совет IT-директоров; федеральный центр разработки и реализации политики развития национальной ИОК; федеральный центр обеспечения и регулирования национальной ИОК и руководитель программ в составе этого центра; центр реализации политики сертификации; центры сертификации; и серверы, предоставляющие информацию о состоянии сертификатов. Кроме того, в состав участников национальной ИОК входят центры регистрации, доверенные субъекты, пользователи, доверяющие стороны и другие участники.

Также показано, что модель доверия национальной ИОК США представляет собой архитектуру на основе СЦС и предназначена для взаимодействия ИОК организаций и ведомств, невзирая на их архитектуры. Единственное целевое предназначение СЦС – формирование доверенных взаимосвязей между ИОК организаций и ведомств.

Далее рассмотрена западноевропейская модель организации ИОК, а также основные концепции и иерархическая структура ИОК Европейского союза. В основе создания западноевропейской ИОК лежит основополагающий нормативный акт: «Директива Европейского парламента и Европейского совета от 13 декабря 1999 года об Основах объединения электронных подписей». ИОК ЕС оценивают, как основу создания электронного правительства и электронного бизнеса в Евросоюзе. Необходимость издания нормативного акта вызвана тем, что национальные ИОК европейских стран создавались и совершенствовались по образцу североамериканской модели ИОК. Однако наличие в ЕС более 20 государственных языков потребовало от Еврокомиссии формирования новых концепций при создании и развитии единой (федеративной) модели ИОК. Такими концепциями являются: ЦПП и РСДС.

Одной из основных услуг ЦПП, которая предоставляется его пользователям, является проверка подлинности $СЕРТ_{ОК}$ в режиме «одного окна». Другой важнейшей услугой, предоставляемой ЦПП, является проверка подлинности ЭП: грамматико-синтаксический анализ и математическая проверка ЭП. На ЦПП могут возлагаться и дополнительные функции: извлечение информации о владельцах $СЕРТ_{ОК}$ X.509v3 и проведение их семантической обработки с целью обеспечения трансграничной функциональной совместимости ЭП; проведение проверки на предмет исторической подлинности $СЕРТ_{ОК}$ и ЭП.

Модель федеративной ИОК ЕС, в широком смысле, включает следующих участников: ЦС, которые выдают $СЕРТ_{ОК}$; ЦПП, которые несут ответственность за проверку ЭП (и, следовательно, за проверку подлинности $СЕРТ_{ОК}$) по отношению к своим потребителям; оператор федерации (орган в рамках Еврокомиссии), который вводит единые правила, чтобы ЦПП, входящие в федерацию, были под контролем, и который будет предоставлять доступ к общим надёжным ресурсам. Данная модель определила следующие основные требования: возможность объединённой проверки подлинности $СЕРТ_{ОК}$ и проверки ЭП с помощью ЦПП, основываясь на единых стандартах подтверждения подлинности, на согласованном внедрении этих стандартов, единых требованиях к качеству $СЕРТ_{ОК}$ и ЭП и на централизованной службе поиска доверенных ЦС и ЦПП с помощью оператора федеративной системы. Также рассмотрен пример модели использования РСДС.

4. В четвёртой части данной главы проанализированы проблемы и риски функционирования ИОК, а также проблемы и риски пользователей ИОК.

В работе показано, что уровень риска, связанного с некачественной идентификацией конечного пользователя, может быть снижен тогда, когда ЦС издаёт цифровые сертификаты, которые будут использоваться только в рамках закрытой системы, так как существуют контракты между некоторыми или всеми пользователями системы. Однако, некоторые ЦС «перешли к другой крайности», т.е. они создали модель УЦ, состоящего из двух частей: ЦР и ЦС (модель «ЦР+ЦС» – это типичная ситуация для ИОК в Российской Федерации). УЦ самостоятельно устанавливает и контролирует содержание $СЕРТ_{ОК}$, что резко снижает доверие к УЦ, так как он может осуществлять мошенническую сертификацию для достижения своих корыстных целей или в условиях давления криминальных структур. В такой ситуации уязвимым становиться пользователь этого УЦ (ИОК).

Кроме того, с точки зрения безопасности, $СЕРТ_{ОК}$ обладает физической и логической уязвимостями, которые являются следствием использования КПО, предназначенного для формирования ЭП. И чем дольше такой КПО используется, тем больше вероятность того, что, либо он станет непригодным, либо нарушитель получит несанкционированный доступ к нему.

Далее рассмотрены дополнительные стратегические риски, связанные с проведением соответствующих транзакций и ухудшением репутации (снижением доверия), которые связаны с процедурами формирования, распределения и документирования факта получения владельцами своих $СЕРТ_{ОК}$. Доступность $СЕРТ_{ОК}$ предполагает, что конечный пользователь соглашается с терминами и условиями, установленными ЦС, а также с любыми специфическими условиями, которые затрагивают самого конечного пользователя. Ошибки, возникающие в процессе установления и поддержания соединения с конечными пользователями и влияющие на доступность, являются следствием, либо неадекватных политик и процедур, либо технических проблем.

Также, с общих позиций, рассматриваются риски, связанные с предоставлением репозитарием услуг конечным пользователям и взаимодействующим сторонам, а именно: раскрытие информации о клиенте; поддержка и обслуживание конечных пользователей; приостановление действия и аннулирование $СЕРТ_{ОК}$ и обработка запросов взаимодействующих сторон.

Показано, что безопасность бизнеса – это цепь, а её прочность определяется самым слабым звеном. Безопасность любой ИТС, использующей КЗСУ на основе ИОК (систему ЦС), основана на множестве каналов/линий связи, и не все из них обеспечивают конфиденциальность данных. А это имеет прямое отношение к пользователям ИОК. Кроме того, сделан вывод, что системы электронной коммерции и предоставления электронных услуг нуждаются в ИОК. Но использование ИОК должно быть тщательно продуманным и учитывать все возможные риски, с которыми могут столкнуться ИТС, включающие системы электронной коммерции и предоставления электронных услуг (в том числе и государственные), а также сами пользователи ИОК.

Глава 4 МОДЕЛИ ДОВЕРИЯ НА ОСНОВЕ ИОК

ИОК можно представить, как совокупность технологий, процедур и политик распространения доверия из системы, в которой оно уже существует, в другие системы, в которых оно необходимо при проведении интерактивной процедуры аутентификации. То, как происходит распространение доверия через конкретные ИОК, зависит от синтаксической структуры доверия самой ИОК, которая, как правило, именуется *моделью доверия*. Однако доверие – это прежде всего семантическое понятие, которое не может быть выражено только в синтаксических терминах. Кроме того, для описания характеристик наиболее важных моделей доверия на основе ИОК необходимо учитывать семантические допущения и человеческое восприятие доверительных отношений, а также, как всё это отражено (т.е. в явном или неявном виде) в политиках сертификации, правовых договорных соглашениях между участниками ИОК, и учитывать то, как информация о ПП отображается на дисплеях компьютерах и в каком она формате. Некоторые из всего многообразия моделей доверия на основе ИОК, описанных в научно-технической литературе, уже реализованы и в настоящее время используются в практических целях, начиная от небольших локальных (корпоративных) сетей, и кончая большими масштабируемыми закрытыми и открытыми сетями, например, Интернет-сеть.

4.1 Системы обеспечения параметрами подлинности

Одним из фундаментальных понятий, используемых в системах аутентификации на основе ИОК, является ПП. ПП – это уникальное свойство (признак) любого субъекта (объекта), которое подтверждает (свидетельствует о) его уникальность(и) или схожесть(и) с самим собой и делает его отличным от других субъектов (объектов) в определённой ИТС.

Наличие возможности отображать и распознавать объекты в компьютерных сетях имеет основополагающее значение для систем электронного взаимодействия и сотрудничества, и является функциональным фундаментом практически всех систем обеспечения безопасности, например, системы авторизации и управления доступом, а также обеспечения репутации. В простейшем случае, когда группа пользователей обращается к одному поставщику услуг (ПЭУ), современная система управления доступом позволяет пользователям идентифицировать себя с помощью *уникальных идентификаторов* (УИД) и аутентифицировать себя с помощью *параметров для аутентификации*, например, паролей. В такой модели требования к доверию между пользователем и ПЭУ хорошо отображаются в форме конкретных предположений об обеспечении безопасности и защите неприкосновенности. Необходимо отметить, что указанная модель используется уже несколько десятилетий, и пользователи знакомы с ней. В [121,122] она получила название *модель изолированного обеспечения ПП*

(изолированная система обеспечения ПП, СОПП), так как каждый идентификатор, которым владеет пользователь, может использоваться для доступа только к одной изолированной интерактивной службе (ПЭУ). Данная модель, которая используется всеми видами доступа к интерактивным службам и ресурсам, а также при обеспечении цифровых прав, относительно проста для ПЭУ, и быстро становится неприемлемой для пользователей. Стремительный рост числа интерактивных служб, основанных на такой модели, приводит к тому, что пользователям необходимо хранить большое число востребованных идентификаторов и параметров для аутентификации. По этой причине, а также с целью координации связанных услуг, предоставляемых различными ПЭУ, необходимы и должны быть реализованы новые модели обеспечения ПП. Некоторые из таких моделей имеют трудновыполнимые требования к обеспечению доверия, а некоторые пользователи не имеют достаточного опыта использования таких моделей. Ниже представлен анализ некоторых требований и проблем обеспечения доверия, вытекающих из различных моделей СОПП.

4.2 Субъекты/объекты, параметры подлинности и идентификаторы

ПП физического лица или организации включает индивидуальные параметры, с помощью которых можно распознать физическое лицо или организацию, или которые известны [121,122]. Такие характеристические параметры (признаки) *могут быть получены* тем или иным способом, и к ним относятся, например, имя, адрес, гражданство, регистрационные номера или членство в организации. Кроме того, характеристические параметры (признаки*) могут быть и неотъемлемыми*, например, биометрические параметры. Если речь идёт о ПП организации, то большинство характеристических параметров (признаков) должно рассматриваться как приобретённое.

Любой характеристический параметр в рамках ИТС представляется в формате атрибута (§3.4.1), который может быть идентификатором или именем, если он используется в процедуре идентификации. Предположим, что ПП – уникальны, т.е. два человека или две организации не могут иметь один и тот же ПП. Тем не менее, одно и то же физическое лицо или одна и та же организация могут иметь различные ПП в различных системах, а каждый ПП отображается с помощью различных групп атрибутов (идентификаторов/наименований). Тот или иной атрибут (идентификатор/имя), как правило, уникален только в границах конкретной ИТС. Различные типы атрибутов могут существенно различаться по своим характеристикам (составу) и могут быть временными или постоянными, неотъемлемыми или прикладные, выбираемыми самостоятельно или сформированные внешней организацией, интерпретируемые людьми, компьютерами или теми и другими и т.д. Пространство атрибутов (идентификаторов/наименований) должно выбираться с особой тщательностью, чтобы обеспечить гарантии того, что

присвоение каждого ПП одному субъекту (объекту) – уникально (взаимно-однозначно). Биометрические идентификаторы, как правило, не совсем адекватны для этой цели в условиях большой группы субъектов, а другие типы атрибутов могут не иметь подобных недостатков, но в других условиях. На рисунке 4.1 представлены взаимосвязи между атрибутами (идентификаторами/именами), ПП и субъектами (объектами).

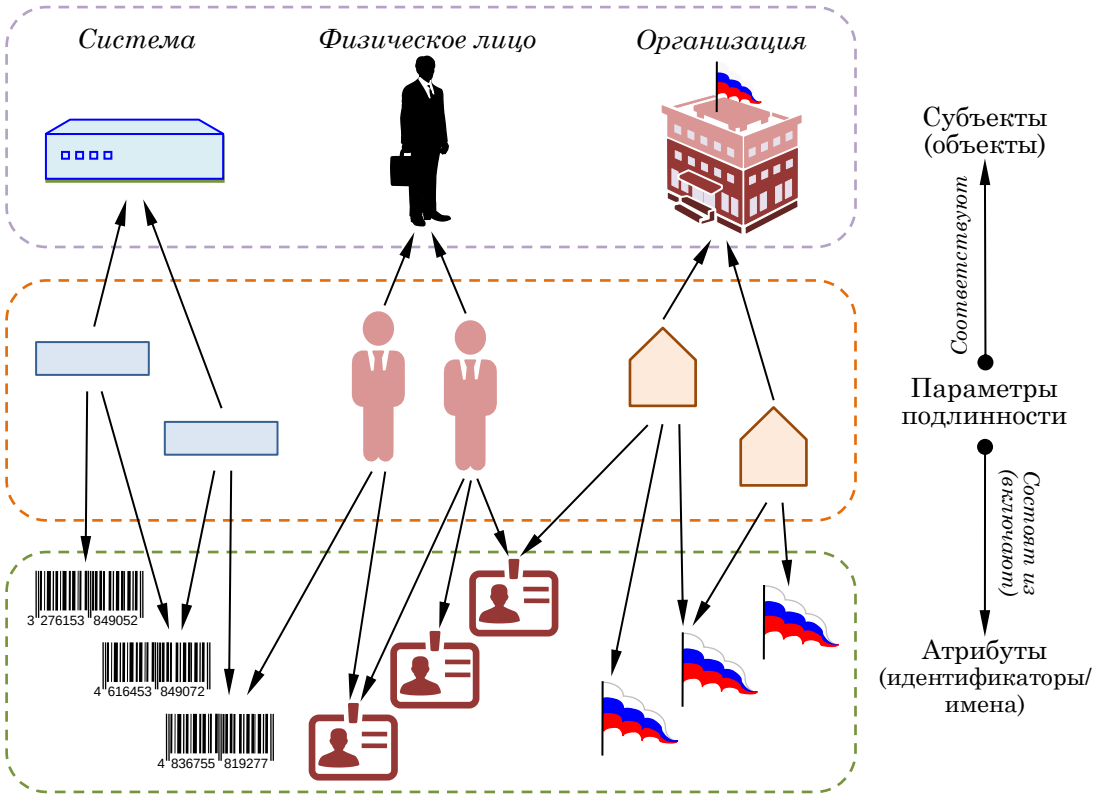

Рисунок 4.1 – Взаимосвязи между субъектами (объектами), ПП и атрибутами (идентификаторами/именами)

Группа атрибутов (идентификаторов/имён) больше группы ПП, которая, в свою очередь, больше группы субъектов (объектов), т.е. физических лиц или организаций, и систем. ПП можно рассматривать как уникальное подмножество атрибутов (идентификаторов/имён).

Цифровые ПП в ИТС также представляются в виде атрибутной модели, которая может включать идентификаторы, имена и параметры субъектов (объектов). Цифровой ПП, по своей сути, – форма представления ПП, которая является результатом кодового преобразования атрибутов и которая приемлема для обработки и отображения в ИТС. Возможные атрибуты ПП могут различаться, в зависимости от типа идентифицируемого субъекта (объекта). Например, дата рождения – часто используемый атрибут в интересах конкретных людей, но не для организаций. Компании очень часто используют отображающие их логотипы, а люди, как правило, нет.

Следует заметить, что с лингвистической точки зрения, различие между ПП и идентификатором весьма неоднозначно, и что термин «параметр подлинности» часто используется в качестве «идентификатора». Это довольно распространённое явление, когда ПП распознается с помощью одного УИД в конкретной системе. В дальнейшем, для устранения неоднозначности будем использовать понятия «параметр подлинности» и «идентификатор» раздельно, вкладывая в них разные смысловые значения.

4.3 Изолированная система обеспечения параметрами подлинности

4.3.1 Архитектура изолированной СОПП

В настоящее время ПЭУ выступают в роли поставщиков параметров для аутентификации и идентификаторов для своих клиентов одновременно. Они контролируют пространство имён в границах конкретного сетевого сегмента, в котором они предоставляют соответствующие интерактивный услуги, и назначают идентификаторы пользователям. Пользователь получает различные УИД от каждого ПЭУ, формирующего идентификаторы, чтобы взаимодействовать с ним. Кроме того, каждый пользователь будет обладать отдельными параметрами для аутентификации, например, паролями, каждый из которых привязан к соответствующему идентификатору (рисунок 4.2).

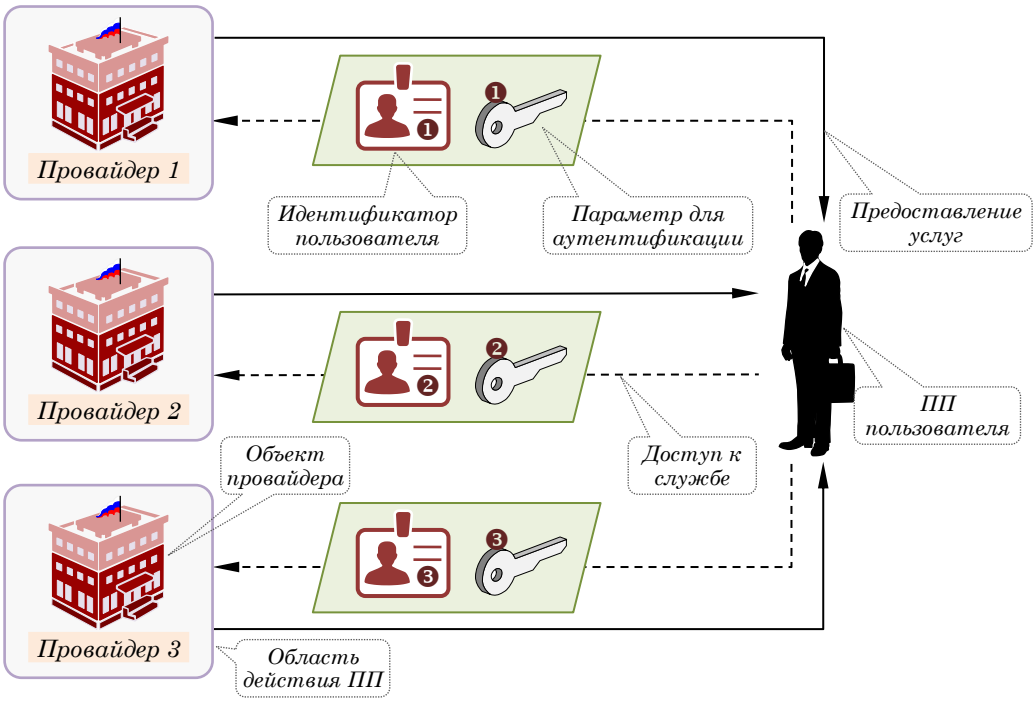

Рисунок 4.2 – Модель изолированной СОПП пользователей

На основе такой модели, с точки зрения ПЭУ, можно создать достаточно простую СОПП, но она будет весьма проблемной для пользователей, так как число ПЭУ, со службами

которых они взаимодействуют, стремительно растёт. Пользователи обычно забывают пароли доступа к тем интерактивным службам, которыми редко пользуются. Забытые пароли или страх забыть их создают значительный барьер для пользования службами, в результате чего такие интерактивные службы не способны «раскрыть» весь свой потенциал, т.е. показать свою востребованность и эффективность.

Если речь идёт о важных конфиденциальных службах, которые предусматривают восстановление паролей в защищённом режиме, то забытые пароли также могут значительно увеличить эксплуатационные (включая материально-финансовые) затраты ПЭУ.

4.3.2 Проблемы доверия в изолированной СОПП

Простота архитектуры изолированной СОПП позволяет относительно легко понять и решить связанные с ней проблемы доверия. Сложность доверия значительно упрощается, когда один и тот же субъект является ПЭУ, который одновременно формирует идентификаторы, параметры для аутентификации и предоставляет услуги. В таких условиях клиенту и ПЭУ необходимо доверять только друг другу при решении небольшого числа целевых задач.

Уровень надёжности (т.е. гарантированности) процессов и процедур, используемых при регистрации и аутентификации ПП, будет определяться ПЭУ в соответствии с результатами проведённого им анализа рисков и уязвимости предлагаемых услуг. Например, более надёжные способы, как правило, необходимы при предоставлении интерактивных банковских услуг, по сравнению с интерактивным доступом к электронной библиотеке. В частности, стандарты [123,124] устанавливают процедуры определения уровней надёжности способов аутентификации.

4.3.2.1 Доверие клиента к ПЭУ

Необходимость клиентов доверять ПЭУ более подробно рассматривается далее в §4.8. Вместе с тем, клиенту необходимы следующие виды доверия к ПЭУ:

Д1: *ПЭУ обеспечивает (защищает) неприкосновенность данных клиента*;

Д2: *ПЭУ внедрил удовлетворяющие пользователя процедуры регистрации и способы аутентификации (исходя из предположений клиента).*

Неспособность ПЭУ защитить персональные данные может вызвать у клиентов разочарования и дискомфорт. Неадекватные процедуры и способы аутентификации могут привести к ошибкам аутентификации, а также к финансовым потерям, как у ПЭУ, так и у клиентов. Под *ошибкой аутентификации* подразумевается событие, при котором неверно отображённый и некорректный идентификатор ошибочно определяется проверяющей стороной как

подлинный. Кроме того, это может означать, что законные пользователи не способны аутентифицировать сами себя, но такой тип ошибки аутентификации представляет меньший риск, чем первый тип.

Первый вид доверия Д1 может быть сформирован, например, на основе опубликованных политик обеспечения неприкосновенности, наличия истории их выполнения на практике и/или на основе стандарта *Web*-консорциума (*World Wide Web Consortium*) «P3P» [125][31]. Второй вид доверия Д2 формируется путём внедрения корректных процедур и способов, за счёт отображения истории, описывающей реальные случаи корректной аутентификации (без сбоев и ошибок), и снижения рисков клиентов на основе внедрения эффективных стратегий анализа и снижения рисков в случае фактических или предполагаемых потерь в результате мошенничества.

4.3.2.2 Доверие ПЭУ к клиенту

ПЭУ необходимо доверять клиенту, т.е.:

Д3: *Клиент обслуживает (хранит) свои параметры для аутентификации адекватным способом.*

Не надлежащее обслуживание (хранение) параметров для аутентификации может привести к их краже, что на практике может привести к ошибке аутентификации и краже ПП. В договорах об условиях обслуживания пользователей, как правило, отражено, что в случае кражи параметров для аутентификации ПЭУ всё бремя ответственности возлагают на клиентов. В таких случаях ПЭУ нет необходимости в доверии Д3. Вместо этого, клиент должен доверять себе с целью формирования доверия Д3, поскольку он несёт персональную ответственность в случае кражи ПП.

Доверие к клиентам Д3 может быть установлено на основе обеспечения гарантии того, что они выполняют рекомендуемые ПЭУ методики по обслуживанию (хранению) параметров для аутентификации, а также могут опубликовать историю взаимодействия с ПЭУ, которая отображает отсутствие каких-либо инцидентов безопасности.

[31] 30 августа 2018 года работа над этим документом прекращена.

4.4 Федеративная система обеспечения параметрами подлинности

4.4.1 Архитектура федеративной СОПП

Одна из целей федеративной СОПП – устранение недостатков, описанных в §4.3.1. Федеративная СОПП может рассматриваться как совокупность соглашений, стандартов и технологий, которая позволяет группе ПЭУ распознавать идентификаторы пользователей и права других ПЭУ внутри группы. Основная идея состоит в том, чтобы связать различные идентификаторы и, следовательно, соответствующие им ПП, принадлежащие одному и тому же пользователю, являющемуся клиентом нескольких ПЭУ, и позволить пользователю аутентифицироваться с помощью одного идентификатора у одного из ПЭУ, и, таким образом, считаться прошедшим процедуры идентификации и аутентификации у всех других ПЭУ. Это позволяет реализовать доступ к службам в режиме «одного окна», который будет рассмотрен в §4.5.1.3, а изолированные сетевые сегменты, являющиеся зонами действия идентификаторов, в границах федеративной группы становятся единым федеративных сетевым сегментом, функционирующим как единая зона действия идентификаторов (рисунок 4.3).

В федеративной зоне действия идентификатора каждый ПЭУ по-прежнему формирует отдельный идентификатор и параметр для аутентификации одному и тому же клиенту, но клиенту не нужно использовать их все. Наиболее вероятный вариант реализации такой СОПП состоит в том, что доступ будет предоставляться через одного ПЭУ, что позволит применение одного набора идентификаторов и параметров для аутентификации при доступе ко всем ПЭУ, входящих в федеративную СОПП.

4.4.2 Проблемы доверия в федеративной СОПП

Несмотря на то, что федеративная СОПП позволяет упросить взаимодействие ПЭУ с пользователями, она существенно усложняет проблему формирования доверия, как для ПЭУ, так и для их клиентов.

4.4.2.1 Доверие между ПЭУ, входящими с федеративную СОПП

Как показано на рисунке 4.3, доступ к службе ПЭУ может предоставляться не напрямую, а через других ПЭУ. Полагая, что клиент использует отдельные цифровые идентификаторы для разных сегментов предоставления услуг, каждому ПЭУ в последствие необходимо знать отображение (взаимосвязи) между идентификаторами, принадлежащими одному и тому же пользователю. Несмотря на то, что основной метод прямого доступа требует цифровой

идентификатор и параметр для аутентификации клиента в границах данного сетевого сегмента, косвенный доступ – это дополнительный маршрут доступа, который не требует параметров для аутентификации клиента. Такой косвенный маршрут доступа просто требует отправки подтверждений (доказательств) обеспечения безопасности между ПЭУ, например, таких как описано в [126]. ПЭУ необходимо доверять друг другу с целью обеспечения доверия Д2, а также:

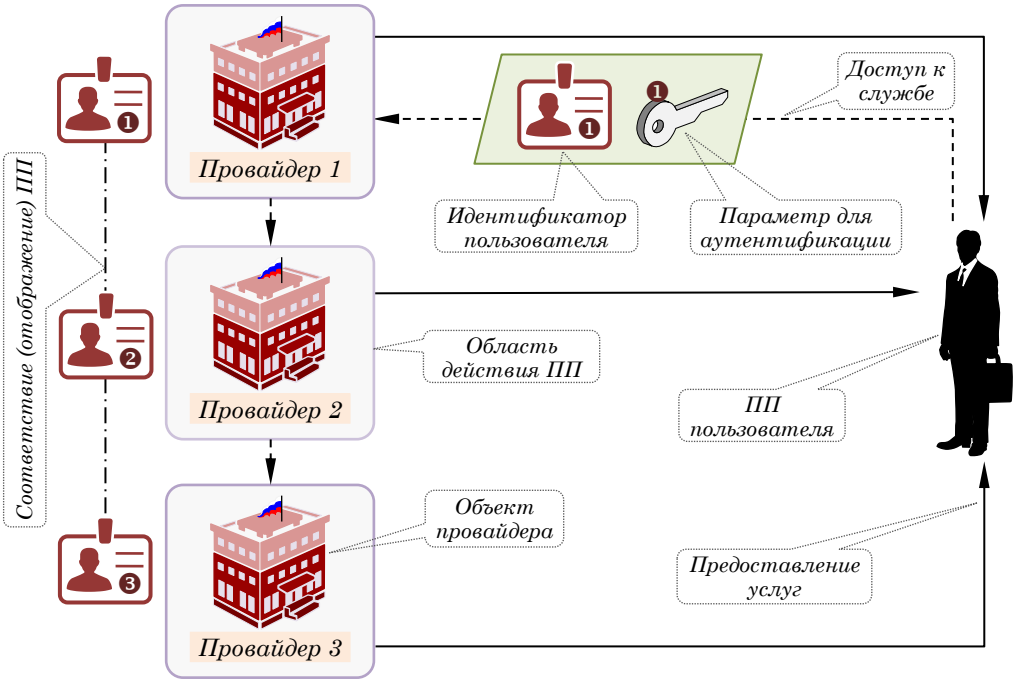

Рисунок 4.3 – Модель федеративной СОПП

Д4: *Доступ к службам на основе отправки подтверждений (доказательств) обеспечения безопасности между ПЭУ от имени пользователей будет предоставляться только тогда, когда он законно запрашивается клиентом.*

Аутентификация клиента третьим ПЭУ основывается именно на таких предположениях. Сбой процедуры аутентификации на стороне третьего ПЭУ может произойти (например), если второй ПЭУ сам потерпел неудачу при проведении процедуры аутентификации или отправил мошеннический запрос доступа третьему ПЭУ (т.е. не от имени клиента). В стандарте [102] это считается серьёзным риском, и отражено следующим образом:

«*При определении того, каким ПЭУ доверять, особенно в тех случаях, когда полученные подтверждения (доказательства) обеспечения безопасности будут использоваться в качестве входных данных при принятии решений относительно результатов аутентификации или авторизации, существует* ***огромный риск компрометации безопасности****, который является следствием использования ложных, но правильно сформированных доказательств безопасности.*»

Предложенный способ формирования доверия Д4 основан на соглашении об использовании единой совокупности политик и процедур, а также на возможном заключении контракта, который устанавливает обязанности и зоны ответственности федеративных ПЭУ [127].

Следует отметить различие между поставщиками услуг, которые формируют обоюдное равнозначное и неравнозначное доверие. Если два ПЭУ должны доверять друг другу в рамках своей повседневной деятельности – например, банки, осуществляющие регулярные финансовые транзакции, – они будут иметь одинаковый риск в случае неудачи и, вероятнее всего, они будут устанавливать равнозначные требования к обоюдному доверию. Однако неравнозначные доверительные отношения между федеративными ПЭУ установить намного сложнее – например, банк, обслуживающий авиакомпанию. В таком случае, реализация двумя сторонами разных функций, означает, что они подвергаются различным рискам в случае нештатной ситуации (например, несоблюдение требований по своевременной финансовой обработке интерактивного бронирования билетов может привести к тому, что авиакомпания потеряет клиентов и, соответственно, десятки и даже сотни тысяч рублей, а банк потеряет только комиссионные, которые во много раз меньше потерь авиакомпании). Проблема неравнозначных доверительных взаимоотношений заключается в том, что одна сторона подвержена более высокому риску, чем другая, и, следовательно, заключение деловых и юридических соглашений становятся более сложным.

4.4.2.2 Доверие к отображению ПП

Отображение цифровых ПП может быть весьма проблематично, так как оно требует адекватного набора единых идентификаторов, которые должны отображаться на каждую пару ПП с целью распознавания реальной принадлежности двух отдельных ПП одному и тому же субъекту. Все ПЭУ, входящие в федеративную СОПП, требуют такого вида доверия, которое можно определить следующим образом:

Д5: *Отображение ПП между ПЭУ должно быть корректным.*

Неправильное отображение ПП неизбежно приведёт к отказу в процедуре аутентификации. Доверие Д5 может быть сформировано путём тщательного проведения процедур отображения ПП, а также путём исторического анализа, подтверждающего отсутствие некорректного отображения. В частности, ПЭУ должны получить согласие от каждого клиента прежде чем отображать их ПП.

4.4.2.3 Доверие клиента к ПЭУ

В дополнение к видам доверия Д1 и Д2, определённым в §3.3.2.1, клиенту также необходимы виды доверия Д4 и Д5. Для удовлетворения требования относительно доверия Д2,

вероятно, необходима более надёжная форма доверия к обеспечению (защите) неприкосновенности, так как отображение ПП потребует от ПЭУ коррелировать персональные данные клиента таким способом, который невозможно было бы реализовать в любом другом случае. Если клиент соглашается на отображение ПП, то он должен согласиться и с конкретной политикой, содержащей правила отображения, и которая может использоваться для корректировки данных, связанных с его различными ПП. Цель такого вида доверия может быть выражена следующим образом:

Д6: *ПЭУ соблюдает установленную совместно с другими ПЭУ политику корректировки персональных данных одного и того же клиента.*

Несоблюдение ПЭУ правил и положений политики обеспечения (защиты) неприкосновенности при отображении ПП может привести к возникновению проблем, неудобств и потенциальных финансовых потерь у клиентов. Вид доверия Д6 может быть сформирован путём точного описания политик, которые приемлемы для клиентов, и, возможно, за счёт наличия истории, описывающей уязвимости в политиках.

4.5 Централизованная система обеспечения параметрами подлинности

4.5.1 Архитектуры централизованной СОПП

В случае сетевого сегмента с централизованным идентификатором, в СОПП представлен всего лишь один ПЭУ, который формирует общий идентификатор и параметры для аутентификации, используемые всеми службами. Централизованная СОПП может быть реализована несколькими различными способами, среди которых СОПП с зоной действия единого идентификатора, СОПП с общей зоной действия мета-идентификатора и СОПП, обеспечивающая предоставление услуг в режиме «одного окна».

4.5.1.1 СОПП с зоной действия единого идентификатора

Существует возможность назначения отдельного субъекта или одного центра в качестве ПЭУ, формирующего идентификаторы и ПП. Такая архитектура называется *СОПП с зоной действия единого идентификатора* (рисунок 4.4).

На рисунке 4.4 показано, что один и тот же идентификатор используется каждым ПЭУ. Это может быть реализовано, например, с помощью ИОК, в которой ЦС выпускает $СЕРТ_{ОК}$ для пользователей. В качестве пространства имён (идентификаторов) можно использоваться адреса электронной почтовой службы Интернет-сети, которые являются уникальными с глобальной точки зрения. В дальнейшем, каждый пользователь может использовать один и тот

же СЕРТ$_{ОК}$ для доступа к службам различных ПЭУ, а все ПЭУ будут аутентифицировать клиента на основе одного и того же СЕРТ$_{ОК}$ до начала предоставления доступа к своим службам.

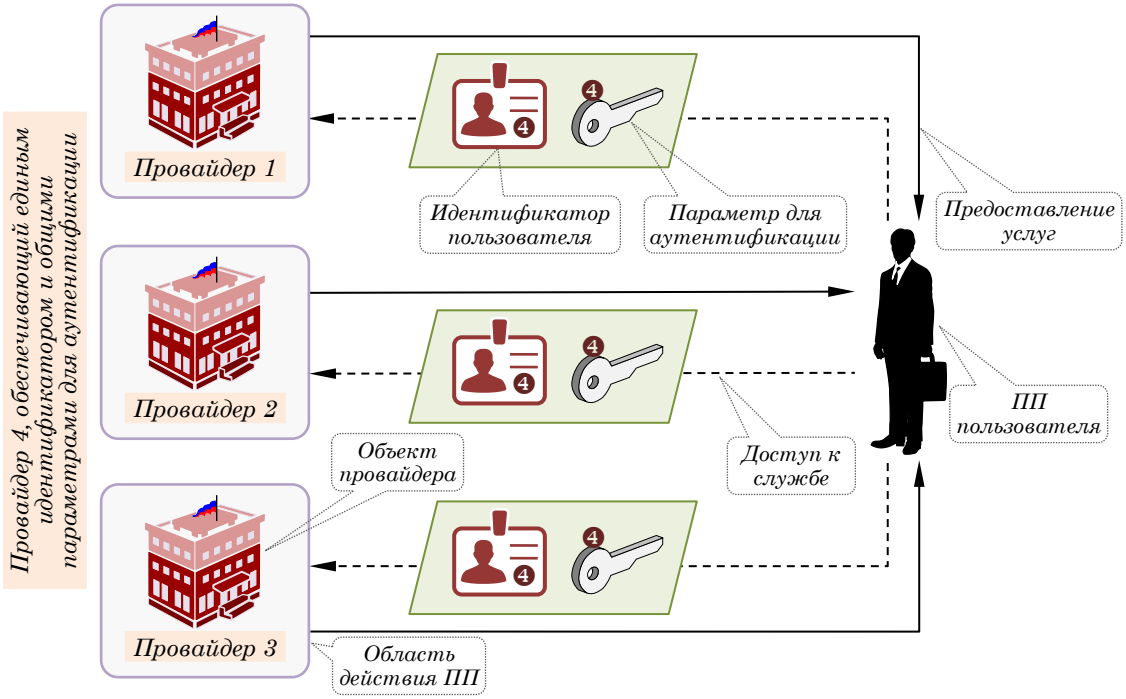

Рисунок 4.4 – СОПП с зоной действия единого идентификатора

4.5.1.2 СОПП с зоной действия общего мета-идентификатора

ПЭУ могут совместно использовать определённые данные, связанные с ПП, на общем или промежуточном (мета-) уровне. Такая система может быть реализована путём отображения конкретных идентификаторов всех ПЭУ в промежуточный (мета-) идентификатор, с которым может быть связан, например, параметр для аутентификации, и представлена на рисунке 4.5.

СОПП с мета-идентификатором обычно реализуется с помощью так называемого *мета-каталога* и часто используется при объединении устаревших систем обеспечения ПП в крупных организациях. В таком случае, все службы, входящие в зону действия промежуточного ПП, как правило, функционируют под управлением администратора(ции) одной организации или органа власти.

С теоретической точки зрения, модель системы обеспечения мета-параметрами подлинности также может обеспечить интегрированный подход к обеспечению ПП для различных ПЭУ, но это потребует согласования политик и надёжного доверия между взаимодействующими сторонами.

Уникальный мета-параметр подлинности, как правило, скрыт от пользователей и используется внутри системы при обеспечении ПП и с целью координации служб. С точки зрения пользователя, это можно рассматривать как синхронизацию паролей (или параметров для аутентификации) между несколькими ПЭУ. Если пользователь изменяет пароль для одного из ПЭУ, то пароль автоматически изменяется для других ПЭУ.

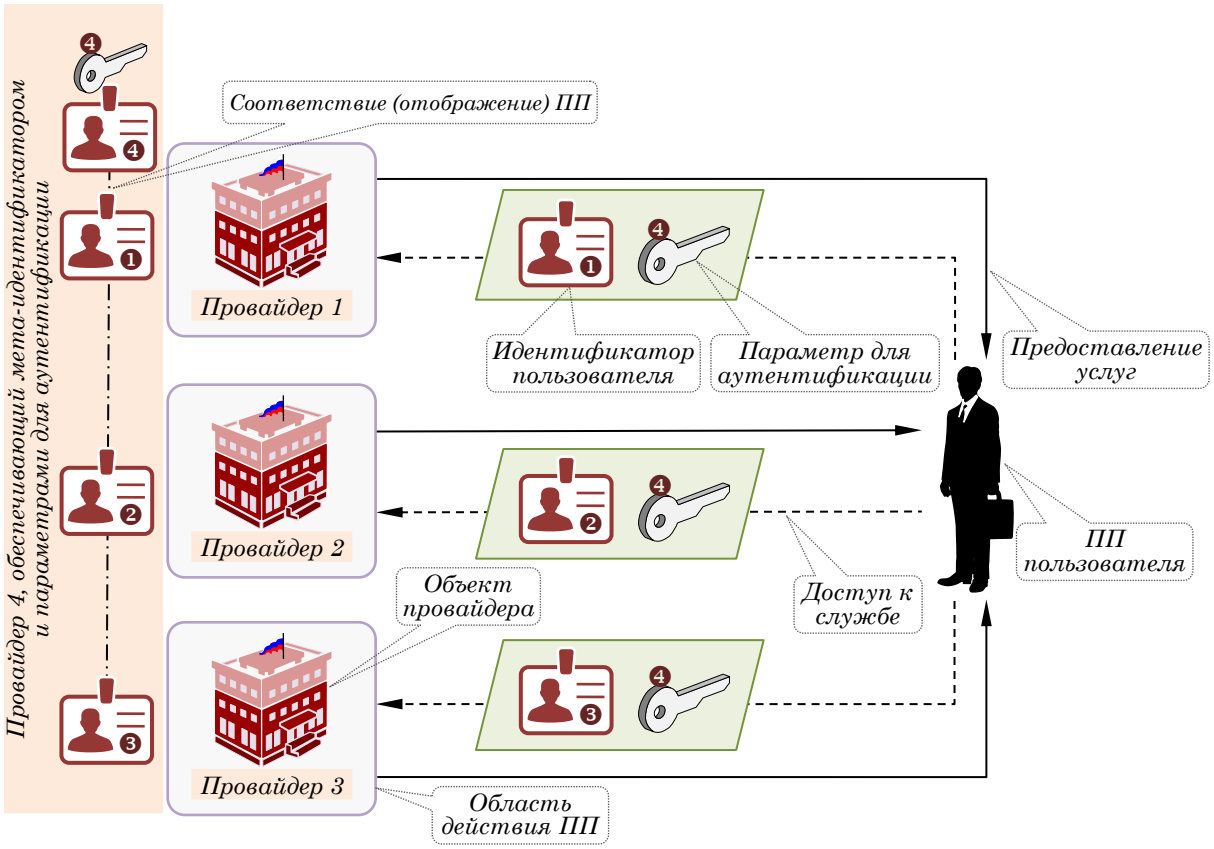

Рисунок 4.5 – СОПП с зоной действия общего мета-идентификатора

4.5.1.3 СОПП, обеспечивающая предоставление услуг в режиме «одного окна»

Простое расширение модели централизованной СОПП (§4.5.1.1 и §4.5.1.2) заключается в том, что пользователю разрешено аутентифицироваться только у одного ПЭУ, а это подразумевает «одновременную» аутентификацию пользователя и у других ПЭУ. Такая модель именуется как *СОПП, обеспечивающая предоставление услуг в режиме «одного окна»*, так как пользователю необходимо аутентифицироваться только один раз (т.е. войти в систему) с целью получения доступа ко всем службам.

Как правило только один субъект (ПЭУ) будет нести ответственность за распределение идентификаторов, выпуск параметров для аутентификации и проведение соответствующей процедуры аутентификации, как показано на рисунке 4.6.

Указанная модель очень напоминает федеративную СОПП (§4.4.1), за исключением того, что в ней не нужно отображение идентификаторов пользователя, так как один и тот же идентификатор используется каждым ПЭУ.

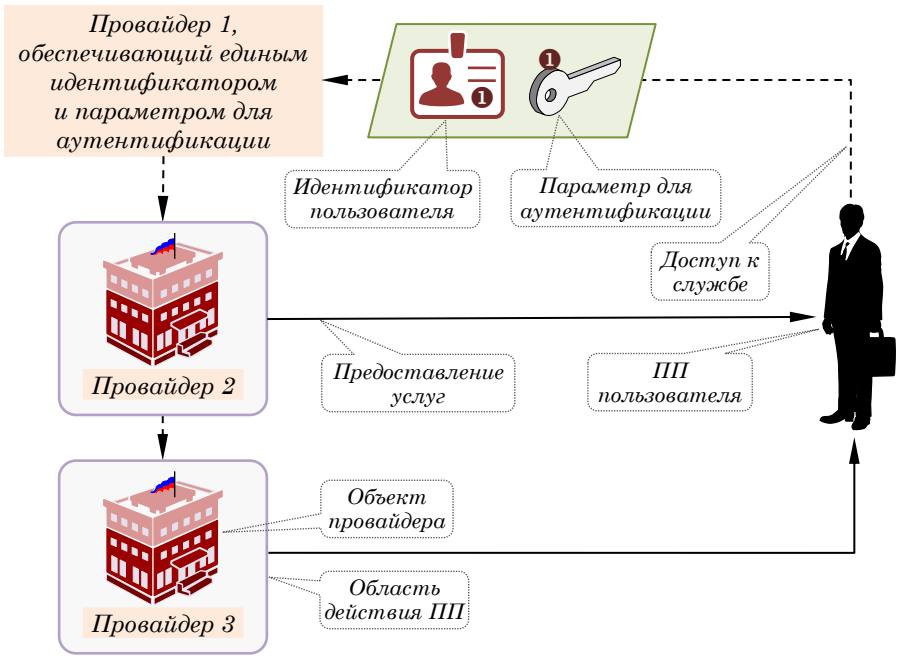

Рисунок 4.6 – Модель СОПП, обеспечивающей предоставление услуг в режиме «одного окна»

4.5.2 Проблемы доверия в централизованных СОПП

4.5.2.1 Доверие клиентов к ПЭУ

Применение доверия Д1 в таких СОПП – очевидно. Если ПЭУ выступает в роли посредника при выпуске параметров для аутентификации на этапе регистрации, и проверяет параметры для аутентификации на этапе аутентификации, то необходим второй вид доверия Д2. Кроме того, необходимо и доверие Д6, так как совместное и централизованное использование ПП предоставляет ПЭУ возможность коррелировать персональные данные одного и того же клиента, обслуживаемого и другими ПЭУ.

4.5.2.2 Доверие ПЭУ к клиентам

В данном случае необходим вид доверия Д3. Однако, если, в случае кражи параметров для аутентификации, риск и вся ответственность возлагается на клиентов, то клиенты должны применять вид доверия Д3 к самим себе.

4.5.2.3 Доверие ПЭУ к ПЭУ, формирующему параметры для аутентификации

Наличие выделенного ПЭУ, формирующего параметры для аутентификации, требует доверия к способу выпуска параметров для аутентификации пользователей:

Д7: *ПЭУ, формирующий параметры для аутентификации, реализовал адекватные процедуры регистрации пользователей и выпуска параметров для аутентификации.*

Невыполнение ПЭУ, формирующим параметры для аутентификации, требований, изложенных в Д7, может привести к проблемам, неудобствам и финансовым потерям у ПЭУ, а также у пользователей.

Вид доверия Д7 может быть сформирован путём внедрения адекватных (приемлемых) процедур регистрации пользователей и выпуска параметров для аутентификации, и за счёт наличия истории, не содержащей фактов ошибок при регистрации. Доверие Д7 пользователей также может быть повышено за счёт снижения рисков пользователей на основе реализации альтернативных стратегий анализа и снижения рисков в случае возможных потерь, вызванных ошибкой при регистрации.

4.6 Системы персональной аутентификации

4.6.1 Архитектура системы персональной аутентификации

Система аутентификации должна учитывать порядок получения, хранения и использования (обслуживания) идентификаторов и параметров для аутентификации самими пользователями. Если пользователям неудобно (затруднительно) обслуживать идентификаторы и параметры для аутентификации, то сама аутентификация будет не надёжной, так как пользователи не смогут надлежащим образом обслуживать (хранить) свои параметры для аутентификации. В связи с этим следует отметить, что ПЭУ услуг обычно используют автоматизированные системы обеспечения ПП и аутентификации, тогда как пользователи обычно обслуживают параметры для аутентификации вручную. В простейшем случае, пользователь записывает идентификаторы, например, в блокнот или иное электронное запоминающее устройство, или запоминает соответствующие пароли для аутентификации. С точки зрения пользователя, увеличение числа идентификаторов и параметров для аутентификации стремительно приводит к невозможности пользователей эффективно их обслуживать (хранить).

Некоторые модели СОПП, рассмотренные выше, особенно модель федеративной СОПП, были обоснованы необходимостью упростить обслуживание идентификаторов и пара-

метров для аутентификации пользователями. Идея состоит в том, что если пользователю необходима только пара идентификатор/параметр для аутентификации, то запоминание или иные простые способы хранения аутентификационных параметров по-прежнему остаются востребованными. Тем не менее, маловероятно, что будет существовать только один федеративный сетевой сегмент, и очевидно, что никогда не будет сетевого сегмента, в котором будет действовать только один ПП в интересах всех ПЭУ. Кроме того, службы с различными уровнями конфиденциальности данных и рисков требуют различные типы аутентификационных параметров. В самом оптимистичном случае, можно предположить, что число пар идентификатор/параметр для аутентификации, которое необходимо обслуживать (хранить) пользователю, когда повсеместно используются федеративные сетевые зоны действия ПП, будет на порядок меньше, чем число ПЭУ, проставляющих услуги по его запросу. К сожалению, мнение пользователей будет по-прежнему отрицательным, если число ПЭУ, предоставляющих интерактивные услуги, продолжает расти с геометрической прогрессией.

Очевидно, что необходим новый способ, который предусматривает автоматизацию процедур обеспечения ПП на стороне пользователей. Ожидать от пользователей, что они будут обслуживать (хранить) постоянно растущее количество паролей и параметров для аутентификации с помощью запоминания или других простых способов, совершенно нереально.

Самое простое решение, которое достаточно очевидно, – позволить пользователям хранить идентификаторы и параметры для аутентификации разных ПЭУ в одном защищённом от несанкционированного доступа (НСД) ПАК, которым может быть смарт-карта (извлекаемое электронное запоминающее устройство) или другое персональное портативное устройство (например, смартфон). Такое решение весьма перспективно и способно убедить пользователей в том, что оно резко снижает их проблемы по обслуживанию (хранению) идентификаторов и параметров для аутентификации, а также повышает надёжность обоюдной аутентификации между пользователями и ПЭУ. Так как основное предназначение такого ПАК – аутентификация, ПАК можно назвать *персональным устройством аутентификации* (ПУА). Это показано на рисунке 4.7.

Термин «*персональное устройство аутентификации*» (*personal authentication device*) используется в контексте компьютерной безопасности достаточно давно, по крайней мере, одно из первых упоминаний ПУА относится к 1985 году [128]. Несмотря на то, что особенности функционирования и ограничения, налагаемые на устройства, с тех пор значительно изменились, ключевая концепция остаётся по-прежнему такой же. Более поздняя интерпретация этой же концепции представлена в форме *персонального доверенного устройства*, определённого в контексте *протокола персональных транзакций* [129]. Так как ПУА – пер-

сональный ПАК, предназначенный для обеспечения ПП и содержащий различные идентификаторы и параметры для аутентификации пользователя, его структуру можно назвать *СОПП, ориентированной на пользователей*. ПУА может быть интегрировано в любую ранее описанную современную модель обеспечения ПП. На рисунке 4.7 представлен вариант встраивания ПУА в изолированные сетевые сегменты – зоны действия идентификаторов (§4.3.1).

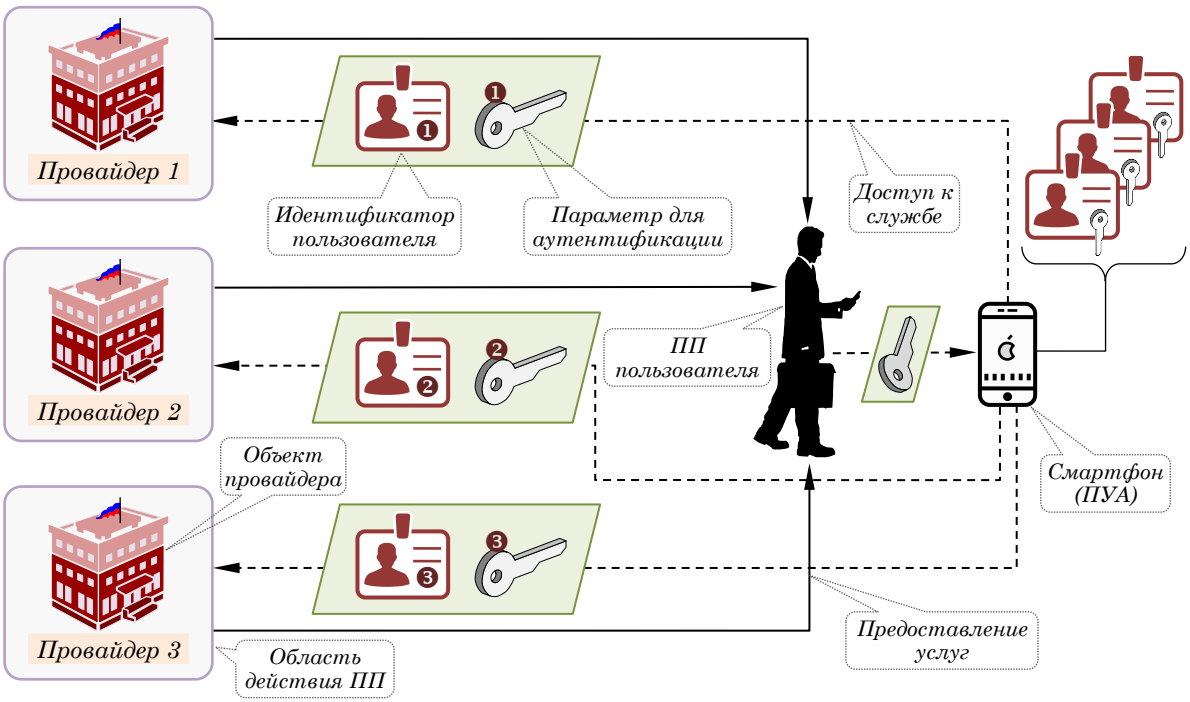

Рисунок 4.7 – Модель СОПП, ориентированной на пользователей

Пользователь обязан аутентифицироваться в самом ПУА, например, с помощью персонального идентификационного номера (ПИН), ещё до того, как ПУА можно использовать в процедурах аутентификации. Можно вообразить множество различных моделей аутентификации и доступа, использующих ПУА. Если ПУА имеет клавиатуру и дисплей, то возможно простое решение – извлечение, например, из памяти ПУА статического пароля или разрешение ПУА генерировать динамический пароль, который пользователь может затем отобразить на экране при входе в систему ПЭУ. Более технологичным решением может быть подключение ПУА к клиентскому программному модулю по каналу связи, например, стандарт беспроводной ЛВС, либо разрешить ПУА напрямую связываться с сервером по вторичному каналу, или ПУА может представлять собой устройство считывания смарт-карт. Такое решение позволяет полностью интегрировать ПУА с процессами аутентификации.

Функциональность ПУА способна интегрировать его с другими устройствами, например, мобильные телефоны (смартфоны), которые в настоящее время получили массовое распространение. Использование смартфона позволило внедрить самые передовые технологии,

например, регистрацию и аутентификацию на основе запросно-ответного способа информационного взаимодействия («*клиент-сервер*») по дополнительному каналу мобильной связи. Если ПУА подключено к клиентскому программному модулю, то возможно использование виртуального режима «одного окна». При таком решении ПУА разрешено автоматически аутентифицироваться от имени пользователя, так как ПУА подключено к программному модулю клиента. Преимущества архитектуры обеспечения пользователей ПП в их интересах – следующие:

1) пользователю необходимо запомнить только один параметр для аутентификации (например, ПИН для ПУА);

2) возможен виртуальный режим доступа «одно окно»;

3) современные модели СОПП могут оставаться неизменными.

Помимо этого, можно избежать большинство недостатков, которые присущи, например, модели федеративной СОПП, таких как высокие требования к доверию и сложные протоколы обеспечения безопасности между ПЭУ.

В настоящее время это решение получило широкое применение. В этой связи, ПУА (смартфон) должно находиться под постоянным контролем пользователя, а не под контролем ПЭУ, формирующих идентификаторы или параметры для аутентификации, или просто ПЭУ услуг. Очевидно, что у пользователя не должно быть много ПУА, а должно быть только одно ПУА. Другими словами, одно защищённое ПУА обеспечивает простое обслуживание пользователями своих ПП, а также упрощает обеспечение самих пользователей ПП. В то же время, многие ПЭУ адаптировали процессы регистрации ПП и выдачи параметров для аутентификации в соответствии с моделью ПУА.

На рисунке 4.8 представлены процедуры аутентификации на основе ПУА (смартфона) с использованием одного или двух каналов связи.

В частности, идея использования двух каналов аутентификации была предложена в начале 2000-х годов [130…134]. При использовании двух каналов аутентификации (рисунок 4.8,*а*), первый обеспечивает аутентификацию пользователя (программного модуля клиента), а второй используется для подтверждения подлинности пользователя, т.е. по каналу мобильной связи сервер аутентификации отправляет пользователю пароль, при получении которого пользователь возвращает его серверу. Таким образом ПЭУ предотвращает попытку злоумышленника разыграть «маскарад». В основе аутентификации по второму каналу лежит «убеждённость сервера ПЭУ» в том, что пользователь является единственным владельцем смартфона, и только пользователь мог аутентифицироваться при доступе к функциям смартфона (ПИН-код, биометрический параметр и т.д.). В данном случае, реализуется трёх-итерационная процедура однонаправленной аутентификации пользователя.

При использовании одного канала аутентификации схема аутентификации (рисунок 4.8,*б*) аналогична описанной выше (с двумя каналами аутентификации). Это объясняется тем, что современные операторы сотовой связи предоставляют услуги не только телефонной связи, но и услуги доступа в Интернет-сеть. Другими словами, смартфон пользователя способен одновременно обеспечивать телефонную связь (передачу речевых сообщений и доставку коротких текстовых сообщений) и передачу данных (доступ в Интернет-сеть).

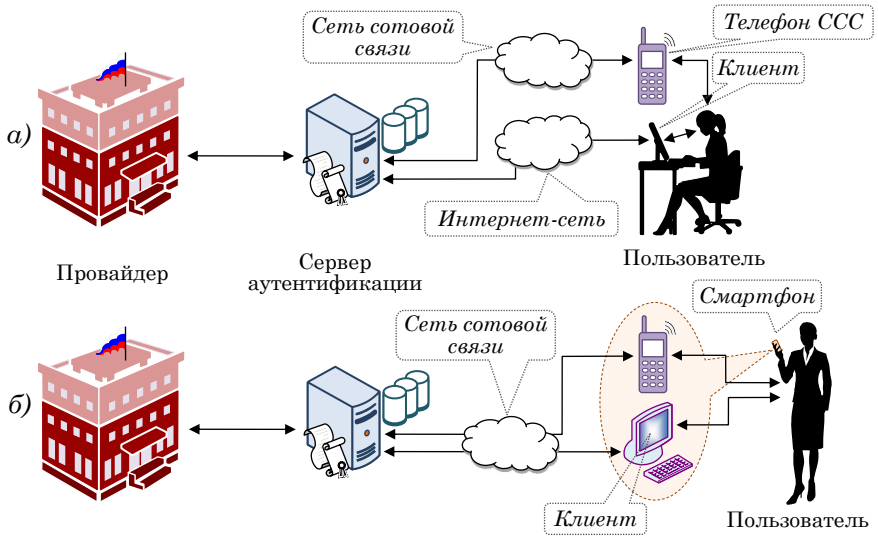

Рисунок 4.8 – Возможные схемы персональной аутентификации с использованием ПУА (смартфона)

Тем не менее, современные системы аутентификации при предоставлении электронных услуг не обеспечивают аутентификацию ПЭУ.

4.6.2 Проблемы доверия в системах персональной аутентификации

Наличие способности доверять ПУА является главным требованием доверия в системах персональной аутентификации. Система с ПУА обеспечивает двух параметрическую аутентификацию с использованием параметров для аутентификации, которые хранятся в ПУА, благодаря тому, что пользователь:

а) должен обладать устройством и контролировать его;

б) обязан знать ПИН для доступа и разблокировки устройства.

Устройство должно быть так защищено от НСД, чтобы в случае кражи ПУА вор не смог им использоваться. Это требование может быть сформулировано следующим образом:

Д8: *ПУА защищено от НСД.*

Если ПУА не будет достаточно защищено от взлома, то злоумышленник, имеющий физический доступ к ПУА, сможет извлечь и/или использовать параметры для аутентификации

и, таким образом, получить доступ к ПЭУ, выдавая себя за законного пользователя и владельца ПУА.

Вид доверия Д8 может быть сформирован на основе оценки защищённости ПУА в соответствие с выбранными критериями, а также при наличии истории, в которой отсутствуют успешные атаки нарушителей.

ПЭУ должны учитывать вид доверия Д3, поскольку они будут полностью зависеть от пользователей и технологий, реализуемых в ПУА, при аутентификации самих ПЭУ. Можно сформировать вид доверия Д8, но доверие ПЭУ к использованию ПУА потребителями может быть неприемлемо, точно так же, как неприемлемо отсутствие согласования при заключении официальных договоров (т.е. вид доверия Д1 – ещё более проблематичен). В модели федеративной СОПП, в которой ссылки (указатели) включены в формат ПП, демонстрация «истории» – наилучшая модель формирования доверия.

4.7 Сравнение моделей обеспечения пользователей ПП

Анализ различных моделей СОПП с точки зрения требований обеспечения доверия представлен в таблице 4.1.

Как видно из таблицы, обеспечение доверия в изолированной СОПП требует намного меньше условий для формирования доверия, тогда как федеративная СОПП требует больше всего. Удовлетворение требований доверия весьма затратно, и поэтому чем меньше требований, тем лучше. С этой точки зрения, обеспечение доверия в системах персональной аутентификации устанавливает меньше всего требований к формированию доверия. При выборе какой-либо конкретной архитектуры СОПП, затраты, связанные с удовлетворением требований обеспечения доверия, также должны учитывать стоимость и удобство использования реализованной СОПП.

Таблица 4.1 – Сравнение моделей обеспечения клиентов ПП

	Д1	**Д2**	**Д3**	**Д4**	**Д5**	**Д6**	**Д7**	**Д8**
Изолированная	✓	✓	✓					
Федеративная	✓	✓	✓	✓	✓	✓		
Централизованная	✓	✓	✓			✓	✓	
Персональная	✓	✓	✓					✓

Кроме того, на основе данных из сравнительной таблицы 4.1, можно установить, имеют ли федеративные и централизованные СОПП явные преимущества при сбалансировании затрат, связанных с усилением требований по обеспечению доверия.

Одной из основных целей функционирования федеративных и централизованных СОПП является упрощение процедур обеспечения клиентов ПП за счёт сокращения количества идентификаторов и соответствующих параметров для аутентификации, которые они должны обслуживать (хранить). Следует признать, что не может быть одной федеративной или централизованной зоны действия идентификаторов, и что даже при наличии федеративных и централизованных зон действия идентификаторов всё равно будут существовать изолированные зоны действия идентификаторов. Например, будут существовать зоны (сетевые сегменты), которые невозможно перенести, и будут ПЭУ с своими конкретными требованиями, которым не будут соответствовать федеративные или централизованные зоны действия идентификаторов. Даже в случае использования федеративных и централизованных зон действия идентификаторов, клиенты всё равно будут сталкиваться с необходимостью обслуживать (хранить) несколько идентификаторов и параметров для аутентификации. Поэтому можно предположить, что персональное обеспечение ПП – это единственная универсальная СОПП, которая может снизить сложность обеспечения клиентов ПП.

4.8 Системы обеспечения ПЭУ параметрами подлинности

В настоящее время, проблема идентификации ПЭУ практически не обсуждается, ни при предоставлении услуг с помощью всемирной ГИТС («*World Wide Web*»), ни при обеспечении безопасности электронной коммерции.

Существует несколько фундаментальных различий между обеспечением пользователей и ПЭУ собственными ПП. Как правило, ПЭУ обладают базами данных, содержащими (цифровые) идентификаторы и параметры для авторизации и аутентификации всех своих клиентов, которые подключены к системам аутентификации. С другой стороны, пользователи, как правило не имеют собственной базы данных о ПЭУ, с которыми они взаимодействуют. Поэтому определение соответствующего цифрового идентификатора ПЭУ, необходимого для аутентификации конкретного ПЭУ, может быть весьма сложным.

Процедура аутентификации требует наличия УИД, который можно «привязать» к параметрам для аутентификации. ПЭУ, которые функционируют в глобальных ИТС, например, Интернет-сети, нуждаются в глобальных идентификаторах. К сожалению, не существует надёжных и реальных глобальных пространств имён для людей и организаций, и поэтому весьма сомнительна значимость аутентификации ПЭУ с учётом нынешней парадигмы обеспечения безопасности во всемирной ГИТС.

Телефонные номера, адреса электронной почты, IP-адреса, наименования сетевых сегментов Интернет-сети и идентификаторы объектов (*object identifier*, OID) фактически представляют собой глобальные идентификаторы, но так как они часто меняются, их нельзя рассматривать как стабильные и надёжные идентификаторы для людей или организаций.

Сегодня существуют примеры сетевых сегментов, т.е. зон действия ПП ПЭУ, и при этом такие ПП представляют собой приемлемые и надёжные идентификаторы. Однако, ни один из таких сетевых сегментов – зон действия ПП – не является одновременно, и глобальным, и всеобъемлющим. В некоторых странах государственными организациями используются собственные реестры, предназначенные, например, для системы налогообложения, и содержат исчерпывающие списки уникальных идентификаторов в рамках конкретной страны (например, в Российской Федерации *индивидуальные номера налогоплательщиков* – ИНН).

4.8.1 Архитектуры систем обеспечения ПЭУ ПП

4.8.1.1 Модель единой СОПП ПЭУ

Несмотря на то, что в целом для ПЭУ не существует надёжного глобального пространства имён, ранее была предпринята попытка внедрения криптографически стойких алгоритмов в процедуры аутентификации, например, ИОК в интересах всемирной ГИТС в сочетании с протоколом обеспечения безопасности на транспортном уровне Интернет-архитектуры (*transport layer security*, TLS [135]).

Несколько идентификаторов, например, наименование компании, адрес её центрального офиса, имя сетевого сегмента и т.п., кодируются в $СЕРТ_{ОК}$ ИОК на основе всемирной ГИТС, используемых TLS-протоколом. Идентификаторы доставляются как часть $СЕРТ_{ОК}$ в начальной фазе TLS-протокола («приветствие», *handshake*). Пользователь не способен самостоятельно проверить параметр для аутентификации и полагается на компьютер, который сделает это за него. После успешной проверки параметров для аутентификации, проведённой сервером с использованием TLS-протокола, *Web*-обозреватель клиента отображает специальный символ («замок») в углу экранного интерфейса *Web*-обозревателя.

Такая модель обеспечения ПП ПЭУ, используемая TLS-протоколом, представлена на рисунке 4.9. В модели обеспечения безопасности с использованием TLS-протокола, ПЭУ, формирующие идентификаторы и параметры для аутентификации поставщиков услуг, как правило называются ЦС.

Процедура аутентификации на основе TLS-протокола – это чисто техническая процедура, которая не отражает семантическое содержание. Однако TLS-протокол обеспечивает высокий уровень конфиденциальности на основе надёжных криптографических процедур и алгоритмов, и поскольку в настоящее время TLS-протокол нашёл широкое применение, это привело практически к полной нейтрализации атак типа «перехват паролей», которые передавались по Интернет-сети в открытом виде.

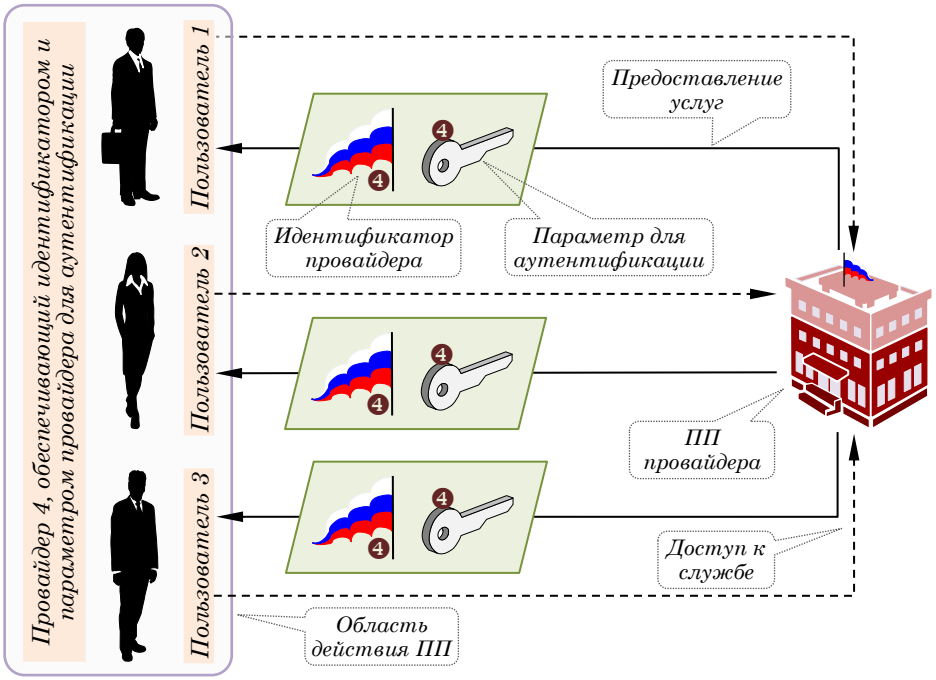

Рисунок 4.9 – Модель единой системы обеспечения ПЭУ ПП

Основное предназначение TLS-протокола заключается в обеспечении безопасности информационного взаимодействия между двумя равноправными субъектами. TLS-протокол основан на надёжной доставке и потоке упорядоченных данных. В частности, защищённый канал должен обеспечивать следующие свойства:

Аутентификация. Взаимодействующий сервер всегда аутентифицирован, а взаимодействующий клиент может аутентифицироваться дополнительно. Процедура аутентификации может проводится с использованием алгоритмов ассиметричной криптографии (например, [136,137,138]) или с использованием предварительно установленного симметричного (секретного) ключа (*pre-shared key*, PSK);

Конфиденциальность. Данные, передаваемые по соединению, после его установления, «видны» только в конечных ПАК. TLS-протокол не скрывает длину передаваемых данных, хотя конечные ПАК могут дополнять TLS-данные с целью сокрытия реальной длины транслируемых данных, что повышает уровень их защищённости от различных вариантов атаки «анализ трафика»;

Целостность. Данные, передаваемые по соединению, после его установления, не могут быть модифицированы злоумышленниками без обнаружения такой модификации.

Эти свойства должны выполняться даже если злоумышленник полностью контролирует сеть [139].

TLS-протокол состоит из двух основных субпротоколов:

Субпротокол «*приветствие*» (СППР, *handshake protocol*, буквально «рукопожатие»), который проводит процедуру аутентификации взаимодействующих субъектов, согласовывает криптографические режимы и параметры, а также формирует совместно используемые ключевые данные. СППР разработан с целью противодействия любому вмешательству, т.е. активный злоумышленник должен быть не способен навязывать субъектам для согласования иные параметры, которые не соответствуют истинным параметрам защищённого канала в случае отсутствия атаки;

Субпротокол «*блочной защиты*» (СПБЗ, *record protocol*), который использует параметры, установленные с помощью СППР, для защиты трафика между взаимодействующими субъектами. СПБЗ делит подлежащий доставке трафик на блоки (т.е. последовательности данных), каждый из которых защищается независимо от других блоков с использованием криптографических ключей для зашифрования трафика.

TLS-протокол не зависит от протокола прикладного уровня Интернет-архитектуры и реализует три основных режима обмена криптографическими ключами:

1. «(EC)DHE» (алгоритм Диффи-Хеллмана на основе алгебры конечных полей или эллиптических кривых, *Diffie-Hellman over either finite fields or elliptic curves*);
2. На основе предварительно установленного ключа (*PSK*);
3. Совместное использование двух режимов «*PSK*» и «*(EC)DHE*».

Проблема модели обеспечения безопасности с использованием TLS-протокола заключается в том, что идентификатор ПЭУ, аутентифицированный *Web*-обозревателем клиента ГИТС, не обязательно является идентификатором ПЭУ, назначенным пользователем. Более того, сами URI-идентификаторы (*universal resource identificator*, универсальный идентификатор ресурсов) могут быть ненадёжными (ложными).

В Интернет-сети существуют способы атак, основанные на использовании *ограниченности когнитивных способностей человека*. Одним из таких примеров является *ошибочный (ложный) URI-идентификатор*, который очень похож на другие URI-идентификаторы, т.е. он отличается только одним символом, и поэтому ложный URI-идентификатор может быть не замечен пользователем Интернет-сети. Следующие URI-идентификаторы: «http:// www.bellabs.com», «http://www.belllabs.com» и «http:// www.bell-labs.com» демонстри-

руют как это можно легко не заметить. Несмотря на то, что используются надёжные криптографические способы и алгоритмы, клиентам, скорее всего, будет сложно узнать, какой ПП был аутентифицирован *Web*-обозревателем [18,140…142].

4.8.1.2 Модель изолированной СОПП ПЭУ

Теперь рассмотрим *модель изолированной СОПП ПЭУ,* которая, с практической точки зрения, нереалистична, но которую можно смоделировать на основе способа, ориентированного на пользователя. Данная модель, представленная на рисунке 4.10, – это зеркальное отображение модели изолированного обеспечения пользователей ПП (§4.3.1).

В данной модели каждый пользователь определяет персональное пространство имён для ПЭУ, и если пользователь желает взаимодействовать с ними, то назначает каждому из них частный (собственный) идентификатор. В итоге, каждый ПЭУ обязан использовать назначенные ему идентификаторы и параметры для аутентификации при проведении процедуры собственной аутентификации различными пользователями. Индексы идентификаторов и параметров для аутентификации, показанные на рисунке 4.10, связаны с тем или иным пользователем, который их присвоил ПЭУ. Преимущество такой модели заключается в том, что персональные идентификаторы ПЭУ вполне понятны, так как они назначаются самими пользователями. Однако, совершенно ясно, что эта модель весьма неудобна, и что она никогда не будет использоваться в реальной жизни.

4.8.1.3 Модель персонального обеспечения пользователей ПП ПЭУ

Предположим, что каждый пользователь имеет своё собственное ПУА (смартфон), тогда пользователи могут сами формировать частные (собственные) идентификаторы для ПЭУ путём отображения глобальных УИД, например, URI-идентификатор ПЭУ, с целью персонального выбора идентификаторов. Такой идентификатор может быть произвольным, только он должен быть узнаваемым, например, текст, изображение, логотип и т.п. (рисунок 4.11).

Индекс «❹», принадлежащий идентификатору и параметру для аутентификации, которые содержаться в сообщениях (рисунок 4.11), указывает на то, что они были назначены одним и тем же ПЭУ, формирующим идентификаторы и параметры для аутентификации с одинаковым индексом. На практике, это может означать, что ПЭУ – это ЦС ИОК. Следовательно, можно предположить, что сообщения содержат $СЕРТ_{ОК}$ ИОК. Индексы «❶», «❷» и «❸», принадлежащие идентификаторам ПЭУ и содержащиеся в ПУА, указывают на то, что они были назначены соответствующими пользователями.

Отображение глобального идентификатора ПЭУ в персональный идентификатор ПЭУ осуществляется в ПУА пользователя. С практической точки зрения, целесообразно, чтобы

пользовательское ПУА непосредственно участвовало в процедуре аутентификации (реализовало соответствующий протокол аутентификации). Существует множество способов решения этой задачи, и каждое такое техническое решение будет зависеть от типа устройства и подключения к Интернет-сети.

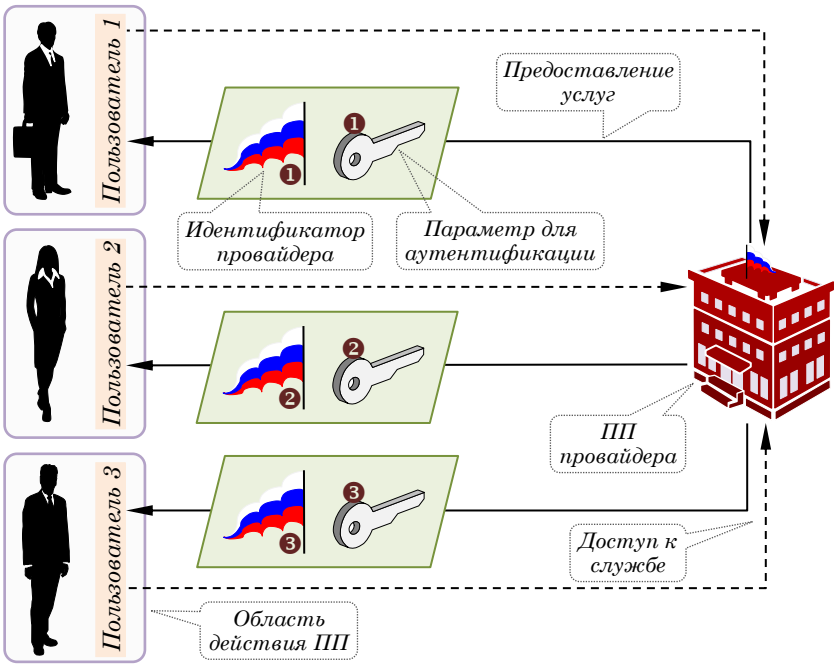

Рисунок 4.10 – Модель изолированной СОПП ПЭУ

В настоящее время ПУА – это смартфоны, представляющие собой единый комплекс технических средств, включающий собственно телефонный аппарат и компьютер (сетевой терминал), и обеспечивающий доступ пользователей к службам через Интернет-сеть. Обоюдная аутентификация сервера ПЭУ и смартфона пользователя проводится путём организации виртуального IP-соединения по радиоканалам между смартфоном и базовой станцией сотовой связи соответствующего ПЭУ мобильной связи, который обеспечивает доступ в Интернет-сеть. Современные ПЭУ электронных услуг предлагают пользователям смартфонов встроить в них свои собственные специализированные КПО (*программный модуль клиента, user agent*), которые в последующем будут настроены и активированы владельцами смартфонов. Таким образом, каждый такой ПЭУ предоставляет владельцу смартфона свой логотип и экранный интерфейс, обеспечивающий доступ пользователя к услугам ПЭУ. Перед началом использования КПО ПЭУ пользователь проводит определённые настройки, включая обмен параметрами для аутентификации. Каждый КПО в смартфоне пользователя обеспечивает аутентификацию ПЭУ.

Для борьбы с вредоносными (мошенническими) КПО используются $СЕРТ_{ОК}$ ИОК (в составе подлинных КПО), которые позволяют обнаружить модифицированное ПО.

Вместе с тем, не все ПЭУ (а их в настоящее время большинство) предоставляют свои КПО для загрузки в смартфоны пользователей. Да и сами смартфоны имеют ограниченные ресурсы памяти и производительности, т.е. невозможно хранить в них КПО всех ПЭУ электронных услуг. Другими словами, проблема аутентификации ПЭУ остаётся до конца нерешённой.

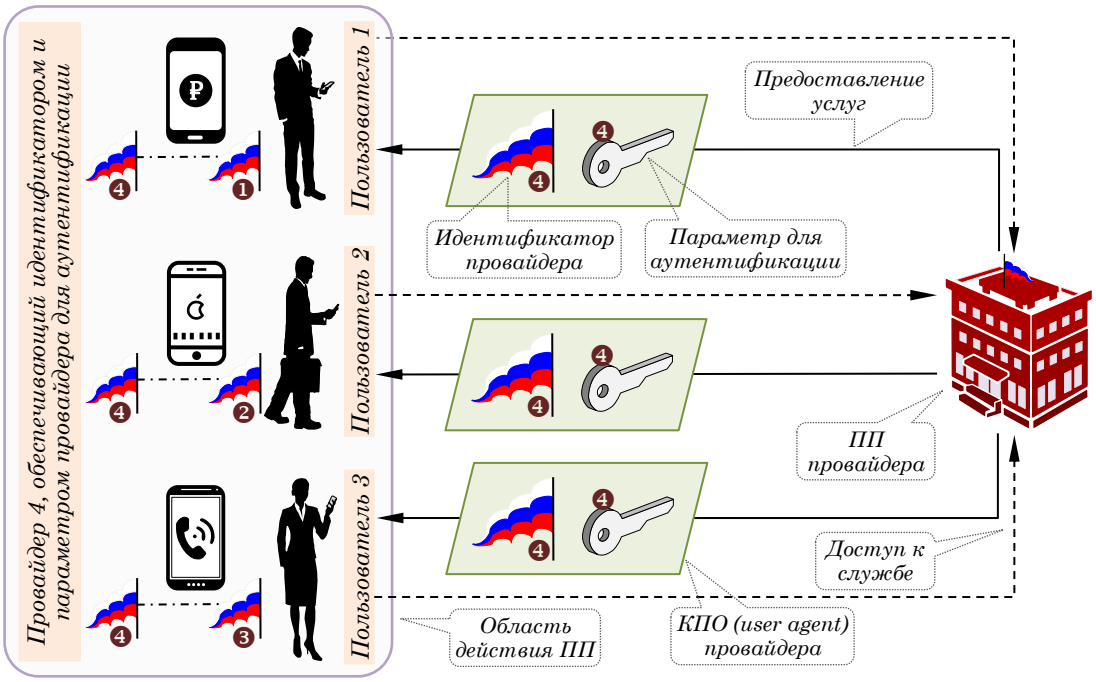

Рисунок 4.11 – Модель системы персонального обеспечения пользователей ПП ПЭУ

4.8.2 Проблемы доверия в системах обеспечения ПЭУ ПП

Главной проблемой для клиента остаётся способность убедится в том, что ПЭУ, к которому он подключён, является именно тем субъектом, с которым он желает установить виртуальное соединение. Даже если такое доверие (убеждённость) не обязательно связано с конкретным идентификатором, а связано, скорее всего, с ПП без использования какого-либо точно определённого УИД, то цель доверия может быть описана следующим образом:

Д9: *ПЭУ обладает предполагаемым ПП.*

Если ПЭУ не имеет предполагаемого ПП, то пользователей можно обмануть и «выманить» у них истинные параметры для аутентификации, например, это происходит при предоставлении интерактивных банковских услуг фальшивыми (мошенническими) *Web*-сайтами. Кроме того, ПЭУ, которые искажают свои ПП с целью привлечения клиентов, могут обмануть и «заставить» пользователей совершать с ними электронные (в том числе фиктивные) сделки [3,143…146].

Тип доверия Д9 может быть сформирован за счёт предоставления пользователю наилучшего интерфейса для аутентификации. Решение проблемы на основе поиска приемлемых глобальных идентификаторов выглядит чрезвычайно сложным. Один из возможных вариантов решения может быть следующим. Глобальные идентификаторы должны состоять из идентификаторов национальных коммерческих регистров и национального определителя, аналогично тому, как телефонные номера становятся глобально уникальными, т.е. путём добавления к ним национального префикса (международного кода страны). Несмотря на то, что такой вариант решения может привести к созданию глобальных УИД ПЭУ, для пользователей он станет проблемой, если формат таких УИД не будет компактным, т.е. не будет включать только цифры и буквы. Очевидно, что ПУА (смартфон) – это наилучшее решение, которое приемлемо для аутентификации и распознавания идентификаторов такого типа.

По аналогии с телефонными номерами с международными кодами государств, в [147,148] предложен способ использования OID государств [149] в качестве «префикса глобальной маршрутизации» в заголовках IP-адресов 6 версии (128-битовые сетевые идентификаторы [150,151]) и разбиения всего пространства таких адресов на национальные диапазоны на основе OID государств (§5.5).

Таким образом, адекватные СОПП в открытых вычислительных сетях имеют *решающее значение* при обеспечении безопасности и повышении эффективности. СОПП требует интегрированной и очень сложной инфраструктуры, в которой все участвующие субъекты должны быть доверенными при решении конкретных задач, в зависимости от их функциональных обязанностей.

4.9 Параметры подлинности в сертификатах ИОК

В Главе 2 было дано определение термина «доверие» – это прямая взаимосвязь между двумя сторонами, которые можно назвать доверяющей стороной (*доверитель,* «*мыслящий субъект*») и доверенной стороной (*доверяемый*). Доверяемый может быть кем угодно, начиная от пользователя, организации или физического объекта до абстрактных описаний, например, информация или криптографический ключ.

У доверительной взаимосвязи есть свои границы применения, означающие, что она применяется с определённой целью или пределах некоторой зоны действия, например, «*быть подлинным*» относительно криптографического ключа или «*высокопрофессиональное качественное лечение зубов*» для стоматологов. В научно-технической литературе термин «*доверие*» (*trust*) используется в самых разнообразных значениях [66], и поэтому не всегда по-

нятно, какое значение вкладывает в него автор. С целью исключения неправильного понимания этого термина, всегда полезно быть конкретным и определять значение доверия при его использовании в соответствующем контексте.

В СЛ (см. §2.12.2) различают доверие при проведении оценки надёжности или принятии решения. Если интерпретировать доверие как субъективную оценку надёжности или корректности чего-либо, или кого-либо, это – *доверие к надёжности*. Если интерпретировать доверие как решение о действиях или поступках в той или иной ситуации в зависимости от чего-то или кого-то, это – *доверие при принятии решения*. На первый взгляд, это различие может показаться едва различимым, но на самом деле является фундаментальным. Например, наличие высокого доверия к оценке субъекта не обязательно является достаточным для принятия решения о том, чтобы перейти в состояние, зависящее от этого субъекта, если воспринимаемый риск, нахождения в таком состоянии, слишком высокий. Доверие к надёжности отражает *благонадёжность* доверенной стороны и не зависит от конкретной ИТС или сетевой среды, тогда как доверие к принятому решению зависит от конкретной ИТС или от сетевой среды, в которой она функционирует. Можно показать, что доверие при принятии решения – функция доверия к оценке и риска [23].

И доверие к надёжности, и доверие при принятии решения отражают позитивную убеждённость доверяющей стороны в то, от чего потенциально или реально зависит её благополучие/благосостояние. Доверие к надёжности, как правило, измеряется как дискретная или непрерывная степень надёжности или убеждённости, тогда как доверие при принятии решения, как правило, измеряется с точки зрения двоичного (двухальтернативного) решения. В некоторых работах было предложено, чтобы $СЕРТ_{ОК}$ отражали степени доверия в дискретном или непрерывном масштабе, например, в [152]. Однако это будет иметь смысл только в том случае, когда ЦС не уверены в корректности того, что они сертифицируют, а отображение степеней доверия к $СЕРТ_{ОК}$, по-видимому, несовместимо с современными функциональными моделями ЦС. Было бы весьма странно, если бы ЦС указал в сертификате, что сертифицированный открытый ключ, например, аутентичен с вероятностью 0.9, так как ни один пользователь не захотел бы приобретать такие $СЕРТ_{ОК}$. Издание $СЕРТ_{ОК}$ осуществляется в соответствие с политикой сертификации. На практике такая политика, как правило, публикуется в виде двух документов, именуемых как *политика сертификации* и *ОДС,* при этом первый определяет требования высокого уровня, а второй – как детально выполняются эти требования на практике. Доверяющая сторона может оценить адекватность политики, определяющей правила использования $СЕРТ_{ОК}$. Кроме того, доверяющая сторона должна учитывать, правильно ли ЦС соблюдает (реализует) политику сертификации. Доверие к надёжности подтверждённого $СЕРТ_{ОК}$ можно определить, как «*качество политики сертификации в сочетании с верой*

(убеждённостью) в то, что ЦС строго соблюдает эту политику». Тем не менее, доверяющие стороны очень часто не обладают достаточным опытом для оценки политики сертификации, и им будет реально сложно проверить соблюдение ЦС политики сертификации.

$СЕРТ_{ОК}$, подлинность которого подтверждена, никогда не обеспечит 100%-ую гарантию, что открытый ключ реально подлинный. Например, злоумышленник может обманным путём принудить ЦС выпустить $СЕРТ_{ОК}$ с неправильным именем (атрибутом), что позволит злоумышленнику подделать соответствующий ПП [153]. Именно доверяющая сторона определяет, как воспользоваться гарантиями, обеспечиваемые конкретным $СЕРТ_{ОК}$, и которые зависят от реальной ситуации. Например, доверяющая сторона может воспринимать подлинный $СЕРТ_{ОК}$, как доказательство подлинности, но при этом будет убеждена только на 90%, что сертифицированный открытый ключ является подлинным, а это будет эквивалентно 90% доверия к оценке. Тем не менее, одна и та же доверяющая сторона может принять решение о признании и использовании $СЕРТ_{ОК}$, несмотря на то, что она не полностью убеждена в корректности ПП, и это могло бы иметь место в случае доверия к принятому двоичному решению. Доверие при принятии решения относительно $СЕРТ_{ОК}$, подлинность которого подтверждена, можно определить, как «*признание сертификата на основе доверия к надёжности и других характеристик сетевой среды*».

Сертификат только частично обеспечивает доверие, которое необходимо при проведении соответствующей транзакции. Доверяющие стороны должны интерпретировать подлинный $СЕРТ_{ОК}$, как доказательство подлинности открытого ключа, но не как доказательство качества и надёжности. Доверяющей стороне, как правило, необходимо учитывать оба типа доверия, но *$СЕРТ_{ОК}$ могут обеспечить только доверие к ПП.*

ИОК и $СЕРТ_{ОК}$ обеспечивают процедуру аутентификации владельца ключа и тем самым обеспечивают обработку ПП. ПП – отображение субъекта в конкретной прикладной ИТС (области). Обычно, ПП отражают субъекты окружающего мира, но в настоящее время в Интернет-сети распространены интерактивные ПП анонимных субъектов. Типичными субъектами окружающего мира являются люди и организации. В случае интерактивных ПП следует обязательно считать, что существует реальный субъект окружающего мира, даже если он неизвестен доверяющим сторонам.

Выделенное пространство уникальных наименований/имён в сетевом сегменте допускает взаимно-однозначное соответствие между ПП и наименованиями/именами. Но не каждый ПП может использоваться как уникальное наименование. Например, дата рождения не является уникальным идентификатором конкретного человека, так как несколько людей могут иметь одну и ту же дату рождения. Определить приемлемое пространство имён может быть довольно сложно, и в целом, чем больше сетевой сегмент (т.е. чем больше субъектов подлежит

идентификации), тем сложнее оно становится. Например, пространство наименований, состоящее из уникальных имён всех людей, кажется реализовать невозможно, и с политической, и с практической точек зрения. Пространства имён должны быть тщательно спроектированы, потому что плохой проект пространства имён, который должен быть изменён на более позднем этапе, может привести к значительным дополнительным затратам. Например, когда стало очевидным, что адресное пространство 32-битовых IP-адресов 4-ой версии с фиксированной длиной (Интернет-протокол) недостаточно, было разработано новое пространство адресов для IP-протокола 6-ой версии, включающее 128-битовые IP-адреса, в результате чего IPv4- и IPv6-адреса стали несовместимы [150,151].

В некоторых системах по различным причинам (практическим или конфиденциальным) могут использоваться *псевдонимы* с целью применения анонимных ПП [154]. Псевдоним – это имя реального владельца, которого знает только сторона, присвоившая ему псевдоним. Псевдонимы могут присваиваться самостоятельно, так что ПП реального субъекта (например, юридического лица), которому присвоен псевдоним, известен только владельцу, а в противном случае скрыт и от всех других взаимодействующих сторон. С другой стороны, псевдоним может определяться и присваиваться ДТС, которая знает реальный ПП и способна раскрыть его при особых обстоятельствах, например, правоохранительным органам.

ПП могут быть сформированы различными способами. С формальной точки зрения, это можно осуществить за счёт процедуры регистрации, реализуемой ЦР, а с неформальной точки зрения – путём повторяемых процедур информационного взаимодействия с другими субъектами, в которых раскрываются различные характеристики ПП. Этимологический смысл ПП: «*тот же самый, как и в последний раз*» («*the same one as last time*»). Таким образом, требование формирования интерактивного ПП состоит в том, чтобы существовал процесс первого определения или регистрации атрибутов ПП. Регистрация нового ПП не обязательно включает характеристики реального мира или другие ранее существовавшие атрибуты ПП. Новый ПП может быть определён «с нуля» и с совершенно новыми атрибутами, и в этом случае он становится виртуальным или псевдоанонимным ПП. Важным свойством является то, что субъект может распознаваться в дальнейших процедурах информационного взаимодействия с помощью тех же самых атрибутов. Такой же принцип реализован и в ИОК, так что уникальное имя и другие атрибуты ПП в сертификате не обязательно связаны с известным субъектом реального мира. Можно даже использовать открытый ключ как таковой в качестве уникального имени, и в этом случае ПП пользователя формируется с помощью открытого ключа, а также других параметров, характеризующих «присутствие» пользователя в сети. Этот принцип реализован в *SPKI/SDSI-модели* (простая ИОК/простая распределённая инфраструктура безопасности, *simple PKI/simple distributed security infrastructure,* [14,155])

Стандартные СЕРТ$_{ОК}$ формируют криптографические привязки между открытым ключом и уникальным именем в конкретном сетевом сегменте, в котором используется ПП. Кроме того, могут быть определены и другие (возможно не уникальные) имена/наименования. Крайне важно, чтобы имена были значимыми для доверяющих сторон. ПП, с помощью которого, как правило, доверяющие стороны распознают пользователя, не обязательно должен включать уникальное имя, содержащееся в сертификате. В таком случае, должна быть возможность привязки уникального имени к значимому ПП, так как, в противном случае, СЕРТ$_{ОК}$ может стать бессмысленным для доверяющих сторон.

4.10 Структуры доверия на основе ИОК

Сложность обеспечения защищённого распределения криптографических ключей является основным препятствием для практического использования криптографии (КЗСУ). В симметричных криптографических системах (с одним ключом) каждая пара взаимодействующих сторон (субъектов), желающих сформировать между собой защищённое виртуальное соединение, обязаны обменяться криптоключами по вспомогательному (дополнительному) каналу связи, и таким образом, сформировать прямое доверенное (надёжное) взаимодействие. Термин вспомогательный канал означает внешний канал (т.е. за пределами системы), который должна защищать ИОК. Защищённость вспомогательных каналов и прямые доверенные (надёжные) взаимосвязи весьма затратны, с точки зрения их организации и обслуживания, и поэтому поиск способов снижения их числа может привести к значительной экономии средств.

Одна из основных целей ИОК – упростить распределение ключей путём снижения числа необходимым вспомогательных защищённых каналов. Вместе с тем, доверие к открытым ключам пользователей формируется на основе криптографии и ограниченной совокупности прямых доверенных взаимосвязей/взаимоотношений. В таком случае, ИОК позволяет распространять доверие оттуда, где оно существует, туда, где оно необходимо [56].

СЕРТ$_{ОК}$ отражает границу между ЦС и владельцем сертифицированного открытого ключа. Обычные границы доверия заключаются в том, что «*владелец открытого ключа по праву владеет уникальным именем, указанным в сертификате*». Такие СЕРТ$_{ОК}$ очень часто называются сертификатами ПП. Любой пользователь, который может доказать, что он обладает закрытым ключом, соответствующим открытому ключу, докажет, что он также обладает собственным уникальным именем, указанным в сертификате. Доказательство, как правило, основано на протоколе криптографической защиты. Таким образом, сертификат с ПП формирует криптопривязку между открытым ключом и ПП. Кроме того, сертификат, помимо уникального имени, может отражать и другие семантические понятия, и в таком случае он

называется $СЕРТ_{АТ}$. Теоретически, любая приемлемая концепция, которая может быть связана с открытым ключом, может быть сертифицирована с помощью $СЕРТ_{АТ}$. $СЕРТ_{АТ}$ в большинстве случаев отражают права доступа, и при этом границы доверия могут быть следующими: «*владелец сертификата имеет право доступа к ресурсу X*». Таким образом, $СЕРТ_{АТ}$ формируют криптопривязку владельца сертификата к конкретным атрибутам (правам доступа) владельца.

Доверяющая сторона, которая доверяет ЦС, подтвердившему подлинность сертификата, и которая успешно провела необходимые протокольные процедуры аутентификации совместно с пользователем, сможет сформировать доверие к надёжности ПП пользователя, представленного с помощью уникального имени, указанного в $СЕРТ_{ОК}$. Связанная цепочка (последовательность) сертификатов отображает *маршрут доверия*, а совокупность взаимосвязанных сертификатов отображает *сеть доверия*. В общем, любую такую сеть доверия, основанную на $СЕРТ_{ОК}$, можно назвать ИОК, но в действительности только несколько классов такой сети доверия представляют собой реальные ИОК с жизнеспособными функциональными моделями. Получатели $СЕРТ_{ОК}$, называемые также *доверяющими сторонами*, сами по себе не нуждаются в сертификатах с целью аутентификации открытого ключа пользователя, им нужна только подлинная копия открытого ключа корневого ЦС. Только тем пользователям, которые желают аутентифицироваться, необходимо иметь $СЕРТ_{ОК}$. В дальнейшем, владелец последнего $СЕРТ_{ОК}$ в цепочке будет называться *пользователем*. Пользователь может быть юридическим субъектом, либо индивидуальным предпринимателем, либо организацией, либо это может быть система или объект обработки, или даже абстрактный функциональный субъект.

На рисунке 4.12 представлена типовая структура доверия на основе ИОК и графическое обозначение, используемое в последующих рисунках. В нижней части рисунка показаны процедуры и порядок (индексы в кружках) формирования доверенных взаимосвязей и цифровых подписей. В верхней части рисунка показано соответствующее графическое отображение ИОК. Предполагается, что ЦР – составной компонент и корневого, и промежуточного ЦС. Предназначение ЦР – предварительная аутентификация ПП пользователя на основе представленных документов реального мира, а также связывание ПП (включает набор атрибутов) пользователя с ЦС. На практике ЦР – отдельная структура, не входящая в ЦС, тогда необходимы дополнительные доверенные взаимосвязи между ЦС и ЦР.

Считается, что корневой и промежуточные ЦС, а также пользователи обладают полным доверием к подлинности своей собственной пары (открытый/закрытый) ключей (индекс «❶»). Корневой ЦС формирует самоподписанный $СЕРТ_{ОК}$ (индекс «❷»), который распространяется по любому с приемлемым уровнем защищённости вспомогательному каналу до потенциальных доверяющих сторон. Когда корневой ЦС уверен в надёжности ПП промежуточного ЦС и

подлинности его открытого ключа, он формирует доверие к криптосвязке ПП с открытым ключом (индекс «❸»). Затем ЦС выпускает СЕРТ$_{ОК}$ в соответствии с конкретной политикой с целью подтверждения этого факта (индекс «❹»). Аналогично, когда промежуточный ЦС уверен в криптосвязке ПП пользователя и его открытого ключа (индекс «❺»), он выпускает СЕРТ$_{ОК}$ пользователя в соответствии с конкретной политикой, который доказывает этот факт (индекс «❻»).

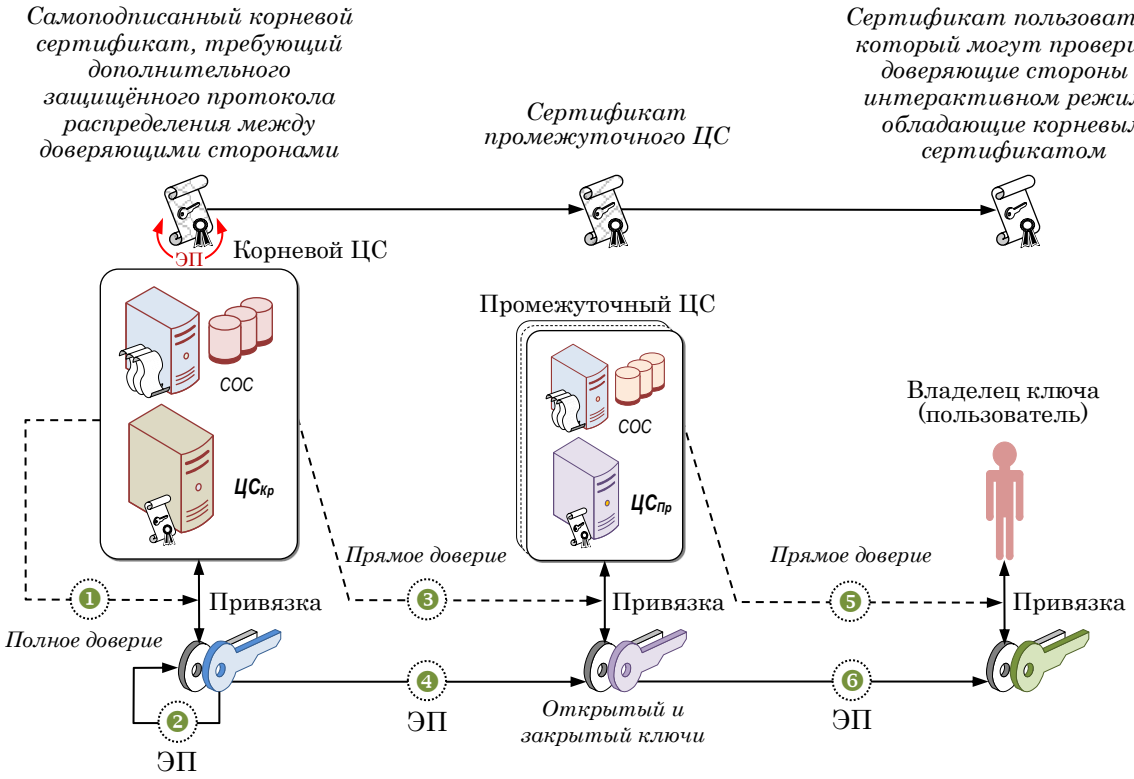

Рисунок 4.12 – Структура доверия при издании СЕРТ$_{ОК}$

Следует отметить, что корневой ЦС также обязан доверять промежуточному ЦС относительно его надёжности (компетентности и добросовестности) с точки зрения корректной регистрации и выдачи СЕРТ$_{ОК}$ пользователя, так что доверительные отношения между корневым и промежуточным ЦС (индекс «❸») обычно имеют двойное предназначение, включающее явную криптопривязку открытого ключа к наименованию ЦС, а также безусловное доверие к надёжности ЦС.

Доверенная взаимосвязь между промежуточным ЦС и пользователем (индекс «❻») имеет единственное предназначение (область назначения) – криптопривязка открытого ключа к имени его владельца, т.е. она ничего «не говорит» о надёжности самого пользователя. На практике это означает, что ЦС не будет проверять, являются ли пользователь или организация, получившие СЕРТ$_{ОК}$, добросовестными или компетентными в каком-либо смысле, так как это не входит в сферу доверия СЕРТ$_{ОК}$ пользователя.

Существуют различные функциональные модели ЦС. Коммерческие ЦС получают доход от продажи СЕРТ$_{ОК}$, в то время как внутренние ЦС организаций выпускают СЕРТ$_{ОК}$ для их структурных подразделений, как часть своего функционального предназначения или своих обязательств. Физические лица также могут выступать в роли ЦС, например, в *PGP*-системах (будет рассмотрена ниже), в которых выпускаемые СЕРТ$_{ОК}$ предназначены для обеспечения «друзей/коллег» или организации виртуальных соединений между такими субъектами.

ПАК, разработанные для хранения и обработки открытых ключей в форме СЕРТ$_{ОК}$, как правило, не способны обрабатывать незащищённые открытые ключи. По этой причине корневые открытые ключи, как правило, распространяются и хранятся в форме самоподписанных СЕРТ$_{ОК}$. Таким образом, корневой открытый ключ является частью СЕРТ$_{ОК}$, который был подписан с помощью соответствующего закрытого ключа (рисунок 4.12, индекс «❷»).

Следует заметить, что самоподписанный СЕРТ$_{ОК}$ не даёт никаких гарантий относительно подлинности корневого открытого ключа, он только обеспечивает более эффективное распространение, хранение и обработку корневых открытых ключей. Это связано с тем, что проверка самоподписанного открытого ключа должна быть выполнена с тем же открытым ключом. Очевидно, что это бессмысленно, так как открытый ключ не может подтвердить свою подлинность, а ИОК были бы не нужны, если бы открытые ключи сами подтверждали свою подлинность.

Процедура подтверждения подлинности (ПРП), проводимая, как правило, доверяющей стороной, включает проверку корректности ЭП в СЕРТ$_{ОК}$. Данные, извлекаемые из СЕРТ$_{ОК}$ с подтверждённой подлинностью (ПРП СЕРТ$_{ОК}$), например, наименование, открытый ключ и другие атрибуты считаются подлинными. На рисунке 4.13 показана ПРП и формирование доверия к открытому ключу пользователя. Доверяющая сторона, имеющая подлинную копию открытого ключа корневого ЦС, содержащегося в СЕРТ$_{ОК}$ корневого ЦС, который она получила по защищённому вспомогательному каналу с использованием некоторого протокола, способна сформировать доверие к привязке между открытым ключом пользователя и именем пользователя.

ПП корневого ЦС, отображаемый, как правило, в формате уникального имени, должен быть известен и распознаваем пользователями и доверяющими сторонами с целью формирования реального доверия к корневому ЦС. Без распознавания ПП корневого ЦС невозможно узнать, кому принадлежит и что отражает самоподписанный СЕРТ$_{ОК}$ корневого ЦС. Это, возможно, обеспечивает зависимость от сертифицированного ключа, например, в интересах аутентификации и проверки ЭП. Кроме того, владельцы открытых ключей обязаны доверять корневому ЦС с целью проведения аутентификации их открытых ключей, например, путём

участия в безопасном распределении корневого открытого ключа среди предполагаемых доверяющих сторон (участников информационного взаимодействия). Пользователи и доверяющие стороны могут получить гарантии такого доверия, например, за счёт того, что востребованные корневой и промежуточные ЦС будут аккредитованы федеральными органами исполнительной власти или другими уполномоченными органами с целью обеспечения процедур регистрации ПП и сертификации открытых ключей. Это означает наличие *доверенного «замыкающего» ЦС* (ДЗЦС, *anchor*) в интересах пользователей и доверяющих сторон.

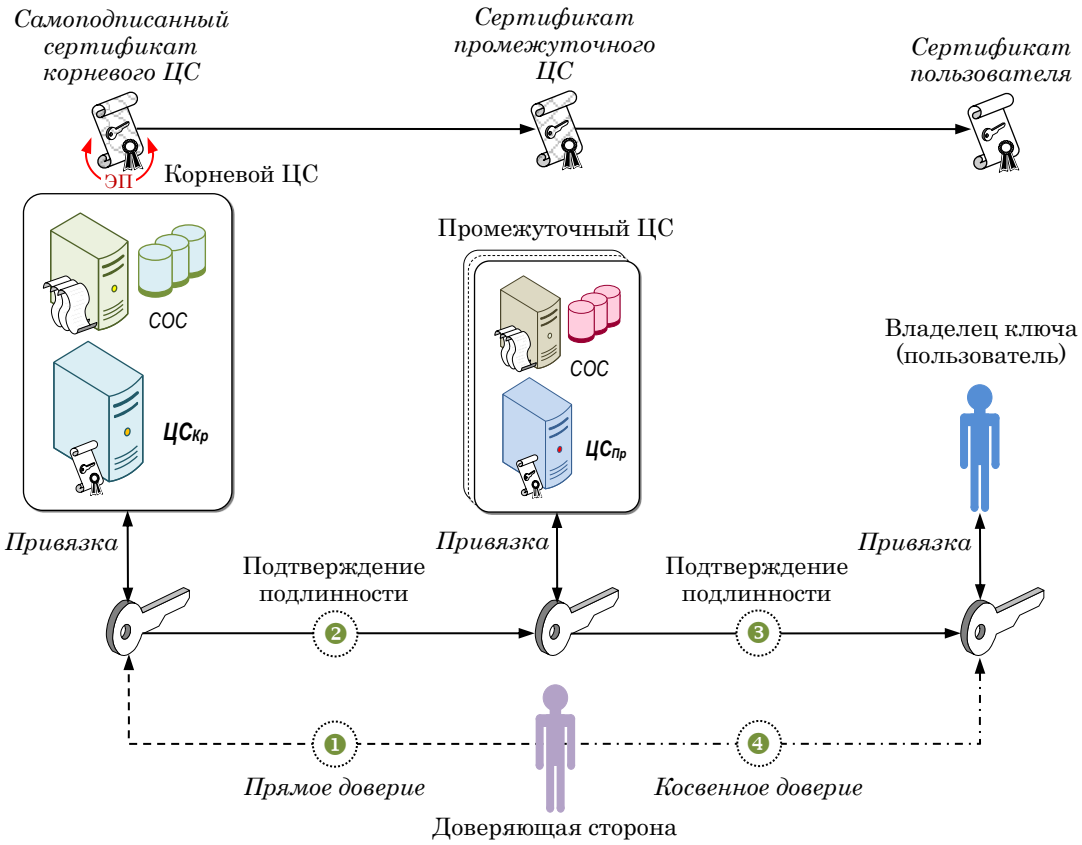

Рисунок 4.13 – Структура доверия при подтверждении подлинности СЕРТ$_{ОК}$

Если организация-владелец корневого ЦС аккредитована федеральными органами исполнительной власти или иными уполномоченными организациями, то решение доверять или нет корневому ЦС, в конечном счёте, становится политическим и философским вопросом. Для ИОК, которая используется только внутри организации, администрация компании представляет собой наивысший орган формирования корневого ЦС в качестве ДЗЦС. В социальных сетях между людьми решение доверять или нет открытому ключу или СЕРТ$_{ОК}$ может быть избирательным и основанным, как правило, на персональных взаимосвязях.

В некоторых ИОК ЦС формируют пару («открытый/закрытый») ключей от имени пользователя. Кроме того, возможна ситуация, когда пользователи сами формируют свои собствен-

ные пары («открытых/закрытых») ключей, в таком случае ЦС обязан проверить, что пользователи обладают закрытым ключом, соответствующим открытому ключу, подлежащему подписи ЦС. Формирует ли подписывающая сторона открытые и закрытые ключи для владельцев или получает их от владельцев – это исключительно практический вопрос и не имеет значения для конкретной ИОК-модели доверия. Тем не менее, следует заметить, что ЦС, который формирует пару «открытый/закрытый» ключей для пользователя, способен, с технической точки зрения, проводить атаки типа «маскарад», надевая маски пользователей, и расшифровывать конфиденциальные сообщения, переданные пользователям, поэтому должна быть уверенность в том, что ЦС не сделает этого. Доверие к ПП, обеспечиваемое ИОК, является таким же сильным, как и основополагающие доверительные взаимосвязи, показанные в нижней части рисунка 4.12. Предполагается, что доверительные взаимосвязи между ПП, начиная от корневого до промежуточного ЦС и далее до пользователей, формируются, как правило, с использованием вспомогательных (дополнительных) каналов связи. Это отражает прямые непосредственные доверительные взаимосвязи, которые формируют основу доверия в ИОК. Такие доверительные взаимосвязи весьма затратны, но предполагается, что дальнейшая автоматизация широкомасштабного распространения и проверки пользовательских $СЕРТ_{ОК}$ сделает реально действующие ИОК эффективными (самоокупаемыми).

Конкретный способ формирования доверительных взаимосвязей, отображённых в нижней части рисунка 4.12, должен устанавливаться политикой сертификации (*certification policy*). *Для $СЕРТ_{ОК}$ с низким уровнем гарантированности может потребоваться*, чтобы ПП предоставлялся в ЦС в интерактивном режиме в формате адреса электронной почты, и чтобы проверка претендента на предмет владения им конкретного адреса электронной почты проводилась путём передачи сообщения на указанный адрес и требования отправки конкретного ответного сообщения. *Для $СЕРТ_{ОК}$ с высоким уровнем гарантированности может потребоваться*, чтобы пользователь (физическое лицо) или представитель организации-пользователя непосредственно прибывал в ЦС/ЦР с удостоверением личности или с документами, подтверждающими его полномочия.

$СЕРТ_{АТ}$ могут отображать всё то, что субъект сертификации захочет указать в сертификате или в соответствующей политике. Типовыми примерами, включёнными в состав $СЕРТ_{АТ}$, являются права должностных лиц и привилегированного доступа. Далее рассматриваются наиболее важные модели ИОК и обеспечиваемые ими доверенные взаимосвязи.

4.10.1 Одиночная иерархическая ИОК

Класс ИОК с наиболее оптимальными характеристиками распределения ключей – это такой класс, в котором все пользователи зависят от одиночной иерархической ИОК (одиночная ИОК-иерархия). Преимуществом такой структуры является то, что только один корневой открытый ключ подлежит распределению среди доверяющих сторон с помощью дополнительного (вспомогательного) канала связи. Более конкретно, каждая доверяющая сторона обязана иметь гарантии того, что полученный открытый ключ корневого ЦС – подлинный. Следует заметить, что корневому открытому ключу могут доверять только те субъекты, которые обладают такими гарантиями, и что он должен быть распределён субъектами, которые не могут получить такие гарантии.

Корневой ЦС, представляющий общепризнанную организацию, обязан быть доверенным. А сама организация должна быть компетентной и, возможно, аккредитованной федеральным органом исполнительной власти или иным уполномоченным органом для осуществления деятельности по регистрации ПП и сертификации открытых ключей. Как упоминалось ранее, *подлинность корневого открытого ключа должна подтверждаться внешними по отношению к самой ИОК средствами*. Доверенный корневой ЦС, обладающий открытым ключом, который был аутентифицирован с использованием вспомогательного (дополнительного) канала связи, называется ДЗЦС.

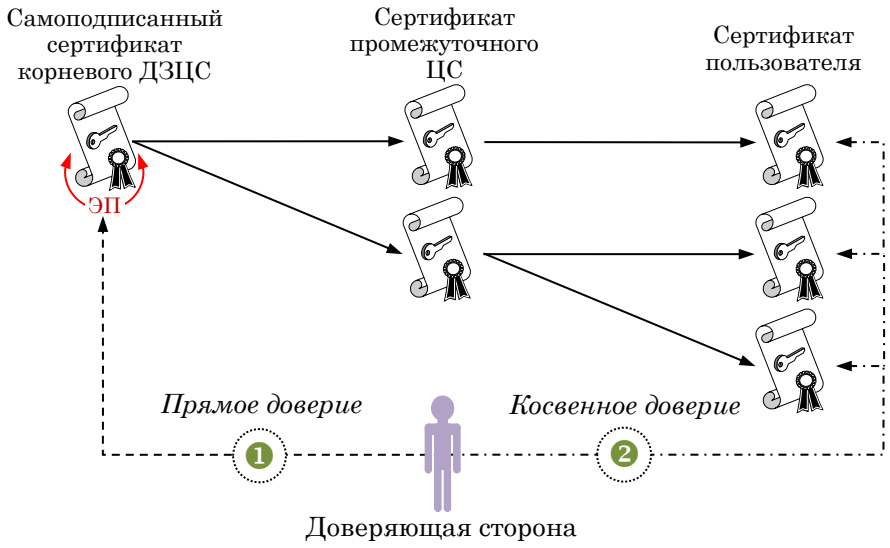

Рисунок 4.14 – Иерархическая ИОК

На рис. 4.14 представлена иерархическая ИОК, «привязанная» к самоподписанному сертификату ДЗЦС. Полагая, что доверяющая сторона получила $СЕРТ_{ОК}$ пользователя, и что корневой ЦС представляет собой ДЗЦС, проверяющая сторона способна аутентифицировать

СЕРТ$_{ОК}$ на основе решения о маршруте сертификации от корневого ЦС до СЕРТ$_{ОК}$ пользователя, который содержит открытый ключ. Кроме того, предполагается, что все промежуточные СЕРТ$_{ОК}$ на маршруте, начиная от корневого до СЕРТ$_{ОК}$ пользователя, также доступны для получателя.

Одиночная иерархическая ИОК может функционировать в интересах одной организации, которая обслуживает корневой и несколько промежуточных ЦС, или нескольких организаций под управлением одного общего корневого ЦС.

4.10.2 Многоиерархическая ИОК

При использовании многоиерархической ИОК возможен случай, когда СЕРТ$_{ОК}$ различных пользователей принадлежат различным ИОК-иерархиям. Полагая, что каждая доверяющая сторона должна быть способной подтвердить подлинность любого СЕРТ$_{ОК}$ пользователя любой ИОК-иерархии, необходимо, чтобы все корневые ЦС были ДЗЦС для доверяющих сторон. Другими словами, всем доверяющим сторонам необходимо получить открытый ключ каждого корневого ЦС по защищённому вспомогательному (дополнительному) каналу связи (рисунок 4.15).

Основная проблема такой модели – увеличение нагрузки на проверяющие стороны при получении СЕРТ$_{ОК}$ корневых ЦС по вспомогательным (дополнительным) каналам связи. Как отмечалось ранее, такие каналы весьма затратны, и поэтому такая ИОК-модель плохо масштабируется. Наличие динамического множества СЕРТ$_{ОК}$ корневых ЦС только усугубляет эту проблему.

Одной из форм реализации такой ИОК-модели является так называемая ИОК на основе всемирной ГИТС (*Web*-инфраструктура, *Web*/ИОК-модель), которая реализуется совместно *Web*-обозревателями. Каналом распределения СЕРТ$_{ОК}$ корневых ЦС является их точное встраивание в КПО *Web*-обозревателей (*Web*-КПО), которые распределяются по всемирной ГИТС.

Однако, весьма сомнительно, что распределение *Web*-КПО во всемирной ГИТС основано на использовании защищённого вспомогательного канала связи. Точное встраивание СЕРТ$_{ОК}$ корневых ЦС в *Web*-КПО обеспечивает автоматическое подтверждение подлинности СЕРТ$_{ОК}$ сервера на основе использования TLS-протокола и проверки цифровых подписей, защищающих целостность КПО. В КПО любых наиболее важных *Web*-обозревателей встроено несколько десятков СЕРТ$_{ОК}$ корневых ЦС. Например, *Web*-обозреватель корпорации *Microsoft* (*Internet Explorer*) включает перечень корневых СЕРТ$_{ОК}$, который может быть просмотрен путём последовательного набора следующих команд: «*Tools*» → «*Internet Options*» → «*Content*» → «*Certificates*» → «*Trusted Root Certification Authorities*».

Как правило, срок действия значительной части предварительно установленных в *Web*-обозревателе корневых СЕРТ$_{ОК}$ истёк ещё несколько лет назад, что характерно и для недавно загруженных *Web*-обозревателей. Просроченные СЕРТ$_{ОК}$ поставляются вместе с *Web*-обозревателями, например, чтобы обеспечить проверку устаревшего ПО, но, как показывает практика, такая модель в действительности не работает. Игнорирование срока действия, указанного в СЕРТ$_{ОК}$, ради устаревшей функциональности является нарушением политики, в соответствии с которой были выпущены СЕРТ$_{ОК}$.

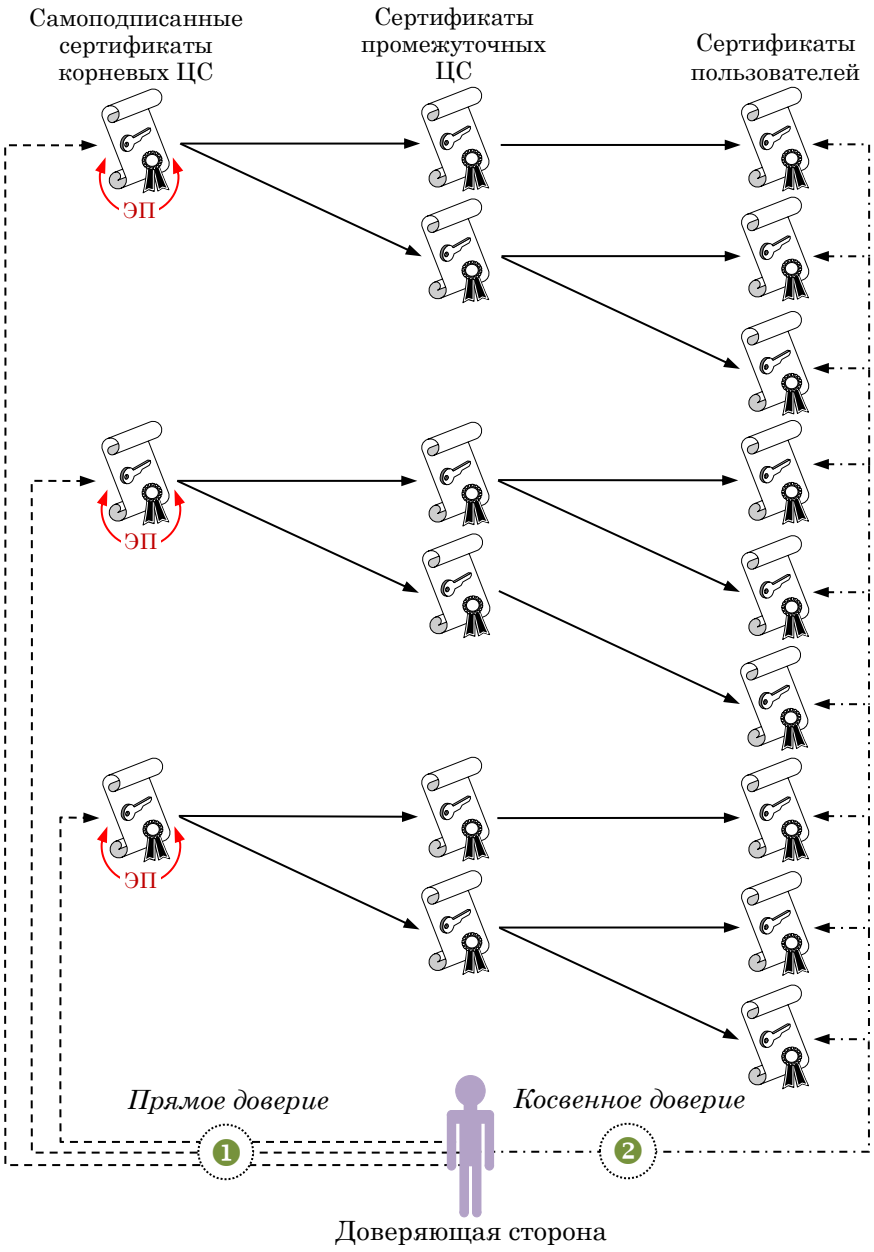

Рисунок 4.15 – Многоиерархическая ИОК

Набор СЕРТ$_{ОК}$ корневых ЦС в *Web*-инфраструктуре является изменяемым, а это означает, что корневые СЕРТ$_{ОК}$ могут быть удалены, и что могут быть добавлены новые корневые СЕРТ$_{ОК}$. А это представляет реальную угрозу типа «подмена», так как злоумышленники могут

заменить подлинный корневой СЕРТ$_{ОК}$ на фиктивный. Подобная атака может быть проведена, например, с помощью вредоносного ПО, которое было встроено в компьютер объекта атаки («жертвы»). Подлинность корневых СЕРТ$_{ОК}$ зависит от защищённости вспомогательного (дополнительного) канала, который обеспечивает их доставку получателям. После того, как фиктивный СЕРТ$_{ОК}$ был инсталлирован, например, вследствие незащищённости канала встраивания, доверяющая сторона будет не способна проверить, что такой СЕРТ$_{ОК}$ – действительно фиктивный. На практике, многие пользователи устанавливают СЕРТ$_{ОК}$ в *Web*-обозреватель и даже корневые СЕРТ$_{ОК}$ на основе самостоятельных случайных решений о доверии. Это означает наличие реальной угрозы подмены ПП во всемирной ГИТС.

К сожалению, *Web/PKI*-модель обладает серьёзными уязвимостями. Дело в том, что *Web*-инфраструктура, фактически, безопасна настолько, насколько безопасна входящая в неё отдельная ИОК с самым низким уровнем защищённости, а каждая отдельная ИОК безопасна настолько, насколько безопасен входящий в неё ЦС с самым низким уровнем защищённости. Таким образом, чем больше корневых СЕРТ$_{ОК}$ и чем больше подчинённых ЦС входят в состав *Web*-инфраструктуры, тем менее защищённой становится сама *Web*-инфраструктура. Существует несколько реальных способов злонамеренного использования уязвимостей *Web*-инфраструктуры, которые описаны ниже [156,157].

1. Атака на ЦС. В 2001 году корпорация *VeriSign* (владеющая одним из крупнейших в мире ЦС) выпустила фиктивные СЕРТ$_{ОК}$ на имя корпорации *Microsoft*. Это стало следствием того, что персонал *VeriSign* не смог установить принадлежность лиц, приобретающих СЕРТ$_{ОК}$, корпорации *Microsoft* [153]. Фальшивые СЕРТ$_{ОК}$ никогда не использовались, а корпорация *VeriSign* пережила это нарушение, слегка «подпортив» свою репутацию. В 2001 году голландский ЦС *DigiNotar* был атакован хакерами с целью получения ими доступа к системам *DigiNotar* и формирования фальшивых СЕРТ$_{ОК}$. Эти СЕРТ$_{ОК}$ использовались преступниками для проведения атак типа «перехват и анализ трафика» (*man-in-the-middle*) против интерактивных служб корпорации *Google* [158]. Через несколько месяцев ЦС *DigiNotar* был объявлен банкротом.

2. Давление или шантаж ЦС. В рамках дела «*Stuxnet*» [159] две отдельные тайваньские компании-разработчики КПО – *Realtek Semiconductor Systems* и *JMicron Technology Corp* – использовали свои подлинные СЕРТ$_{ОК}$, предназначенные для подписи КПО, для формирования цифровых подписей вредоносного КПО «*Stuxnet*», что позволило злоумышленникам внедрить вредоносный КПО во внутренние компьютерные системы предприятий атомной отрасли Ирана. Указанные компании не подверглись санкциям, и поэтому вполне вероятно, что *их принудили к применению своих закрытых ключей для подписи* КПО «*Stuxnet*».

3. Нелегальные ЦС. С технической точки зрения, любой ЦС, входящий в *Web*-инфраструктуру, способен формировать фиктивные СЕРТ$_{ОК}$ и подписи, которые будут автоматически и повсеместно признаваться всеми стандартными компьютерами. Нелегальные ЦС или, с другой стороны, недобросовестные сотрудники легальных ЦС могут получить значительные финансовые прибыли от своей противоправной деятельности, связанной с выпуском фиктивных СЕРТ$_{ОК}$ или формированием фиктивных подписей (рисунок 1.3). В Российской Федерации также имели место аналогичные правонарушения [3,143…146].

Рынок *Web*-инфраструктур в основном принадлежит небольшому числу транснациональных компаний. Этот рынок имеет значительные барьеры для входа в него, так как новые ЦС должны проходить ежегодный аудит безопасности (например, «*Web-Trust3*» для центров сертификации: *http://www.Webtrust.org/*) для включения в список доверенных ЦС, содержащийся в *Web*-обозревателях. После того, как ЦС будет включён в состав сообщества *Web*-инфраструктуры, его корневой СЕРТ$_{ОК}$ будет включён в КПО основных *Web*-обозревателей и другие прикладные КПО, которые распространены среди миллиардов пользователей по всему миру. В КПО было включено более 50 корневых СЕРТ$_{ОК}$, и, таким образом, они автоматически стали доверенными для наиболее популярных *Web*-обозревателей. В обзоре от компании *Netcraft* за 2009 год [160] составлен рейтинг компаний на рынке СЕРТ$_{ОК}$ *Web*-инфраструктуры: *VeriSign* и её дочерние (приобретённые) компании (включая *Thawte* и *Geotrust*) занимают 47,5% затем идут *GoDaddy* (23,4%) и *Comodo* (15,44%).

4.10.3 Избираемое прямое доверие

Модель избираемого прямого доверия – неофициальная ИОК-модель, так как она нарушает основополагающие принципы ИОК-доверия. Она рассматривается только потому, что она получила широкое распространение в Интернет-сети и в других областях, в которых используются ИОК. В модели избираемого прямого доверия доверяющая сторона получает СЕРТ$_{ОК}$ пользователя – или даже корневой СЕРТ$_{ОК}$ – в интерактивном режиме, и выборочно принимает решение о доверии к СЕРТ$_{ОК}$ (рисунок 4.16). Модель избираемого прямого доверия игнорирует требование наличия защищённых вспомогательных каналов для получения корневых СЕРТ$_{ОК}$. Вместо этого, в модели избираемого прямого доверия доверяющая сторона сама решает доверять СЕРТ$_{ОК}$ пользователя без наличия надёжного СЕРТ$_{ОК}$ корневого ЦС в качестве ДЗЦС, либо принимает решение о приобретении корневого СЕРТ$_{ОК}$ без проверки его подлинности. В данном случае, удобство и экономия являются основными причинами такого избирательного доверия к СЕРТ$_{ОК}$.

Данная модель может применяться в ситуациях с небольшими рисками, когда СЕРТ$_{ОК}$ используются в некритичных ИТС. В таких случаях СЕРТ$_{ОК}$ не может быть проверен, потому

что нет доступного корневого ЦС (или его СЕРТ$_{ОК}$), либо потому что политика подтверждения подлинности не может быть реализована, например, когда истёк срок действия корневого СЕРТ$_{ОК}$. СЕРТ$_{ОК}$, который не прошёл стандартную процедуру подтверждения подлинности, как правило, блокируется, с точки зрения доступа к службе, но до тех пор, пока СЕРТ$_{ОК}$ не будет признан некоторым иным способом. В таких ситуациях доверяющая сторона может просто принять избирательное решение о доверии к СЕРТ$_{ОК}$ с целью получения доступа к службе. Однако, данная модель обычно используется в ситуациях, когда существует реальный риск, например, при загрузке и установке КПО.

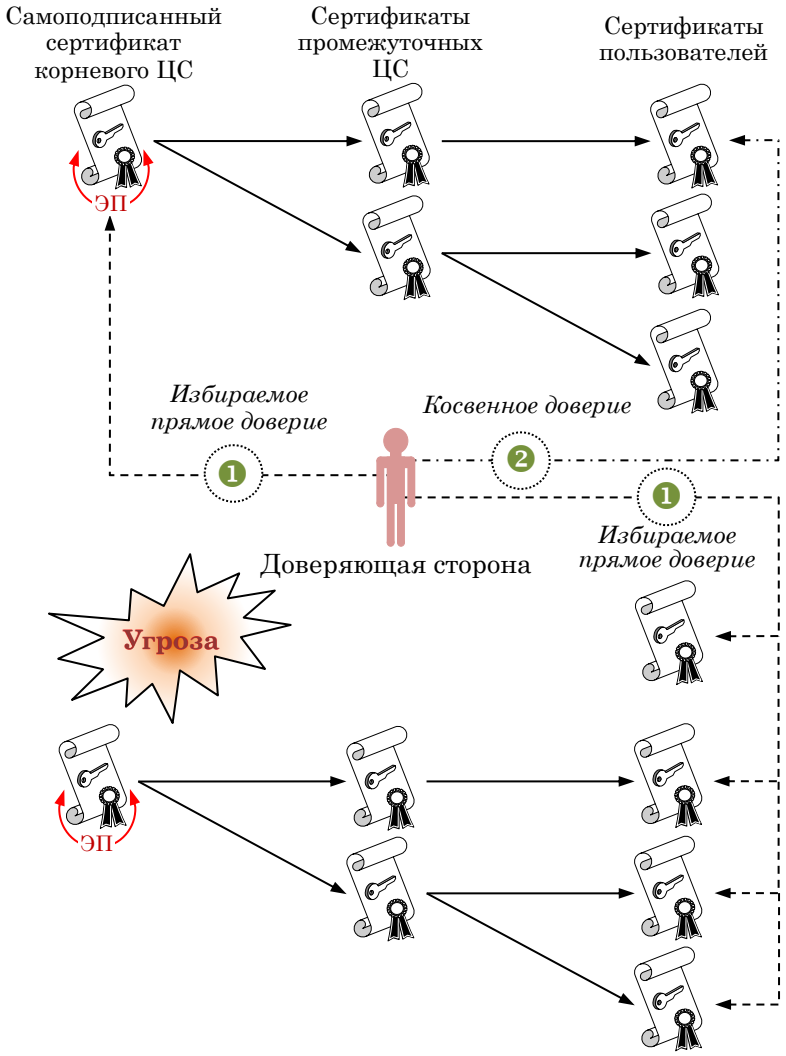

Рисунок 4.16 – Решения относительно избираемого прямого доверия

Проблема этой модели заключается в том, что двоичные решения о доверии (т.е. доверять или нет) принимаются исключительно по причине «удобства», несмотря на наличие слабого или на полное отсутствие прямого доверия. Можно утверждать, что эта проблема затрагивает все модели ИОК-доверия, так как во многих случаях доверяющие стороны просто иг-

норируют существование корневых СЕРТ$_{ОК}$, а если проверяющие стороны и знают о существовании корневых СЕРТ$_{ОК}$, то зачастую существует слишком мало или вообще нет каких-либо данных для подтверждения подлинности таких СЕРТ$_{ОК}$.

Это – фундаментальная проблема для всех ИОК. Наличие синтаксической цепочки СЕРТ$_{ОК}$ от корневых ЦС до пользователей само по себе бессмысленно, но если цепочки СЕРТ$_{ОК}$ имеют надёжный ДЗЦС, то они могут быть основой обеспечения надёжного доверия. Таким образом, *рекомендация* здесь может быть только одна: *доверяющие стороны должны избегать принятия решений об избирательном доверии в ИОК!*

4.10.4 Взаимная сертификация нескольких корневых ЦС

С теоретической точки зрения, самым простым способом снижения нагрузки на доверяющие стороны – позволить корневым ЦС *взаимно сертифицировать* (*cross certification*) свои СЕРТ$_{ОК}$. В таком случае, каждой доверяющей стороне необходимо получить СЕРТ$_{ОК}$ только одного корневого ЦС, и при этом она будет по-прежнему способна проверить подлинность СЕРТ$_{ОК}$ любого пользователя, расположенного в другой ИОК-иерархии (рисунок 4.17).

Недостаток модели со взаимно-сертифицированными ИОК-иерархиями заключается в том, что значительно увеличивается нагрузка на корневые ЦС, так как каждый корневой ЦС должен взаимно сертифицировать СЕРТ$_{ОК}$ всех остальных корневых ЦС. Число необходимых процедур взаимной сертификации равно $(n(n-1)/2)$, где n – число отдельных ИОК-иерархий. Это похоже на число симметричных ключей, которое необходимо в сетевом сообществе из n субъектов. Для каждой процедуры взаимной сертификации необходимо сформировать свою политику сертификации, и это может привести к значительному росту нагрузки на корневые ЦС, а некоторые ЦС могут отказаться от участия в процедурах взаимной сертификации, например, по политическим соображениям. Поэтому модель со взаимно-сертифицированными ИОК-иерархиями плохо масштабируется и нецелесообразна для практического применения.

4.10.5 ИОК-модель со связующим ЦС

Повышение эффективности предыдущей ИОК-модели можно обеспечить за счёт использования СЦС, связывающего несколько корневых ЦС (*bridge CA*). Преимущество такого решения заключается в том, что доверяющим сторонам необходимо получить СЕРТ$_{ОК}$ только одного корневого ЦС, используя для этого защищённый вспомогательный канал связи, и в том, что каждому корневому ЦС необходимо взаимно сертифицироваться только со связующим ЦС (рисунок 4.18).

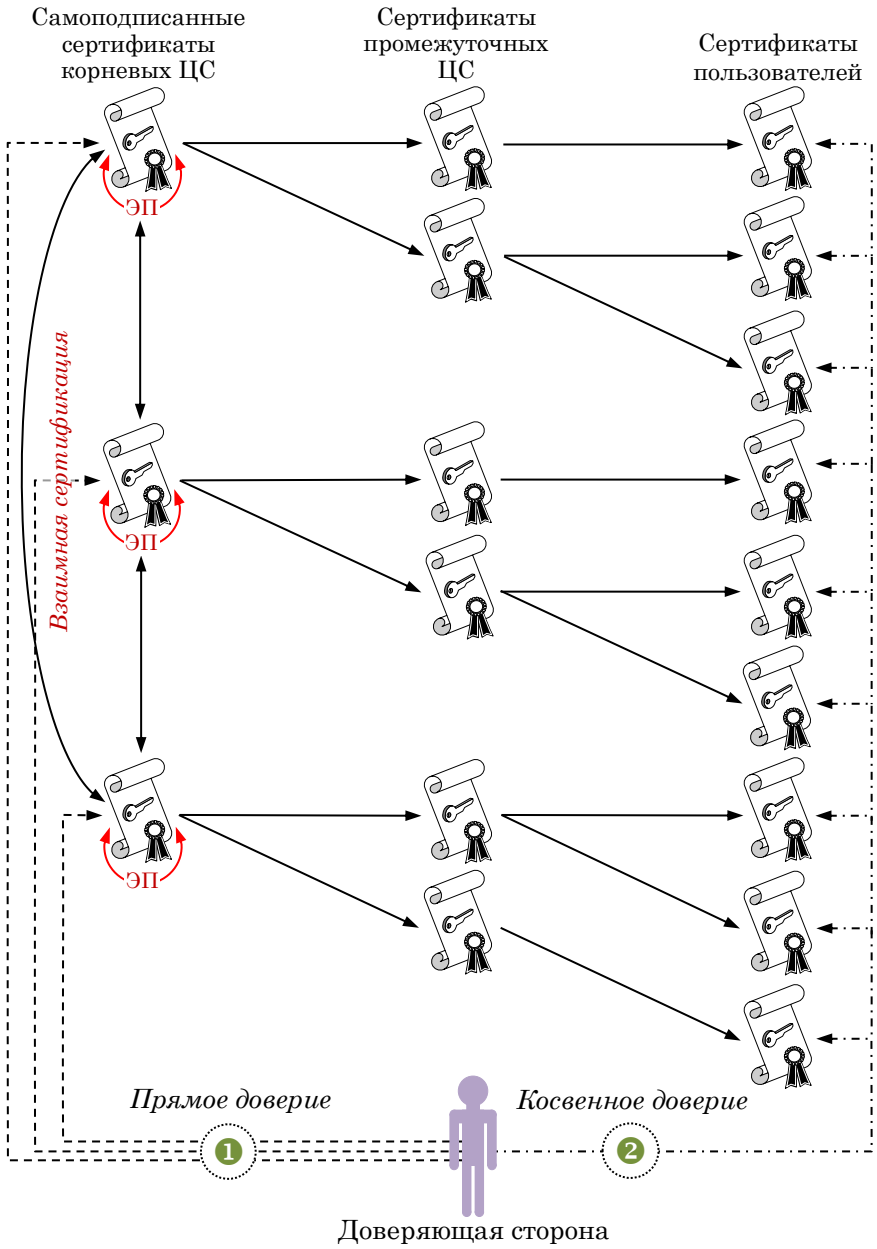

Рисунок 4.17 – Взаимно-сертифицированные ИОК-иерархии

Недостаток ИОК-модели со связующим ЦС заключается в том, что формирование приемлемой для всех сторон политики взаимной сертификации может быть чрезвычайно трудной задачей. Некоторые корневые ЦС могут отказаться от взаимной сертификации со связующим ЦС, например, по политическим причинам. В свою очередь, и связующий ЦС может отказаться от взаимной сертификации с корневым ЦС по аналогичным причинам.

4.10.6 PGP-модель доверия

Коммерческий КПО шифрования, именуемый как *PGP* (*Pretty Good Privacy*, буквально «хорошее средство обеспечения неприкосновенности», [102]) и его свободно распро-

страняемая версия *GPG* (*GNU Privacy Guard*, буквально «средство защиты неприкосновенности на основе ОС (UNIX-подобной) *GNU*», [103]) представляют собой систему обеспечения открытыми ключами и СЕРТок.

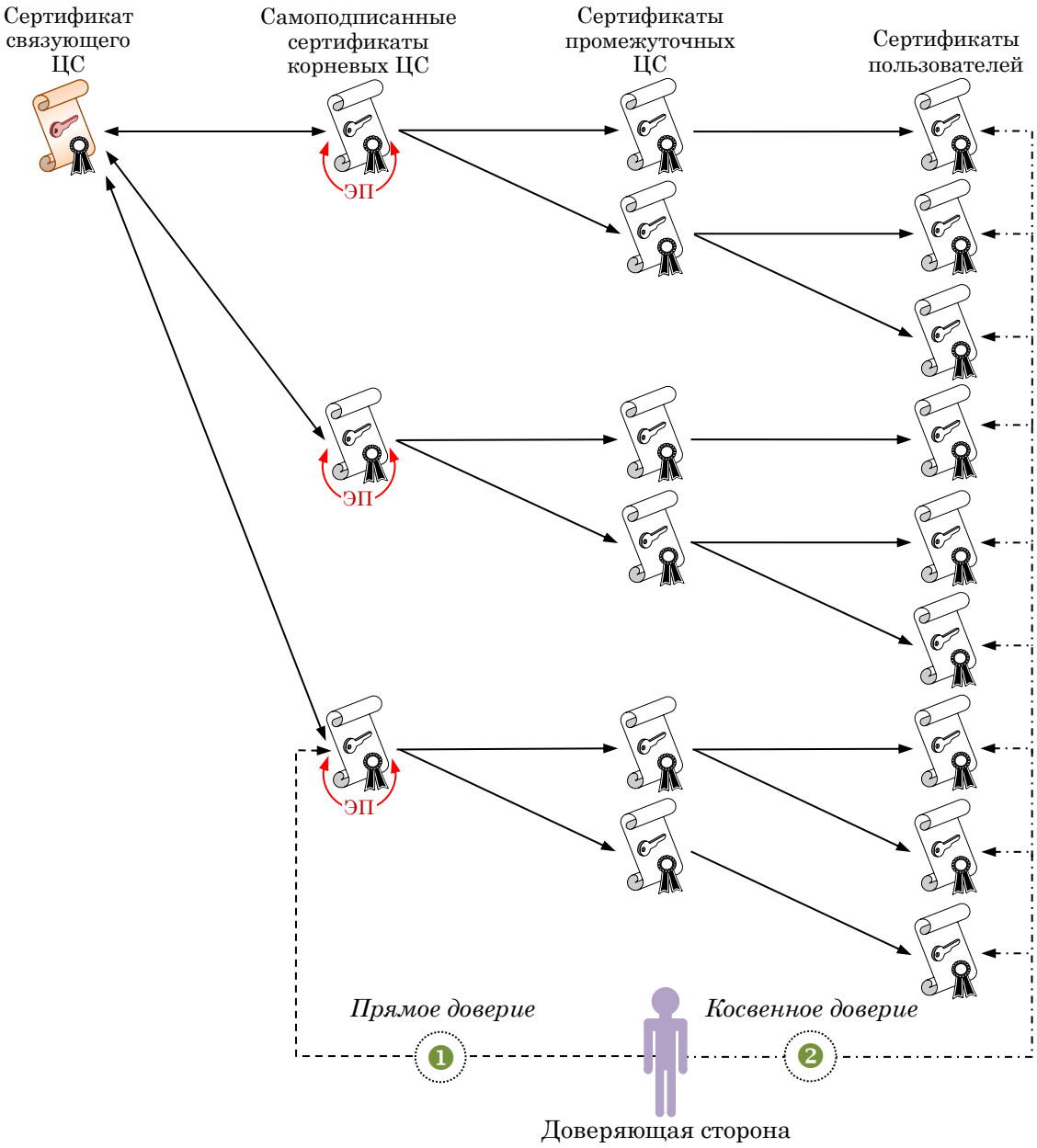

Рисунок 4.18 – ИОК-модель с ЦС, связывающим несколько ИОК-иерархий

PGP-инфраструктура представляет практическую модель распространения и использования открытых ключей, и, следовательно, является ИОК, но *не является иерархической моделью*, т.е. не основана на иерархической модели. В *PGP*-инфраструктуре каждый её участник выполняет функции доверяющей стороны, т.е. функции пользователя и ЦС одновременно, а это означает, что пользователи могут передавать и рекомендовать СЕРТок друг другу.

Существует несколько способов получения пользователем и доверяющей стороной открытых ключей друг друга. Можно использовать защищённый вспомогательный канал, например, личная встреча, можно использовать интерактивный канал взаимодействия для принятия решения о доверии, основанного на введении новых $СЕРТ_{ОК}$ от предыдущих доверенных пользователей, или можно использовать принятое избирательное решение о доверии при получении открытого ключа, например, в сообщении электронной почты, или скопированного с *Web*-сайта. Полученные открытые ключи хранятся в файле, называемом *кольцо открытых ключей* (*public-key ring*, рисунок 4.19). Доверяющая сторона может подписать полученные ключи и определить уровень доверия к ключу, так как он храниться в файле *Public-Key Ring*. Избирательное доверие должно быть основано на реальном доказательстве, например, подтверждение по телефону того, что открытый ключ был передан с использованием системы электронной почты, с последующей проверкой, того, что электронное почтовое сообщение было получено своевременно, как и предполагалось. В противном случае, такие решения о доверии будут иметь слабое обоснование.

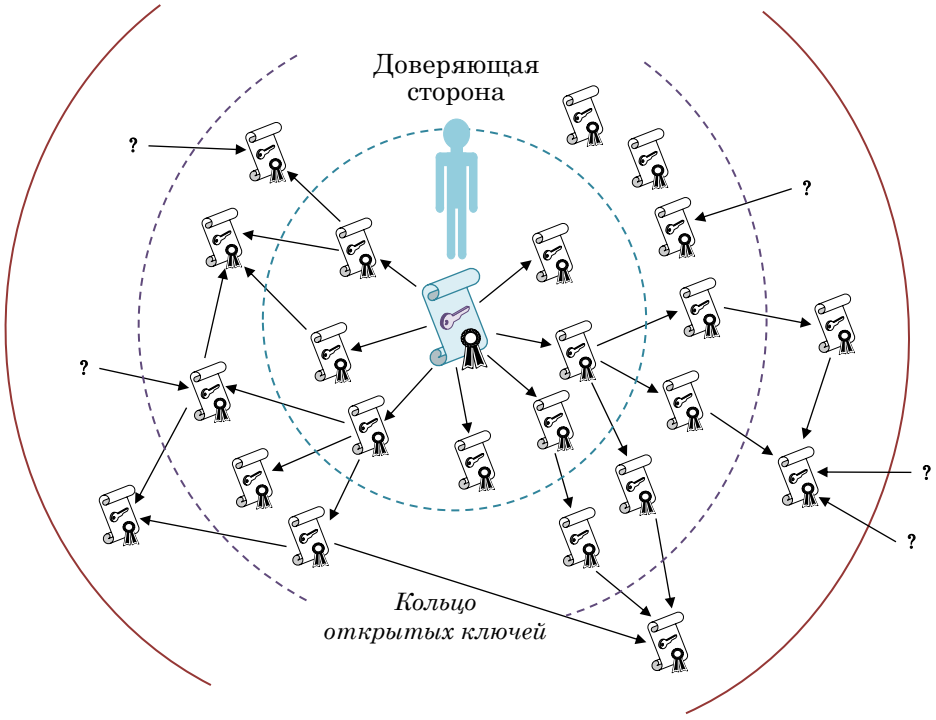

Рисунок 4.19 – *PGP/PKI*-инфраструктура

Общее доверие к полученным ключам формируется на основе использования соответствующей *PGP*-модели доверия, которая представлена в [102]. Например, программный *PGP*-модуль может быть настроен так, что доверие к полученному открытому ключа будет сформировано только в том случае, когда он будет подписан определённым числом доверенных

пользователей. Как правило, программный *PGP*-модуль не доверяет полученному ключу, который был подписан неизвестными или не доверенными пользователями, но доверяющая сторона всегда может принять решение об избранном доверии к ключу и подписать полученный открытый ключ.

Следует заметить, что никто не делает бизнес на продаже $СЕРТ_{ОК}$ (т.е. подписанных ключей) для *PGP*-инфраструктуры, поэтому нет и бизнес-модели для использования ЦС в рамках *PGP*-модели. Физические лица и организации пользуются *PGP/GPG*-инфраструктурой по причине её простоты и низкой начальной стоимости. Популярность *PGP/GPG*-инфраструктуры – следствие простоты её использования, а также того, что она удовлетворяет реальные потребности пользователей.

4.10.7 ИОК с центром подтверждения подлинности сертификатов

Задача получения открытых ключей корневого ЦС с использованием защищённых вспомогательных каналов и ПРП $СЕРТ_{ОК}$ пользователей является основной (иногда нежелательной) нагрузкой для проверяющих сторон. Введение отдельной функции по снижению указанной нагрузки и проведению ПРП $СЕРТ_{ОК}$ пользователей, реализуемой от имени доверяющей стороны, основано на использовании нового ДЗЦС, именуемого *центром подтверждения подлинности* (ЦПП[32], рисунок 4.20).

Однако нет необходимости, чтобы ЦПП был ЦС. Организация может выполнять функции, либо только ЦС, либо только ЦПП, либо обоих центров одновременно. Для проведения ПРП $СЕРТ_{ОК}$ необходимо, чтобы доверяющая сторона могла установить защищённое виртуальное соединение с ЦПП. А такому виртуальному соединению должна предшествовать первоначальная процедура обмена криптографическими ключами на основе защищённого вспомогательного канала связи. ПРП отличается от процедуры сертификации, так как первоначальный обмен ключами не обязательно должен основываться на криптографии с открытыми ключами. Например, возможен первоначальный обмен симметричными ключами.

Необходимо учитывать два важных аспекта обеспечения безопасности, во-первых, доверяющая сторона должна иметь возможность аутентифицировать ЦПП, чтобы сформировать доверие к $СЕРТ_{ОК}$ с подтверждённой подлинностью. И во-вторых, может потребоваться аутентификация доверяющей стороны ЦПП в целях предоставления ей доступа к самому ЦПП.

Модель ИОК с ЦПП удовлетворяет реальные потребности доверяющих сторон, и отражает современные тенденции в ИОК-индустрии [161]. ЦПП не зависят от ЦС, а их применение

[32] В §3.7.1 рассматривается Западноевропейская модель ИОК, в основе которой лежат национальные ЦПП.

делает возможным объединение нескольких независимых ИОК. Несмотря на то, что широкомасштабные и дорогие, с точки зрения реализации, ИОК часто не соответствуют ожиданиям на рынке, *модель ИОК с ЦПП становится «переломным» фактором*, который может сделать бизнес-модели ИОК жизнеспособными.

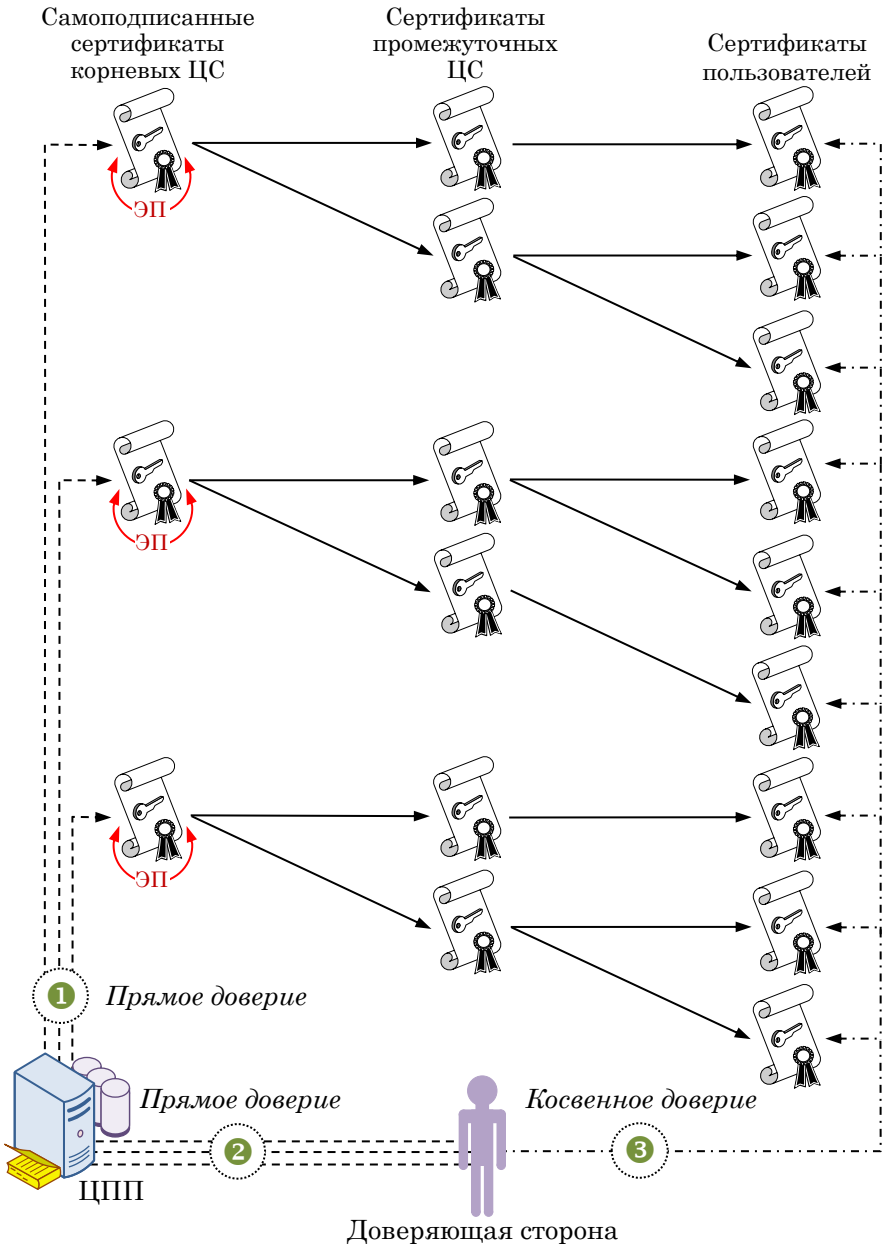

Рисунок 4.20 – Многоиерархическая ИОК с ЦПП

4.10.8 Простая ИОК (простая распределённая инфраструктура обеспечения безопасности) и делегирование сертификатов

Простое расширение классической иерархической ИОК-модели состоит в том, чтобы последовательность $СЕРТ_{ОК}$ начиналась от доверяющей стороны, т.е. доверяющая сторона, фактически, становится ЦС. ИОК-модель такого типа представляет собой, либо простую ИОК (*simple PKI,* SPKI), либо простую распределённая инфраструктура обеспечения безопасности

(*simple distributed security infrastructure*, SDSI), *SPKI/SDSI*-инфраструктуру (рисунок 4.21, [14,155]).

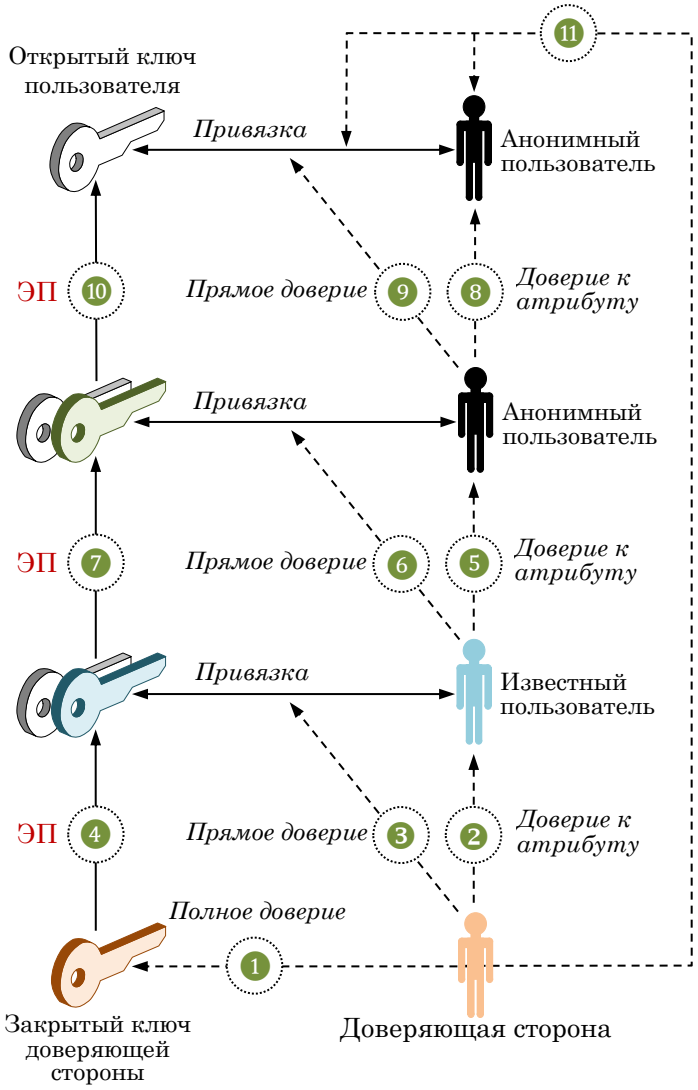

Рисунок 4.21 – *SPKI/SDSI*-модель с известными и анонимными пользователями

Так как каждая сторона, включая доверяющую сторону, реализует функции ЦС, доверительные взаимосвязи в *SPKI/SDSI*-инфраструктуре будут аналогичны внутренним доверительным взаимосвязям в классических ИОК (например, на рисунке 4.12). Такая модель не нашла широкого применения вследствие нескольких причин. Например, в такой модели требуется, чтобы каждая доверяющая сторона получила пару открытый/закрытый ключей, а это усложняет обнаружение цепочки СЕРТ$_{ОК}$, по сравнению с иерархическими моделями.

Одно из начальных требований *SPKI/SDSI*-инфраструктуры заключалось в том, чтобы открытые ключи использовались как уникальные имена. Таким образом, это позволяло пользователям оставаться анонимными, так как они раскрывали только свои интерактивные идентификаторы (индекс «❺» и «❽», рисунок 4.21). Кроме того, пользователи имеют возмож-

ность предоставить свои реальные параметры подлинности (например, биометрические, индекс «❷»), используя для этого вспомогательные каналы связи, а это позволяет сформировать доверие к самим пользователям и их открытым ключам (индекс «❸»). Различие между интерактивным доверием к анонимным пользователям (индексы «❺» и «❽») и доверием к их открытым ключам (индексы «❻» и «❾») едва уловимо.

Имена, отображаемые с помощью открытых ключей, – абстрактные описания, которые не могут сами, как таковые, осуществлять какие-либо процедуры или применять ЭП, это могут делать только пользователи. Более того, необходимо быть уверенным в том, что открытые ключи в *SPKI/SDSI*-инфраструктуре принадлежат реальным пользователям, которым вполне можно доверять. Конечно, пользователь может делегировать свои полномочия по формированию ЭП и сертификации прикладному программному процессу, но при этом необходимо быть уверенным в том, что пользователь, в конечном счёте, контролирует этот процесс.

Доверие к открытому ключу – убеждённость в том, что он корректно и однозначно отображает (принадлежит) предполагаемого(му) пользователя(ю). Смысл доверия к анонимным пользователям (индексы «❺» и «❽») заключается в том, что они корректно выпускают следующий $СЕРТ_{ОК}$ в последовательности (цепочке, индекс «❿»). Несмотря на то, что *SPKI/SDSI*-сертификаты проще, чем X.509-сертификаты, поскольку они не содержат отдельного атрибута в формате уникального имени, как в стандартных X.509-сертификатах, *SPKI/SDSI*-модель доверия является более «изощрённой» и трудной для понимания, чем наиболее распространённые классические ИОК-модели.

Дополнительной сферой применения последовательностей $СЕРТ_{ОК}$ является обеспечение процедуры делегирования, например, с целью авторизации [162]. В частности, это составляет основу для системы авторизации *KeyNote* [163], в которой $СЕРТ_{ОК}$, изданный стороной-подписантом, включает параметры авторизации (полномочия) или привилегии. Доверяющая сторона представляет собой корневой субъект в цепочке делегирования, и способна подтвердить подлинность и, таким образом, доверять полученному $СЕРТ_{ОК}$ в цепочке, а также предоставлять доступ в зависимости от полномочий, указанных в $СЕРТ_{ОК}$. Такой способ представляет собой альтернативу классической модели управления доступом (УД) на основе списка доступа, устанавливающей политики авторизации в системе УД. В случае использования $СЕРТ_{ОК}$, основанного на модели делегирования, системе УД даже не нужно знать биометрический (или ему подобный) параметр подлинности владельца $СЕРТ_{ОК}$, так как процедура авторизации осуществляется на основе интерактивного ПП, отображаемого с помощью открытого ключа. Любой, кто сможет доказать, что он обладает закрытым ключом, соответствующим сертифицированному открытому ключу, получит доступ в соответствии с политикой авторизации, указанной в $СЕРТ_{ОК}$.

4.10.9 ИОК на основе защищённой DNS-системы

Угроз безопасности DNS-системе (*domain name system*, система именования сетевых сегментов/областей) весьма много [164,165], что снижает надёжность DNS-ответов, например, при преобразовании имён сегментов/областей в IP-адреса. Техническое решение указанной проблемы заключается в применении защищённой DNS-системы (DNS *Security Extension*, DNSSEC [166]), которая спроектирована для защиты DNS-клиентов (*resolver*, КПО на стороне Интернет-пользователя) от сфальсифицированных DNS-данных, например, вследствие атак типа «модификация DNS-данных, хранящихся в сверхоперативной памяти (СОП-модулях)». Все ответы, полученные с использованием DNSSEC-системы подписываются с помощью ЭП.

Открытые ключи, используемые при подтверждении подлинности ЭП, распространяются по DNSSEC/PKI-инфраструктуре, которая имеет единственный корневой узел. Путём подтверждения подлинности ЭП, DNS-клиент получает гарантии того, что полученная информация идентична (корректна и обладает полнотой) той информации, которая предоставляется подлинным DNS-сервером, т.е. эта информация не была сфальсифицирована (модифицирована).

Следует отметить, что DNS-узлы (системы именования сегментов/областей) совпадают с узлами *Web*-инфраструктуры, что делает их смежными иерархическими структурами (рисунок 4.22, на котором многоуровневая *Web*-инфраструктура зеркально отображается слева направо). Анализируя структуру на рисунке 4.22, становится очевидным, что иерархическая структура самой DNS-системы может использоваться в качестве ИОК в интересах владельцев СЕРТ$_{ОК}$. Фактически DNSSEC-система уже является «надстройкой» DNS-системы, что позволяет DNS-клиентам аутентифицировать ответы на свои DNS-запросы.

IETF-стандарт [167] вводит TLSA-протокол, основу которого составляет TLS-протокол (*transport layer security*), используемый для аутентификации поименованных DNS-объектов (*DNS-Based Authentication of Named Entities*). TLSA-протокол, в основном, использует DNSSEC-систему в качестве платформы для распределения СЕРТ$_{ОК}$ в интересах TLS-протокола, что, по сути, устраняет требование доверия к ЦС третьих сторон, и, следовательно, обеспечивает более надёжные гарантии безопасности, чем современная *Web*-инфраструктура. Принятие IETF-стандарта [167] и корректное внедрение необходимого КПО позволяет постепенно отказаться от проблемной *Web*-инфраструктуры, описанной выше. Такое решение обеспечивает подписание СЕРТ$_{ОК}$ сервера в DNS-зоне, в которой расположен соответствующий сервер (рисунок 4.23).

Например, сервер интерактивного банковского обслуживания банка *Barclays* называется «*ibank.barclays.co.uk*» и использует СЕРТ$_{ОК}$ для формирования защищённых виртуальных TLS-соединений. СЕРТ$_{ОК}$ этого сервера подписан с помощью закрытого ключа DNS-зоны «*barclays.co.uk*». СЕРТ$_{ОК}$ может храниться как запись ресурса (*resource record*) в DNS-сервере «*barclays.co.uk*» и будет доступен для всех клиентов, обладающих правом доступа к серверу.

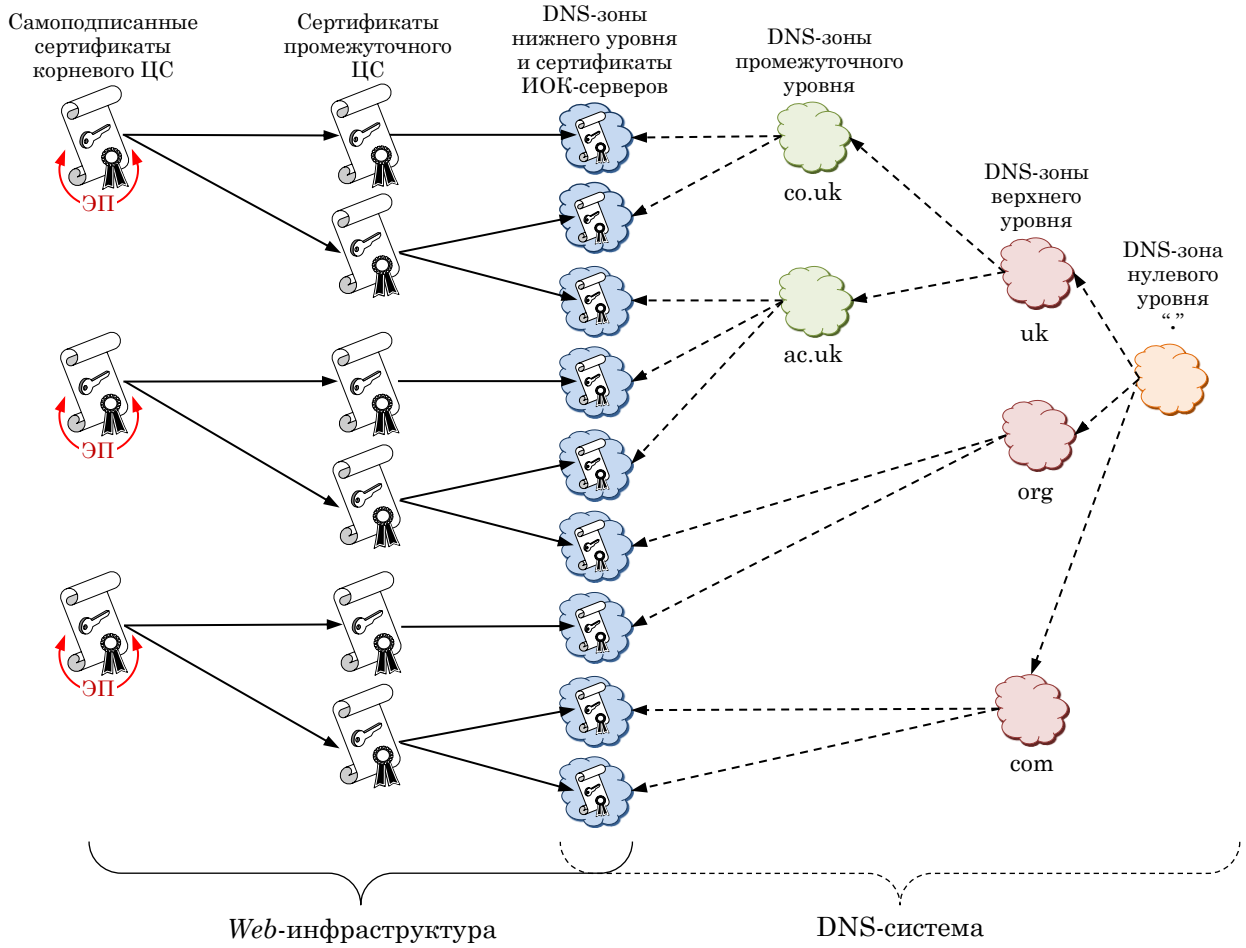

Рисунок 4.22 – Смежная структура, состоящая из DNS-системы и *Web*-инфраструктуры

В случае использования DNSSEC-системы структура доверия требует очень тщательного анализа, а множество субъектов доверия, отображается доверенными лицами в Интернет-сообществе. Интерактивная ПРП корневого открытого ключа DNS-системы невозможна, и, более того, именуется как «*заведомо недопустимая корневая зона*» (*deliberately unvalidatable root zone*). А это означает, что никто не может подтвердить подлинность корневого открытого ключа DNS-системы. Вместо этого, ПРП корневого открытого ключа может быть проведена вручную (или полуавтоматически) с помощью *OpenPGP*-подписей корневого открытого ключа (рисунок 4.23). Так что пока корневой открытый ключ связан с корневой DNS-зоной «**.**», его можно скопировать в интерактивном режиме. А его подлинность может быть

подтверждена с помощью дополнительной процедуры, реализуемой другим прикладным протоколом. Например, администратор DNS-системы может получить один или несколько открытых *OpenPGP*-ключей от пользователей, которым он доверяет, что, в свою очередь, позволяет администратору DNS-системы вручную подтвердить подлинность открытого ключа корневой DNS-зоны.

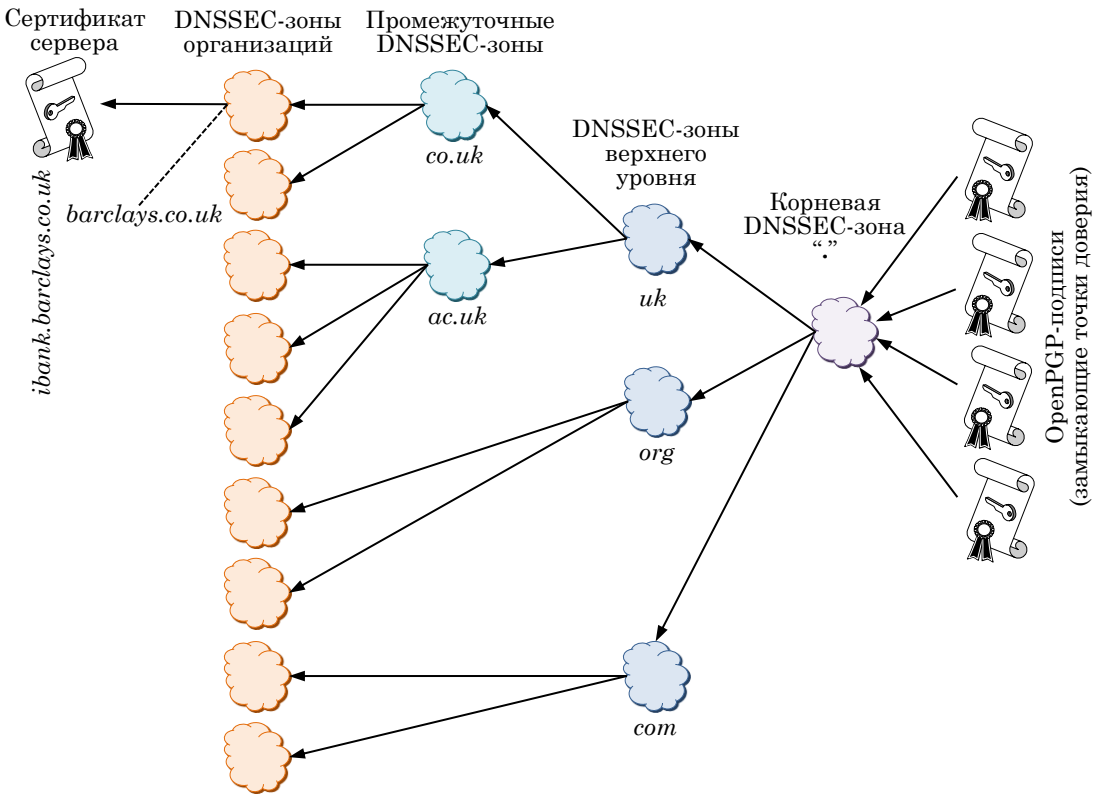

Рисунок 4.23 – DNSSEC-система как платформа для CEPT_{OK} сервера

Такой способ решает проблему зависимости от отдельной структуры доверия в виде *Web*-инфраструктуры, которая, к тому же, должна характеризоваться как «*весьма ненадёжная*». Мало того, что будет повышена надёжность аутентификации сервера, также может быть уменьшена и стоимость системы вследствие упрощения инфраструктуры. В любом случае, когда DNSSEC-система начнёт функционировать, её можно будет использовать в качестве платформы для подписи и распределения CEPT_{OK} сервера.

Тем не менее, о полномасштабном внедрении DNSSEC-системы говорить пока ещё рано, так как существуют объективные проблемы её реализации [168], среди которых, например, резкий рост служебного трафика (по разным оценкам трафик может увеличиться в 6-7 раз), использование TCP-протокола, каждый клиент должен получить хотя бы один доверенный открытый ключ до того момента, как он начнёт использовать DNSSEC, и др.

4.11 Семантика доверия и параметра подлинности

В условиях доверительной взаимосвязи, доверяющая сторона имеет полное или неполное представление о предполагаемом доверии. Область доверия – это определённый(е) тип(ы) доверия, предполагаемый(е) в конкретной доверительной взаимосвязи. Другими словами, считается, что доверенная сторона обладает определёнными качествами, а область доверия означает, что доверяющая сторона предполагает наличие таких качеств.

В случае ИОК, границы доверия определяются политикой сертификации. Для доверяющей стороны важно правильно оценивать границы доверия, отражённые в политике. Некорректное понимание области (границ) доверия к СЕРТ$_{ОК}$ аналогично неправильному доверию, которое становится уязвимостью, которой, в свою очередь, могут воспользоваться злоумышленники. *Типичная ошибка* состоит в том, что СЕРТ$_{ОК}$ с ПП якобы обеспечивают гарантию добропорядочности и надёжности владельца параметра подлинности. Однако, факт прохождения пользователем процедуры аутентификации, ничего не говорит о том, является ли этот пользователь благонадёжным или злонамеренным. Это распространённое недоразумение является, например, основой для атак типа «вскрытие данных (НСД к данным)» (*phishing*).

ЦС стремятся к тому, чтобы избежать какой-либо ответственности, которая может привести к юридическому или финансовому риску, и поэтому типичные политики сертификации содержат юридический жаргон и исключают ответственность. Некоторые ЦС настолько обеспокоены собственной ответственностью, что в поле «наименование издателя сертификата» (*issuer name*) внутри самого СЕРТ$_{ОК}$ специально указывают: «*No Liability Accepted*» (*ответственность исключена*).

Издание СЕРТ$_{ОК}$, обеспечивающих гарантии добропорядочности и надёжности владельца сертификата, практически невозможно, вследствие того, что ЦС должен был бы принять ответственность за риск на себя. Несмотря на то, стандартная политика сертификации может занимать несколько страниц, её суть, как правило, можно выразить в одном простом предложении, например, «*владелец сертифицированного открытого ключа законно владеет указанным именем*» («*the owner of the certified public key rightfully holds the specified name*»). В *Web*-инфраструктуре сетевое имя владельца ключа (или URI) является уникальным именем. Теоретически СЕРТ$_{ОК}$ сервера позволяет доверяющей стороне (пользователю услуг) аутентифицировать подлинность ПП владельца открытого ключа (ПЭУ), но на практике это не всегда возможно из-за несоответствия между уникальным именем (сетевым именем) и ПП ПЭУ, который видит доверяющая сторона. Если уникальное имя, отображающее ПП, не установлено, то процедура аутентификации ПП с помощью уникального имени

становится бессмысленной. Семантическое различие между тем, что сертифицировано, и тем, что сертифицировано по мнению пользователей, является общей проблемой ЭП [141].

Аутентифицировать значит проверить корректность доказательства принадлежности конкретного ПП. В случае положительного результата проверки, ПП считается подтверждённым, а доверяющая сторона может принять решение продолжить транзакцию. В случае отрицательного результата проверки, доверяющая сторона должна приостановить транзакцию. Таким образом, процедура аутентификации предполагает принятие решения доверяющей стороной. Если используется *Web*-инфраструктура, то очень часто невозможно принять обоснованное и полноценное решение, так как в большинстве случаев URI-идентификаторы не имеют никакого смыслового значения для человека, являющегося доверяющей стороной.

Наиболее распространённое применение TLS-протокола – обеспечение функционирования *Web*-инфраструктуры, на что указывает символ в виде «закрытого замка» в углу экранного интерфейса *Web*-обозревателя, т.е. сеанс связи защищён с помощью TLS-протокола. Доверяющая сторона может проверить различную информацию о $СЕРТ_{ОК}$ сервера, но, к сожалению, такая информация не обязательно будет достаточной для того, чтобы принять обоснованное и полноценное решение о ПП *Web*-сервера.

В [92,95] дано следующее определение аутентификации взаимодействующего субъекта: «*подтверждение того, что взаимодействующий субъект является именно тем, за кого себя выдаёт*» («*the corroboration that a peer entity in an association is as claimed*»). Однако, даже если заявленное наименование (имя субъекта) может быть проверено, этого недостаточно, что принять обоснованное решение о доверии, особенно в случае, когда само имя не признано доверяющей стороной. Например, ПП реального ПЭУ, признанный клиентом, – это не одно и тоже, что URI-идентификатор того же самого реального ПЭУ, признанный клиентом TLS-протокола. Следовательно, ПЭУ – субъект, имеющий несколько ПП.

С точки зрения клиента, простое имя и логотип ПЭУ составляют большую часть ПП. А с точки зрения *Web*-обозревателя пользователя, такой ПП не может использоваться, так как обычные имена неоднозначны, а визуальные/графические логотипы не могут однозначно интерпретироваться.

$СЕРТ_{ОК}$, которые должны быть обязательно однозначными, требуют глобально уникальных имён, которые необходимы для обеспечения эффективной автоматизированной обработки. Наименования сетевых сегментов, в большинстве случаев, удовлетворяют этому требованию (несмотря на то, что со временем они могут изменяться), и поэтому они были выбраны для отображения ПП интерактивных ПЭУ в $СЕРТ_{ОК}$ серверов. Очевидно, что наличие различных ПП одного и того же пользователя может повлечь за собой возникновение проблемы. С теоретической точки зрения, решением этой проблемы могло бы стать требование к

доверяющим сторонам, чтобы последние были способны идентифицировать интерактивных ПЭУ по именам сетевых сегментов, в которых они расположены. К сожалению, следствием такого решения – риски для ПЭУ, которые часто используют несколько и различные имена сетевых сегментов в зависимости от конкретной предоставляемой ими услуги.

Практика показывает, что защищённый *Web*-сайт организации имеет URI-идентификатор с неочевидным наименованием сетевого сегмента, который не соответствует имени сетевого сегмента, в котором расположен её основной *Web*-сайт.

Сущность проблемы заключается в том, что использование наименований сетевых сегментов с целью идентификации организаций весьма неудобны для пользователей. Это связано с тем, что наименования сетевых сегментов уникальны, с глобальной точки зрения, и поэтому не запоминаемы. В реальном мире для обозначения организаций подходят обычные имена, но они не приемлемы для автоматической интерактивной процедуры аутентификации. Следствием этого является то, что доверяющие стороны не знают какой ПП может быть запрошен ПЭУ при запросе интерактивного доступа к службам. Таким образом, это – случай строгой аутентификации с использованием криптографии, которая, с семантической точки зрения, не может быть осмысленна. Другими словами, доверяющие стороны не знают, какой вывод о защищённости следует сделать, и какое решение относительно доверия следует принять. Эта уязвимость представляет собой угрозу, которая может быть реализована с помощью, например, способа проведения атак типа «вскрытие данных пользователя». В [140] представлено описание этой проблемы и того, как злоумышленники могут воспользоваться такой уязвимостью.

4.12 Дальнейшее развитие ИОК

При развитии ИОК основное внимание, как правило, уделяется архитектуре ИОК и синтаксическим структурам сертификации, а также политике и правовым аспектам, в соответствие с которыми функционируют ИОК. В этих сферах обеспечения надёжного функционирования ИОК существует много нерешённых проблем, например, дополнительные издержки, связанные с аннулированием $СЕРТ_{ОК}$, сложность системы автоматизированного подтверждения ПП, а также низкая ответственность ЦС за (случайный или преднамеренный) выпуск ошибочных $СЕРТ_{ОК}$.

Области, которым в настоящее время уделяется недостаточное внимание, – это семантические и аналитические аспекты развития ИОК. К сожалению, наиболее частой причиной сбоя процедур аутентификации является именно то, что доверяющие стороны неправильно

интерпретируют или игнорируют синтаксис ПП, которые, с технической точки зрения, подтверждаются с использованием ИОК. В этой связи, необходимо обеспечить удобство использования и восприятия (анализа) ПП.

Другим важным аспектом совершенствования ИОК, который, как правило, игнорируется, – это способы получения корневых $СЕРТ_{ОК}$ и обеспечение гарантий при их получении. Очень часто политики сертификации не затрагивают эту проблему, а ЦС заинтересованы в гарантированном и эффективном распределении своих корневых $СЕРТ_{ОК}$. При этом очевидно, что возникает противоречие между указанной заинтересованностью ЦС и требованиями наличия защищённых вспомогательных каналов для распространения корневых $СЕРТ_{ОК}$.

Учитывая многие проблемы надёжного функционирования ИОК, которые потенциально могут привести к сбою процедуры аутентификации, в первую очередь, необходимо проанализировать условия, которые лежат в основе обеспечения соответствующего уровня надёжности процедуры аутентификации, реализуемой конкретной ИОК. Есть, например, предложения по созданию специализированных систем аутентификации ПЭУ, которые аналогичны национальным системам аутентификации пользователей [142]. Способ распространения корневых $СЕРТ_{ОК}$ также может рассматриваться как одно из таких условий надёжности и гарантированности.

Несмотря на кажущуюся простоту, ИОК намного сложнее, с точки зрения их проектирования, и стоят они дороже, чем предполагалось изначально. Таким образом, задача состоит в том, чтобы найти приемлемые решения для оставшихся вопросов проектирования, а также разработать эффективные методики, которые отражали бы жизнеспособные бизнес-модели ИОК.

Гарантии, предоставляемые ИОК, основаны на совокупности прямых доверительных взаимоотношений, которые были установлены между ЦС в рамках ИОК с использованием защищённых вспомогательных каналов связи, а также между внешними доверяющими сторонами и корневыми ЦС, входящими в ИОК. Несмотря на то, что формирование прямых доверительных взаимоотношений является медленным и весьма затратным процессом, ИОК можно использовать с целью обеспечения автоматизированного и эффективного крупномасштабного распределения открытых ключей пользователей, которые, в свою очередь, могут быть востребованы службами криптографической защиты информации.

Наличие надёжной основы доверия к ИОК имеет решающее значение при обеспечении защищённости ИТС и прикладных служб, которые она обслуживает. Потеря доверия может привести к возникновению крупномасштабным уязвимостей и многочисленным атакам нарушителей, поэтому правильная интерпретация надёжности, обеспечиваемой ИОК, имеет реша-

ющее значение. Многие доверяющие субъекты ошибочно полагают, что $СЕРТ_{ОК}$ обеспечивают гарантию благонадёжности пользователя или ПЭУ, а на самом деле они обеспечивают надёжность только ПП или конкретных атрибутов.

Гарантии, предоставляемые $СЕРТ_{ОК}$, должны определяться в политиках сертификации, но большинство доверяющих сторон никогда не читают такие политики, и даже если бы они их читали, то им было бы трудно их интерпретировать. Если речь идёт о доверяющих субъектах, то трудность понимания и интерпретации политики сертификации является проблемой функциональности системы обеспечения информационной безопасности. Существует большой потенциал для повышения защищённости ИТС, КЗСУ которых основаны на ИОК. Такой потенциал зависит, в том числе, от улучшения читаемости и понимаемости $СЕРТ_{ОК}$ и соответствующих политик сертификации.

Выводы по Главе 4

1. В первой части данной главы рассмотрены проблемы обеспечения параметрами подлинности. Показано, что одним из фундаментальных понятий, используемых в системах аутентификации на основе ИОК, является ПП. ПП – это уникальное свойство (признак) любого субъекта (объекта), которое подтверждает (свидетельствует о) его уникальность(и) или схожесть(и) с самим собой и делает его отличным от других субъектов (объектов) в определённой ИТС. Наличие возможности отображать и распознавать объекты в компьютерных сетях имеет основополагающее значение для систем электронного взаимодействия и сотрудничества, и является функциональным фундаментом практически всех систем обеспечения безопасности, например, системы авторизации и управления доступом, а также обеспечения репутации.

Далее определено, что любая современная система УД позволяет пользователям идентифицировать себя с помощью УИ) и аутентифицировать себя с помощью параметров для аутентификации, например, паролей. В такой модели, которая получила название изолированной СОПП, требования к доверию между пользователем и ПЭУ хорошо отображаются в форме конкретных предположений об обеспечении безопасности и защите неприкосновенности. Кроме того, проанализированы концепции «субъекты/объекты», «параметры подлинности» (включая цифровые ПП), «идентификаторы» и «атрибуты».

2. Во второй части данной главы рассмотрены системы обеспечения пользователей параметрами подлинности. В частности, были проанализированы изолированная, федеративная,

централизованная СОПП, а также система персональной аутентификации. Для каждой из указанных СОПП были описаны их архитектуры, проблемы доверия (клиента к ПЭУ и ПЭУ к клиенту) и определены восемь типов функционального доверия.

Кроме того, показано, что любая система аутентификации должна учитывать порядок получения, хранения и использования (обслуживания) идентификаторов и параметров для аутентификации самими пользователями. Если пользователям неудобно (затруднительно) обслуживать идентификаторы и параметры для аутентификации, то сама аутентификация будет не надёжной, так как пользователи не смогут надлежащим образом обслуживать (хранить) свои параметры для аутентификации. Очевидно, что рост числа предоставляемых электронных услуг, а, следовательно, и рост числа ПЭУ, приводит к увеличению числа идентификаторов и параметров для аутентификации, а это, в свою очередь, приводит к невозможности пользователей эффективно их обслуживать (хранить). Другими словами, ожидать от пользователей, что они будут обслуживать (хранить) постоянно растущее количество паролей и параметров для аутентификации с помощью запоминания или других простых способов, совершенно нереально.

Вместе с тем, понадобился новый способ, который предусматривает автоматизацию процедур обеспечения ПП на стороне пользователей. Самое простое решение, которое достаточно очевидно, – позволить пользователям хранить идентификаторы и параметры для аутентификации разных ПЭУ в одном защищённом от несанкционированного доступа ПАК, которым может быть персональное портативное устройство (например, смартфон). Такое решение резко снижает их проблемы по обслуживанию (хранению) идентификаторов и параметров для аутентификации, а также повышает надёжность обоюдной аутентификации между пользователями и ПЭУ. Такой ПАК назван ПУА. Системы аутентификации пользователя, основанные на ПУА, называются СОПП, ориентированной на пользователей. ПУА может быть интегрировано в любую ранее описанную современную модель обеспечения ПП.

Показано, что функциональность ПУА способна интегрировать его с другими устройствами, например, мобильные телефоны (смартфоны), которые в настоящее время получили массовое распространение. Использование смартфона позволило внедрить самые передовые технологии, например, регистрацию и аутентификацию на основе запросно-ответного способа информационного взаимодействия («клиент-сервер») по дополнительному каналу мобильной связи. Был рассмотрен пример использования двух каналов аутентификации, т.е. первый обеспечивает аутентификацию пользователя (программного модуля клиента), а второй используется для подтверждения подлинности пользователя. В основе аутентификации по второму каналу лежит «убеждённость сервера ПЭУ» в том, что пользователь является единственным владельцем смартфона, и только пользователь мог аутентифицироваться при доступе к функциям

смартфона (ПИН-код, биометрический параметр и т.д.). В данном случае, реализуется трёх-итерационная процедура однонаправленной аутентификации пользователя.

Однако, современные системы аутентификации при предоставлении электронных услуг не обеспечивают аутентификацию ПЭУ. Был рассмотрен пример использования специализированного КПО ПЭУ, загружаемого (копируемого) в смартфон пользователя. Однако, большое число ПЭУ, а значит и большое число указанных КПО, копируемых в смартфон, может привести к недостатку памяти, что является одной из самых распространённых проблем, которая характерна даже для смартфонов с большими объёмами хранилищ.

3. В третьей части данной главы рассмотрены системы обеспечения провайдеров электронных услуг параметрами подлинности. Показано, что в настоящее время существует проблема идентификации ПЭУ, которая характерна практически всем системам предоставления услуг с помощью всемирной ГИТС и обеспечения безопасности электронной коммерции. И что самое главное – эта проблема практически не находит своего отражения в современных научных исследованиях.

Отмечено, что ПЭУ, которые функционируют в глобальных ИТС, например, Интернет-сети, нуждаются в глобальных идентификаторах. К сожалению, не существует надёжных и реальных глобальных пространств имён для людей и организаций, и поэтому весьма сомнительна значимость аутентификации ПЭУ с учётом нынешней парадигмы обеспечения безопасности во всемирной ГИТС. Проблема модели обеспечения безопасности с использованием TLS-протокола заключается в том, что идентификатор ПЭУ, аутентифицированный *Web*-обозревателем клиента ГИТС, не обязательно является идентификатором ПЭУ, назначенным пользователем. В частности, в Интернет-сети существуют способы атак, основанные на использовании ограниченности когнитивных способностей человека. Одним из таких примеров является ошибочный (ложный) URI-идентификатор, который очень похож на другие URI-идентификаторы, и поэтому ложный URI-идентификатор может быть не замечен пользователем Интернет-сети.

Далее рассмотрена проблема способности клиента убедится в том, что ПЭУ, к которому он подключён, является именно тем субъектом, с которым он желает установить виртуальное соединение. Это определяет девятый тип функционального доверия клиента к ПЭУ: ПЭУ обладает предполагаемым ПП. В противном случае, пользователей можно обмануть и «выманить» у них параметры для аутентификации, например, это происходит при предоставлении интерактивных банковских услуг фальшивыми (мошенническими) *Web*-сайтами. Кроме того, ПЭУ, которые искажают свои ПП с целью привлечения клиентов, могут обмануть и «заставить» пользователей совершать с ними электронные (в том числе фиктивные) сделки.

4. В четвёртой части данной главы рассмотрены структуры (системы) доверия на основе инфраструктуры открытых ключей. Одна из основных целей ИОК – упростить распределение ключей путём снижения числа необходимым вспомогательных (дополнительных) защищённых каналов. Вместе с тем, доверие к открытым ключам пользователей формируется на основе криптографии и ограниченной совокупности прямых доверенных взаимосвязей/взаимоотношений. В таком случае, ИОК позволяет распространять доверие оттуда, где оно существует, туда, где оно необходимо.

Далее показано, что $СЕРТ_{ОК}$ отражает границу между ЦС и владельцем сертифицированного открытого ключа. Обычные границы доверия заключаются в том, что «владелец открытого ключа по праву владеет уникальным именем, указанным в сертификате». Такие $СЕРТ_{ОК}$ очень часто называются сертификатами ПП. Любой пользователь, который может доказать, что он обладает закрытым ключом, соответствующим открытому ключу, докажет, что он также обладает собственным уникальным именем, указанным в сертификате. Доказательство, как правило, основано на протоколе криптографической защиты. В общем, любую ИОК, основанную на $СЕРТ_{ОК}$, можно назвать сетью доверия. Процедура подтверждения подлинности, проводимая, как правило, доверяющей стороной, включает проверку корректности ЭП в сертификате. Данные, извлекаемые из $СЕРТ_{ОК}$ с подтверждённой подлинностью, например, наименование, открытый ключ и другие атрибуты считаются подлинными.

Если организация-владелец корневого ЦС аккредитована федеральными органами исполнительной власти или иными уполномоченными организациями, то решение доверять или нет корневому ЦС, в конечном счёте, становится политическим и философским вопросом. Для ИОК, которая используется только внутри организации, администрация компании представляет собой наивысший орган формирования корневого ЦС в качестве доверенного замыкающего ЦС. В социальных сетях между людьми решение доверять или нет открытому ключу или $СЕРТ_{ОК}$ может быть избирательным и основанным, как правило, на персональных взаимосвязях.

Далее анализируются модели архитектур ИОК, среди которых одиночная иерархическая, многоиерархическая ИОК, модель избираемого прямого доверия, модель со взаимной сертификацией корневых ЦС, модель со связующим ЦС, *PGP*-модель, модель на основе центра подтверждения подлинности и модель на основе защищённой DNS-системы. Для каждой из них указаны проблемы обеспечения доверия, их преимущества и недостатки. Сделан вывод о том, что в современных условиях модель с ЦПП является наиболее перспективной и востребованной, в частности, эта модель лежит в основе ИОК (системы доверия) ЕС.

В завершении данной главы рассмотрены основные направления развития и совершенствования ИОК.

Глава 5 МОДЕЛЬ СИСТЕМЫ УПРАВЛЕНИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТОЙ (СИСТЕМЫ ДОВЕРИЯ) НА ОСНОВЕ ИОК

В любой ИТС, в которой предусмотрено использование СКЗИ, функционирует КЗСУ, призванная обеспечить максимальный уровень защиты передаваемых в ИТС данных, следствием которого является высокий уровень доверия к ИТС и её компонентам. СОИБ (включая КЗСУ) ИТС формирует ИТИБ, которая обслуживает все компоненты ИТС, включая СКЗИ. Основной формой реализации ИТИБ любой ИТС, исходя из опыта экономически развитых стран, является ИОК, которая обладает уникальными свойствами и возможностями по обеспечению ИБ (см. Главу 3). Таким образом, в основе функционирования КЗСУ, обслуживающей ИТС и её компоненты, должна быть ИОК.

В данной главе представлен синтез и анализ модели КЗСУ на основе ИОК для ИТС с применением математического аппарата (методы и средства) СЛ. В частности, была использована *теория синтеза и анализа сетей субъективного доверия*. Рассмотрим основные положения этой теории.

5.1 Синтез сетей субъективного доверия в СЛ

Сеть субъективного доверия (ССД, *subjective trust network*) отображает доверенные взаимосвязи, начиная от доверяющих субъектов, через других субъектов, и заканчивая целевыми доверенными объектами (субъектами), в которой каждая доверенная взаимосвязь представляет собой субъективное мнение [19]. Сеть доверия, как правило, отображается с помощью графа. Простая ССД была рассмотрена в Главе 2 (§2.12.2), как доверие в ИТС, включая маршруты транзитивного доверия и простые сети слияния доверия.

В случае более сложных ССД, необходимо использовать алгоритмический метод моделирования и анализа. Операторы понижения (§2.12.4), слияния (§2.12.5) и переоценки (§2.12.6) доверия, используемые для описания доверенных взаимосвязей, могут отображаться как *последовательно-параллельные ориентированные графы* (или орграфы [169], ППОГ, *directed series-parallel graph*).

5.1.1 Графы сетей доверия

5.1.1.1 Последовательно-параллельные орграфы

Последовательно-параллельные графы (ППГ) отображают конкретный тип графов, который включает пару отдельных вершин, называемых *источник* (*исток*) и *сток*. Дадим определение ППГ [170].

Определение 5.1 (ППГ). Граф называется ППГ, если его можно преобразовать в одиночное ребро, соединяющее узел-исток s и узел-сток t, с помощью следующих процедур:

i. Замена пары рёбер, *инцидентных* двухвалентной вершине $\{deg(x) = 2\}$, которая отлична от истока или стока, на одно ребро;

ii. Замена пары параллельных рёбер на одно ребро, которое соединяет, их общие конечные вершины.

На рисунке 5.1 показан пример возможного поэтапного преобразования ППГ (расположен сверху) на основе процедур, описанных в **Опред.5.1**.

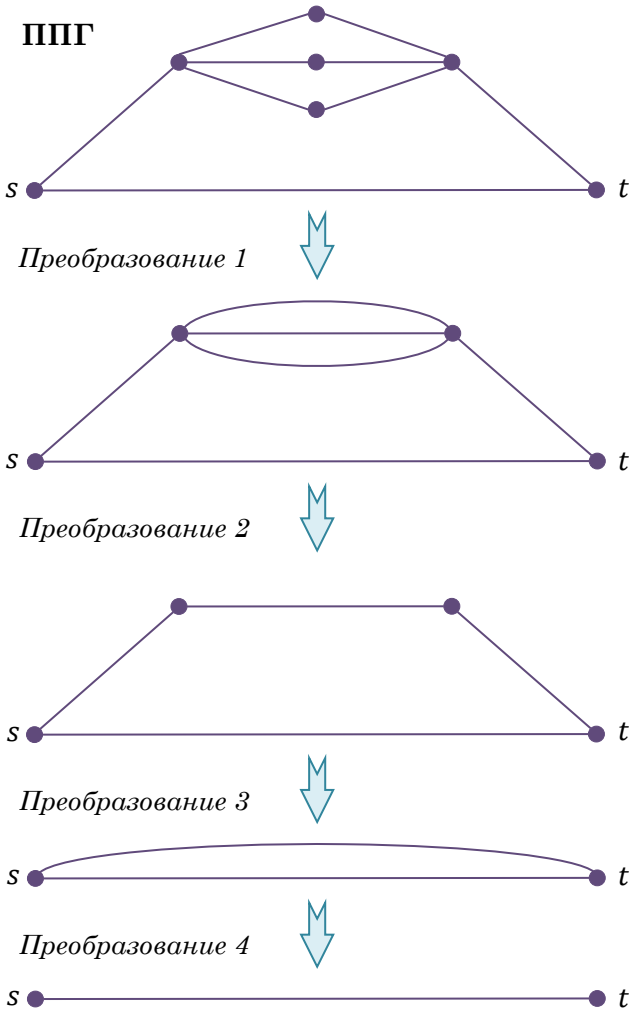

Рисунок 5.1 – Процедура преобразования ППГ в одиночное ребро

Преобразование 1 – это результат четырёхкратного выполнения процедуры i. *Преобразование 2* – это результат двукратного выполнения процедуры ii. *Преобразование 3* – это результат двукратного выполнения процедуры i. *Преобразование 4*, в результате которого получается одиночное ребро, – это результат однократного выполнения процедуры ii. Факт того, что граф таким способом преобразуется в одно ребро, доказывает, что это ППГ.

Сети доверия отображаются как орграфы. В дальнейшем будет полагать, что ППГ, отображающий сеть доверия, является ориентированным от истока (источника) к стоку, и в таком случае он будет именоваться ППОГ [171].

Определение 5.2 (ППОГ). Граф является ППОГ тогда и только тогда, когда он является последовательно-параллельным графом согласно **Опред.5.1**, и состоит только из ориентированных (направленных) рёбер, которые образуют маршруты (пути) без петель от истока (источника) к стоку. □

С точки зрения сетей доверия, узел-исток/источник ППОГ – мыслящий субъект, т.е. доверяющая сторона, которая отображается символом $\mathcal{A}$. В общем, узел-сток в ППОГ – целевая переменная (объект), которая, как правило, отображается с помощью символа X, а если речь идёт о доверенном мыслящем субъекте, то используется символ $\mathcal{E}$.

5.1.2 Выходное-входное множество

ППОГ может состоять из нескольких подсетей, которые сами являются направленными последовательно-параллельными ориентированными подграфами. *Подсеть с параллельными маршрутами* представляет собой подсеть, которая состоит из параллельных маршрутов в последовательно-параллельном ориентированном подграфе.

Вершина (узел) может быть частью одного или нескольких рёбер. В общем, *валентность вершины* (узла) отражает число рёбер, частью которых является вершина (узел). Так как ППОГ – это орграф, то можно различать *входную валентность* и *выходную валентность* вершины (узла). Входная валентность вершины (узла), $\deg_{in}(x)$ – число рёбер, входящих в эту вершину (узел).

Аналогично, выходная валентность вершины (узла), $\deg_{out}(x)$ – число рёбер, выходящих из этой вершины (узла).

Предположим, например, следующую сеть рекомендуемого доверия:

$$\mathcal{A} \dashrightarrow \mathcal{B} \dashrightarrow \mathcal{C} \quad . \tag{5.1}$$

Узел $\mathcal{B}$ – двухвалентная вершина, $\deg(\mathcal{B}) = 2$, так как она инцидентна двум рёбрам $[\mathcal{A};\mathcal{B}]$ и $[\mathcal{B};\mathcal{C}]$. Вместе с этим, узел $\mathcal{B}$ имеет входную одновалентность, $\deg_{in}(\mathcal{B}) = 1$, так как у него только одно входной ребро $[\mathcal{A};\mathcal{B}]$. Кроме того, $\mathcal{B}$ имеет выходную одновалентность, $\deg_{out}(\mathcal{B}) = 1$, так как у него только одно выходное ребро $[\mathcal{B};\mathcal{C}]$. Узел $\mathcal{A}$ – одновалентная вершина, $\deg(\mathcal{A}) = 1$, $\deg_{in}(\mathcal{A}) = 0$ и $\deg_{out}(\mathcal{A}) = 1$. Очевидно, что для любого узла (вершины) $\mathcal{V}$, его валентность отображается как, $\deg(\mathcal{V}) = \deg_{in}(\mathcal{V}) + \deg_{out}(\mathcal{V})$.

Говорят, что упорядоченная пара узлов $(\mathcal{V}_s, \mathcal{V}_t)$ в ППОГ соединена, если второй узел $\mathcal{V}_t$ может быть достигнут после «выхода» из первого узла $\mathcal{V}_s$. Например, легко заметить, что $(\mathcal{A}; \mathcal{C})$ в (5.1) – пара соединённых узлов.

Рассмотрим узел в ППОГ. Выходное множество узла представляет собой множество рёбер, которые могут быть пройдены после выхода из этого узла. Аналогично, входное множество узла представляет собой множество рёбер, которые могут быть пройдены до того, как будет достигнут этот узел.

Определение 5.3 (выходное-входное множество, ВВМ). Предположим, что в ППОГ существует упорядоченная пара узлов $(\mathcal{V}_s, \mathcal{V}_t)$. Тогда выходное-входное множество упорядоченной пары – пересечение исходящего множества первого узла $\mathcal{V}_s$ и входящего множества второго узла $\mathcal{V}_t$.

Теперь можно рассмотреть некоторые простые свойства ВВМ.

Теорема 5.1 [19]. Два узла $(\mathcal{V}_s, \mathcal{V}_t)$ в ППОГ являются соединёнными тогда и только тогда, когда ВВМ этой пары узлов – не пустое.

Доказательство. Если ВВМ $\neq \emptyset$, то ВВМ, по крайней мере, состоит из одного ребра, которое может быть пройдено после выхода из первого узла $\mathcal{V}_s$ и до достижения второго узла $\mathcal{V}_t$. А это означает, что можно достичь второй узел $\mathcal{V}_t$ путём «выхода» из первого узла $\mathcal{V}_s$, т.е. они должны быть соединёнными. Если ВВМ $= \emptyset$, то ВВМ не содержит маршрутов, соединяющих узлы, а это означает, что они не соединены. □

5.1.2.1 Подсети с параллельными маршрутами

ППОГ, как правило, может включать несколько подсетей, которые сами собой представляют ППОГ. А последние могут включать параллельные маршруты. В контексте данной работы наибольший интерес представляет идентификация подсетей внутри ППОГ, содержащие параллельные маршруты. *Подсеть с параллельными маршрутами* внутри ППОГ – множество маршрутов между парой соединённых узлов.

Определение 5.4 (подсеть с параллельными маршрутами). Выберем в ППОГ упорядоченную пару соединённых узлов $(\mathcal{V}_s, \mathcal{V}_t)$. Подсеть, состоящая из ВВМ пар, является подсетью с параллельными маршрутами тогда и только тогда, когда, и выходная валентность первого узла $\mathcal{V}_s$ в ВВМ удовлетворяет условию $\deg_{out}(\mathcal{V}_s) \geq 2$, а входная валентность второго узла $\mathcal{V}_t$ в ВВМ удовлетворяет условию $\deg_{in}(\mathcal{V}_t) \geq 2$.

Узел $\mathcal{V}_s$ называется истоком (источником) подсети с параллельными маршрутами, а узел $\mathcal{V}_t$ называется стоком подсети с параллельными маршрутами. □

Рассмотрим в качестве примера ВВМ пары узлов $(\mathcal{C}, \mathcal{J})$, как показано на рисунке 5.2. В рамках этого ВВМ имеем $\deg_{out}(\mathcal{C}) = 2$ и $\deg_{in}(\mathcal{J}) = 3$, что удовлетворяет требованиям **Опред.5.4**, следовательно, ВВМ – подсеть с параллельными маршрутами.

Кроме того, можно определить, что соответствующая ВВМ состоит из пар узлов $(\mathcal{E}, \mathcal{J})$, $(\mathcal{C}, \mathcal{F})$, $(\mathcal{F}, \mathcal{X})$ и $(\mathcal{C}, \mathcal{X})$, которые также являются подсетями с параллельными маршрутами. А это означает, что ППОГ на рисунке 5.2, в целом, включает пять подсетей с параллельными маршрутами.

Тем не менее, подсеть между парами соединённых узлов $(\mathcal{E}, \mathcal{X})$ не является подсетью с параллельными маршрутами внутри такого ВВМ, так как $\deg_{in}(\mathcal{X}) = 1$, что не удовлетворяет требованиям **Опред.5.4**.

5.1.2.2 Степень вложенности

Понятие *степень вложенности* (*nesting level*) играет важную роль при анализе сетей доверия, которые отображаются как ППОГ. В целом, степень вложенности некоторого ребра отражает число подсетей с параллельными маршрутами в ППОГ, к которым данное ребро относится. Каждое ребро обладает конкретной степенью вложенности, которая равна или больше 0. Например, сеть доверия, состоящая из одиночного маршрута доверия, имеет рёбра доверия со степень вложенности 0, так как рёбра не являются частью какой-либо подсетью с параллельными маршрутами. Далее приводится определение степени вложенности в ППОГ.

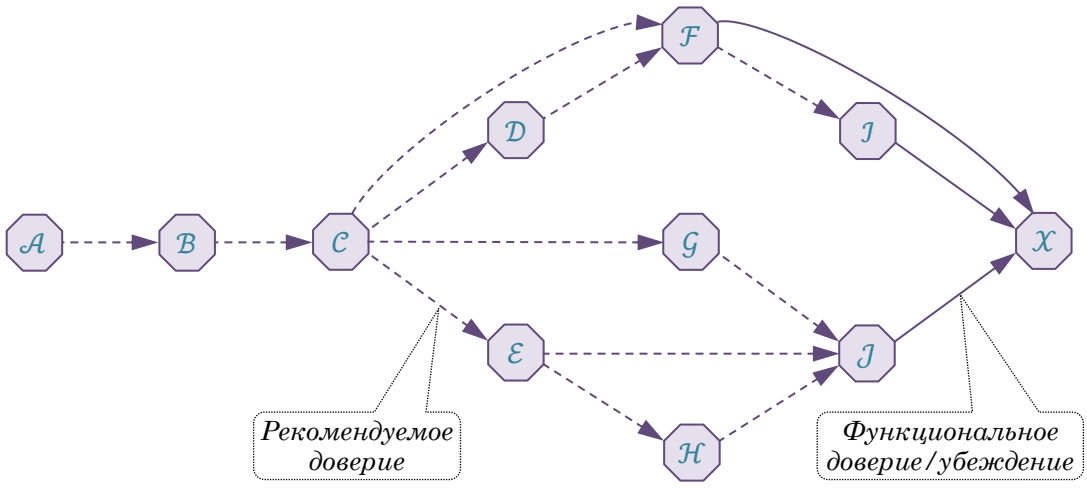

Рисунок 5.2 – ППОГ, состоящий из пяти подсетей с параллельными маршрутами

Определение 5.5 (степень вложенности). Предположим, что ППОГ состоит из нескольких узлов, соединённых между собой направленными (ориентированными) рёбрами.

Степень вложенности ребра в ППОГ равна числу подсетей с параллельными маршрутами, для которых данное ребро является их составной частью.

Пусть, например, $[\mathcal{V}_m; \mathcal{V}_n]$ будет ребром в ППОГ. Степень вложенности ребра $[\mathcal{V}_m; \mathcal{V}_n]$ формально обозначается как $\mathrm{NL}([\mathcal{V}_m; \mathcal{V}_n])$. Степени вложенности могут быть равны 0 или больше. □

На рисунке 5.3 представлены степени вложенности рёбер (ромбы с зелёными цифрами на стрелках).

Можно заметить, что ребро $[\mathcal{A}; \mathcal{B}]$ не является частью какой-либо подсети с параллельными маршрутами, т.е. его степень вложенности $\mathrm{NL}([\mathcal{A}; \mathcal{B}]) = 0$. Кроме того, можно заметить, что ребро $[\mathcal{H}; \mathcal{J}]$ является частью трёх подсетей с параллельными маршрутами, принадлежащих парам узлов $(\mathcal{E}, \mathcal{J})$, $(\mathcal{C}, \mathcal{J})$ и $(\mathcal{C}, \mathcal{X})$, т.е. его степень вложенности $\mathrm{NL}([\mathcal{H}; \mathcal{J}]) = 3$.

Степень вложенности определяет порядок вычисления доверия в сети доверия, отображаемой в форме ППОГ.

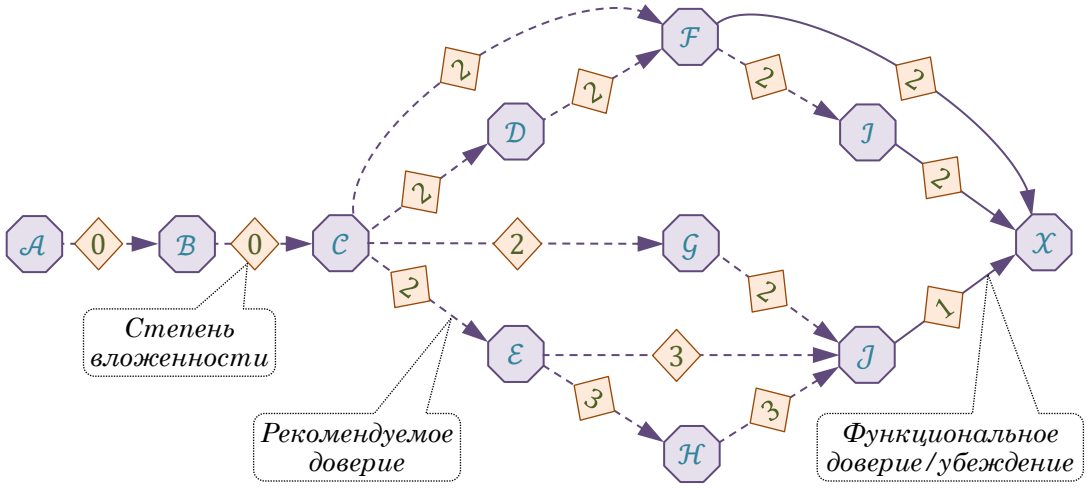

Рисунок 5.3 – Степени вложенности рёбер в ППОГ

5.1.3 Анализ сетей доверия, отображаемых в форме ППОГ

Предположим, что подлежащая анализу сеть доверия отображается в форме ППОГ. В соответствие с **Опред.5.2**, можно проверить, что сеть доверия, представленная на рисунке 5.4, представляет собой ППОГ.

Кроме того, можно заметить, что ППОГ на рисунке 5.4 включает три подсети с параллельными маршрутами, отображаемые с помощью пар исток-сток $(\mathcal{D}, \mathcal{J})$, $(\mathcal{A}, \mathcal{J})$ и $(\mathcal{A}, \mathcal{X})$. Компактное формальное выражение сети доверия (рисунок 5.4) имеет следующий вид:

$$[\mathcal{A}, \mathcal{X}] = [\mathcal{A}; \mathcal{B}; \mathcal{E}; \mathcal{I}, \mathcal{X}] \diamond ([\mathcal{A}; \mathcal{C}; \mathcal{F}; \mathcal{J}] \diamond ([\mathcal{A}; \mathcal{D}] : ([\mathcal{D}; \mathcal{G}; \mathcal{J}] \diamond [\mathcal{D}; \mathcal{H}; \mathcal{J}]))) : [\mathcal{J}, \mathcal{X}]. \quad (5.2)$$

Далее рассматривается простой алгоритм анализа и определения доверия/убеждённости на основе сети доверия, отображаемой в форме ППОГ, которая аналогична сети, представленной на рисунке 5.4.

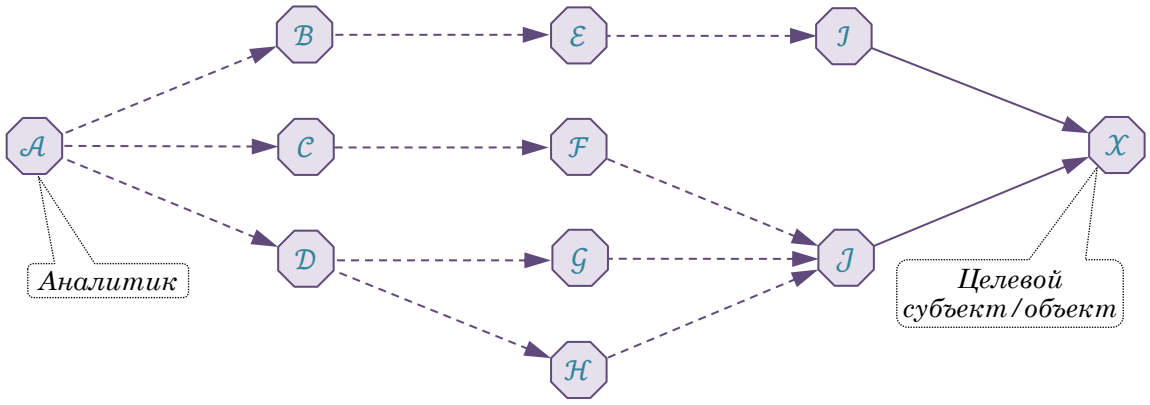

Рисунок 5.4 – Сеть доверия в форме ППОГ

5.1.3.1 Алгоритм анализа ППОГ

Процедура вычисления итогового доверия в сети доверия, представленной в формате ППОГ, представлена на рисунке 5.5 в виде блок-схемы алгоритма и рассматривается ниже. Процедура может использоваться, например, при вычислении мнения о доверии ω_X^A, представленного на рисунке 5.4. Процедура полностью соответствует процедурам преобразования графа, указанным в **Опред.5.1**. В соответствие с правилами вычисления, определёнными в данной работе, субъекты и целевой субъект (объект) будут называться *узлами*. Итерации блок-схемы алгоритма (рисунок 5.5) – следующие:

(а) Подготовка к анализу сети доверия. Она включает отображение сети доверия в виде множества ориентированных (направленных) рёбер с парами узлов. Проверка того, что сеть доверия действительно является ППОГ;

(б) Определение каждой подсети с параллельными маршрутами со своими парами истока (источника) и целевых узлов $(\mathcal{V}_s, \mathcal{V}_t)$. Определение степени вложенности каждого ребра, как функции числа подсетей с параллельными маршрутами, для которых данное ребро является их частью;

(в) Выбор подсети с параллельными маршрутами, в которой все рёбра имеют наивысшую степень вложенности, затем переход к итерации (г). Если же подсетей с параллельными маршрутами не осталось, то переход к итерации (ж);

(г) Для выбранной подсети с параллельными маршрутами, определяем двухрёберное или многорёберное понижение доверия для каждого маршрута между $\mathcal{V}_s$ и $\mathcal{V}_t$, где узел $\mathcal{V}_t$ рассматривается как целевой узел анализа. В результате, каждый маршрут преобразуется в одиночное ребро;

(д) Для выбранной подсети с параллельными маршрутами, вычисляет слияние доверия для всех рёбер. В результате, подсеть с параллельными маршрутами преобразуется в одиночное ребро;

(е) Теперь определяем степень вложенности ребра, которое заменило выбранную подсеть с параллельными маршрутами;

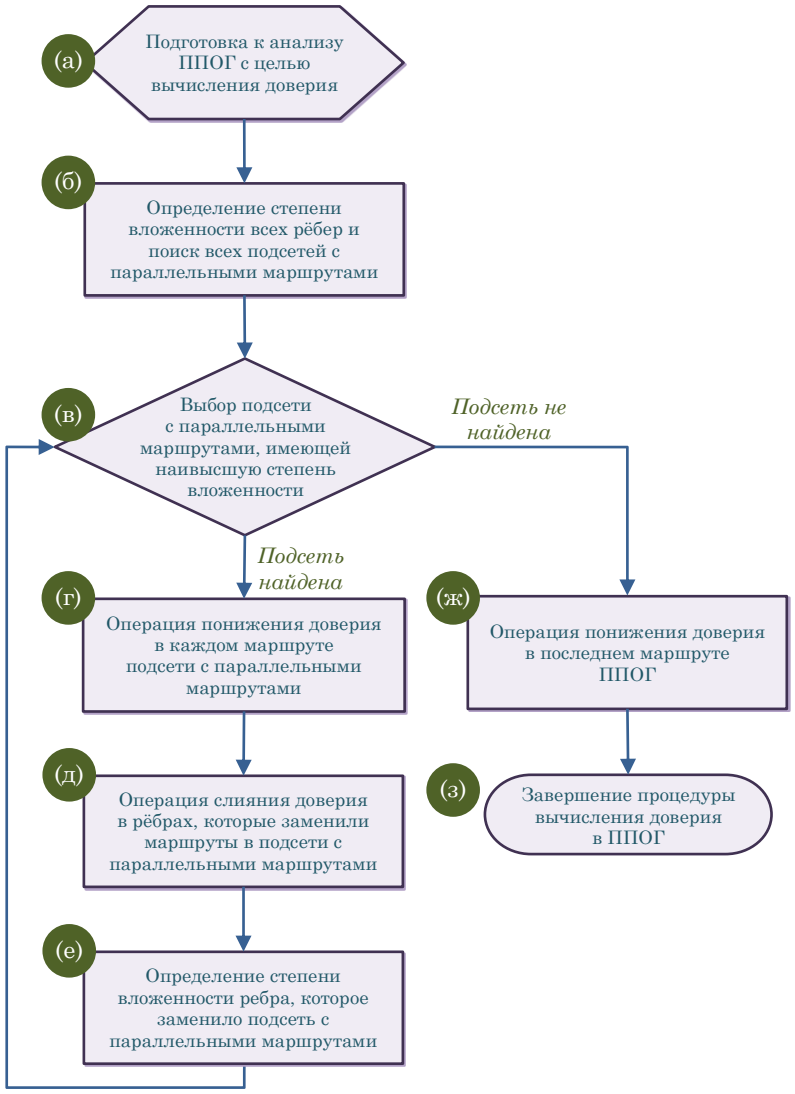

Рисунок 5.5 – Блок-схема алгоритма анализа сети доверия форме ППОГ с целью вычисления доверия

(ж) Если подсети с параллельными маршрутами не существует, то сеть доверия по-прежнему может состоять из последовательности рёбер. В таком случае, определяем двухрёберное или многорёберное понижение доверия. В итоге сеть состоит из одиночного ребра, т.е. больше ничего делать не нужно;

(з) Сеть доверия теперь преобразована в одиночное ребро между аналитиком и конечным целевым субъектом (объектом), т.е. вычисление завершено.

Грамматико-синтаксический анализатор (ГСА), реализующий вычислительный алгоритм, представленный на рисунке 5.5, способен анализировать граф, представленный, например, на рисунке 5.4, и определять мнение $\omega_{\mathcal{X}}^{\mathcal{A}}$.

5.1.3.2 Требования надёжности при получении рекомендуемых мнений

Аналитик должен получить мнение источника в первоначальной форме от источника, а не в форме не направленного вычисленного мнения. Причина этого рассматривается ниже. На рисунке 5.6 показан пример того, как не следует получать мнения источников.

На рисунке 5.6 стрелки доверия и рекомендаций проиндексированы в соответствии с порядком их формирования, в то время как начальные доверенные отношения индексов не имеют.

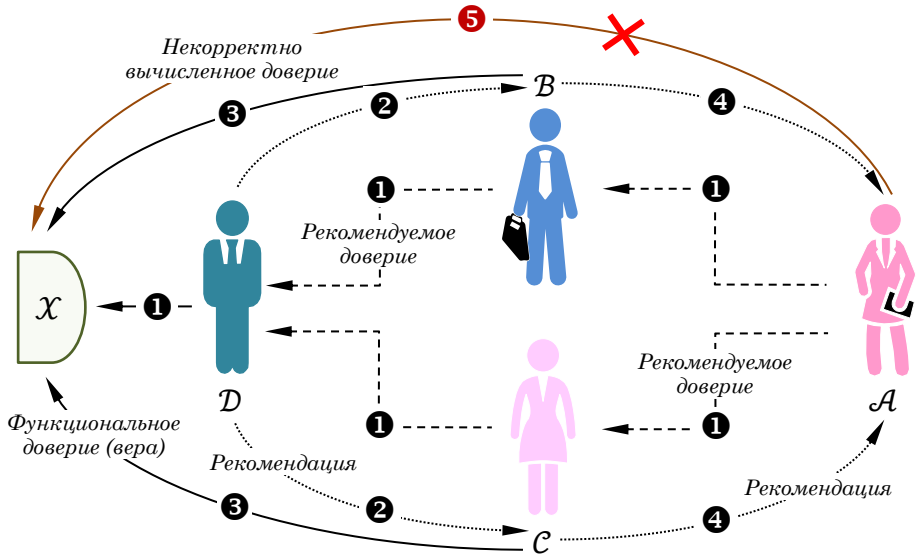

Рисунок 5.6 – Некорректный способ получения рекомендуемых мнений

Как показано н рисунке 5.6, субъект $\mathcal{D}$ даёт собственную рекомендацию относительно субъекта (объекта) $\mathcal{X}$ субъектам $\mathcal{B}$ и $\mathcal{C}$ (индекс ❷), т.е. субъекты $\mathcal{B}$ и $\mathcal{C}$ способны сформировать свои собственные мнения о субъекте (объекте) $\mathcal{X}$ (индекс ❸). Далее, субъекты $\mathcal{B}$ и $\mathcal{C}$ направляют свои собственные сформированные мнения о субъекте (объекте) $\mathcal{X}$ субъекту $\mathcal{A}$ (индекс

❹), т.е. теперь субъект $\mathcal{A}$ может сформировать своё собственное мнение о субъекте (объекте) $\mathcal{X}$ (индекс ❺).

В результате, субъект $\mathcal{A}$ воспринимает топологию сети доверия как $([\mathcal{A};\mathcal{B},\mathcal{X}]\diamond[\mathcal{A};\mathcal{C},\mathcal{X}])$. Следует заметить, что в данном случае используется компактная форма записи (2.12) в §2.12.3.3.

Проблема примера, представленного на рисунке 5.6, состоит в том, что субъект $\mathcal{A}$ игнорирует наличие субъекта $\mathcal{D}$, т.е. субъект $\mathcal{A}$ не видит скрытую топологию сети доверия, которая отличается от воспринимаемой субъектом $\mathcal{A}$ топологии, и которая также отличается от реальной топологии. Все три топологии сети доверия представлены в таблице 5.1.

Причина такого несоответствия состоит в том, что доверенная взаимосвязь субъекта $\mathcal{B}$ $[\mathcal{B},\mathcal{X}]$ формируется из $[\mathcal{B};\mathcal{D},\mathcal{X}]$, а доверенная взаимосвязь субъекта $\mathcal{C}$ $[\mathcal{C},\mathcal{X}]$ формируется из $[\mathcal{C};\mathcal{D},\mathcal{X}]$. Таким образом, когда субъекта $\mathcal{B}$ предоставляет рекомендуемое мнение $\omega_{\mathcal{X}}^{\mathcal{B}}$, он неявно даёт рекомендацию $\omega_{\mathcal{X}}^{[\mathcal{B};\mathcal{D}]}$, а когда субъект $\mathcal{C}$ предоставляет рекомендуемое мнение $\omega_{\mathcal{X}}^{\mathcal{C}}$, он неявно даёт рекомендацию $\omega_{\mathcal{X}}^{[\mathcal{C};\mathcal{D}]}$, но субъект $\mathcal{A}$ игнорирует влияние субъекта $\mathcal{D}$ на полученные рекомендуемые мнения [22]. Можно заметить, что ни воспринимаемая, ни скрытая топологии не совпадают реальной топологии сети доверия, т.е. очевидно, что такой способ получения рекомендуемых мнений может привести к некорректным результатам.

Таблица 5.1 – Несоответствие топологий сети доверия

Воспринимаемая топология	**Скрытая топология**	**Реальная топология**
$([\mathcal{A};\mathcal{B},\mathcal{X}]\diamond[\mathcal{A};\mathcal{C},\mathcal{X}])$	$([\mathcal{A};\mathcal{B};\mathcal{D},\mathcal{X}]\diamond[\mathcal{A};\mathcal{C};\mathcal{D},\mathcal{X}])$	$([\mathcal{A};\mathcal{B};\mathcal{D}]\diamond[\mathcal{A};\mathcal{C};\mathcal{D}]):[\mathcal{D},\mathcal{X}]$

Надёжный способ получения рекомендуемых мнений состоит в том, что субъект $\mathcal{A}$ получает от субъектов $\mathcal{B}$ и $\mathcal{C}$ рекомендуемые мнения, которые они получили от субъекта $\mathcal{D}$ без изменений, а также их собственные мнения о доверии к субъекту $\mathcal{D}$. Это правило, безусловно, необходимо соблюдать, но оно также требует, чтобы субъект $\mathcal{A}$ был уверен в том, что субъекты $\mathcal{B}$ и $\mathcal{C}$ не изменили рекомендации субъекта $\mathcal{D}$, т.е. именно эту часть рекомендуемого доверия субъекта $\mathcal{A}$ к субъектам $\mathcal{B}$ и $\mathcal{C}$.

Таким образом, необходимо, чтобы субъект $\mathcal{A}$ получил все рекомендуемые мнения в неизменном виде, а также в том виде, в каком они отражены в первоначальных источниках. На рисунке 5.7 представлен пример корректного получения рекомендуемых мнений.

Как показано на рисунке 5.7, воспринимаемая топология сети доверия совпадает с реальной топологией, которую можно отобразить следующим образом:

$$[\mathcal{A},\mathcal{X}] = ([\mathcal{A};\mathcal{B};\mathcal{D}]\diamond[\mathcal{A};\mathcal{C};\mathcal{D}]):[\mathcal{D},\mathcal{X}]\,. \qquad (5.3)$$

Вывод, который следует из примеров, представленных на рисунках 5.6 и 5.7, состоит в том, что существует принципиальное различие между получением мнения об источнике, основанного на непосредственном наблюдении источника или получении доказательства от самого источника, и получением мнения об источнике, основанного на косвенно полученных доказательствах от источника, например, рекомендуемое доверие или мнения об источнике, которые были получены источником из других источников.

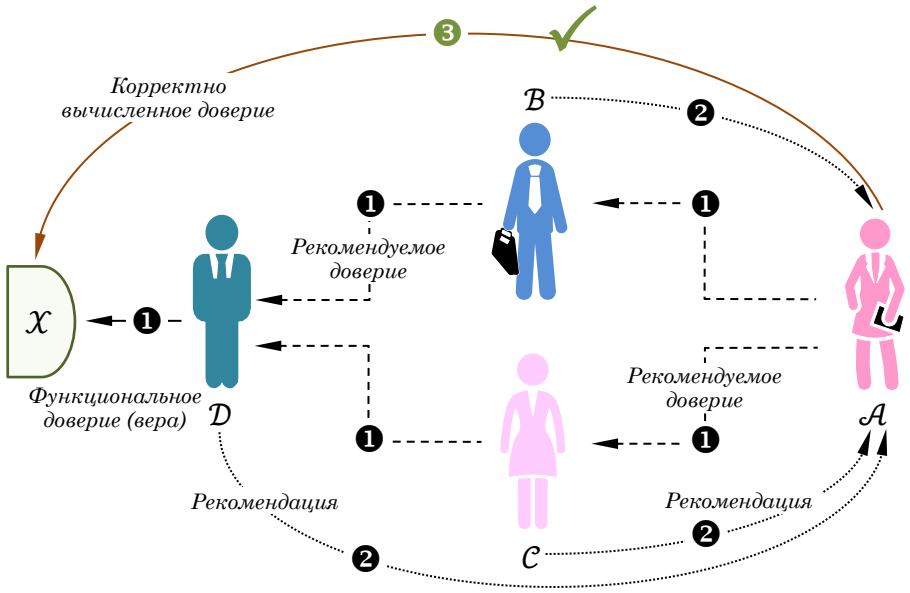

Рисунок 5.7 – Корректный способ получения рекомендуемых мнений

Сказанное выше означает, что аналитики должны осознавать разницу между получением прямых и косвенных мнений об источниках. Рисунок 5.6 показывает, как могут возникнуть проблемы, когда полученные косвенные мнения об убеждённости будут ошибочно интерпретироваться как прямые мнения об убеждённости. На этот счёт существует *золотое правило* – признавать только те источники, которые могут предоставить прямые мнения о доверии/убеждённости [22]. Однако, не всегда возможно придерживаться золотому правилу, тем не менее весьма полезно просто знать о потенциальных несоответствиях при оценке результатов анализа или при рассмотрении стратегий устранения таких несоответствий.

Если субъекты $\mathcal{B}$ и $\mathcal{C}$ были ненадёжными, то они могут попытаться изменить мнение об источнике, которое предоставляется субъектом $\mathcal{D}$. Вместе с тем, злоумышленник может перехватить и изменить мнения об источнике, предоставленные источниками (субъектами) $\mathcal{B}$, $\mathcal{C}$ или $\mathcal{D}$, ещё до того, как они будут получены субъектом $\mathcal{A}$, и поэтому субъект $\mathcal{A}$ может потребовать доказательства подлинности и целостности полученных рекомендуемых и мнений о доверии. Для решения данной проблемы используются криптографические способы и средства защиты информации.

5.1.4 Анализ сложных сетей доверия, не отображаемых в форме ППОГ

Аналитик может столкнуться с более сложной сетью доверия, которая не является ППОГ. Желательно не накладывать никаких ограничений на возможную топологию сети доверия, которая должна быть проанализирована, за исключением того, что она не должна быть циклической. Это означает, что множество возможных маршрутов доверия от аналитика (субъект $\mathcal{A}$) до целевого субъекта (объекта) $\mathcal{X}$ может включать маршруты, которые не совместимы с ППОГ. В такой ситуации возникает естественный вопрос о том, как анализировать такую сеть доверия.

Сложная сеть доверия, которая не является ППОГ, также не является ППГ, в соответствие с **Опред.5.1**. Если речь идёт о сложной сети, то во многих случаях бывает весьма непросто распознать, какие компоненты рекомендуемого доверия – последовательные, а какие – параллельные. На рисунке 5.8 представлен пример сложной сети доверия. Сеть доверия состоит только из рёбер от субъекта $\mathcal{A}$ до субъекта $\mathcal{E}$ и от субъекта $\mathcal{A}$ до субъекта $\mathcal{F}$. Таким образом, сеть доверия состоит только из рёбер рекомендуемого доверия.

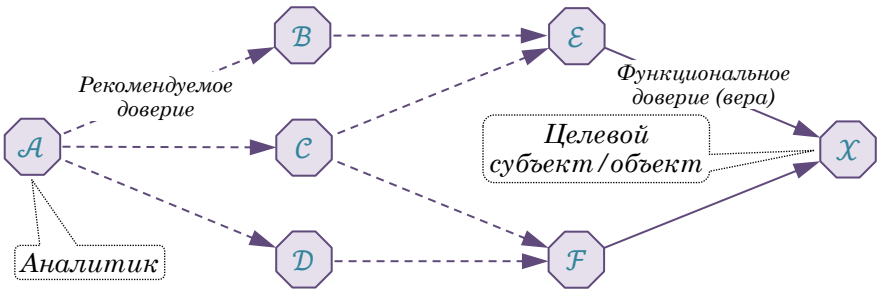

Рисунок 5.8 – Сеть доверия, не отображаемая в форму ППОГ

Последние рёбра от субъектов $\mathcal{E}$ и $\mathcal{F}$ до целевого субъекта (объекта) $\mathcal{X}$ отображают функциональные доверенные взаимосвязи, которые могут также рассматриваться как взаимосвязи с функциональным доверием, в соответствие с рисунком 5.2. Тем не менее, для представленного ниже анализа сети доверия важна только сеть рекомендуемого доверия от субъекта $\mathcal{A}$ до субъектов $\mathcal{E}$ и $\mathcal{F}$.

Анализ рисунка 5.8 показывает, что представленная на нём сеть доверия не может быть разбита на группы последовательно-параллельных маршрутов, что усложняет проблему вычисления итогового доверия на основе сети доверия. В случае использования ППОГ, которую можно разбить на последовательно-параллельные компоненты, можно достаточно просто определить математическую или аналитическую формулу, которая позволяет вычислить ито-

гового доверия на основе сети доверия. Однако, в случае сложной сети доверия, не отображаемой в форму ППОГ, вычисление итогового доверия требует применения более сложных методов.

ССД могут быть представлены в цифровом виде и сохранены в виде списка ориентированных рёбер доверия с дополнительными атрибутами, например, область анализа доверия σ, тип доверия (рекомендуемое или функциональное) и мнение о доверии. На основе перечня рёбер автоматизированный ГСА, при необходимости, может сформировать приемлемые ППОГ между двумя узлами. Например, в таблице 5.2 представлены ребра доверия сети доверия, не отображаемой в форму ППОГ, которая представлена на рисунке 5.8.

Для анализа сложных (т.е. не отображаемых в форму ППОГ) сетей субъективного доверия можно использовать несколько способов. Эта задача может показаться похожей на случай анализа надёжности сложных систем [19]. Однако, задача анализа сложных сетей субъективного доверия отличается от анализа надёжности сложных систем. Основные различия следующие. Во-первых, сети доверия допускают возможный обман субъектов, чего нет в сетях, основанных на надёжности систем, и во-вторых, сети доверия реализуют функцию слияния (§2.12.5), которая не используется при анализе надёжности систем. Следовательно, принципы анализа системной надёжности сложных сетей не приемлемы для сложных сетей субъективного доверия. Таким образом, для анализа сложных сетей субъективного доверия необходим иной способ.

Таблица 5.2 – Рёбра доверия сложной сети доверия, представленной на рисунке 5.8

Источник $\mathcal{V}_s$	**Целевой субъект** $\mathcal{V}_t$	**Область анализа**	**Тип доверия**	**Мнение**
$\mathcal{A}$	$\mathcal{B}$	σ	Рекомендуемое	$\omega_{\mathcal{B}}^{\mathcal{A}}$
$\mathcal{A}$	$\mathcal{C}$	σ	Рекомендуемое	$\omega_{\mathcal{C}}^{\mathcal{A}}$
$\mathcal{A}$	$\mathcal{D}$	σ	Рекомендуемое	$\omega_{\mathcal{D}}^{\mathcal{A}}$
$\mathcal{B}$	$\mathcal{E}$	σ	Рекомендуемое	$\omega_{\mathcal{E}}^{\mathcal{B}}$
$\mathcal{C}$	$\mathcal{E}$	σ	Рекомендуемое	$\omega_{\mathcal{E}}^{\mathcal{C}}$
$\mathcal{C}$	$\mathcal{F}$	σ	Рекомендуемое	$\omega_{\mathcal{F}}^{\mathcal{C}}$
$\mathcal{D}$	$\mathcal{F}$	σ	Рекомендуемое	$\omega_{\mathcal{F}}^{\mathcal{D}}$
$\mathcal{E}$	$\mathcal{X}$	σ	Функциональное	$\omega_{\mathcal{X}}^{\mathcal{E}}$
$\mathcal{F}$	$\mathcal{X}$	σ	Функциональное	$\omega_{\mathcal{X}}^{\mathcal{F}}$

Процедура упрощения сложной сети субъективного доверия удаляет маршруты, которые препятствуют последовательному вычислению доверия, и формирует сеть доверия, отображаемую в форму ППОГ, которую, в свою очередь, можно легко проанализировать.

Оптимальная сформированная сеть доверия в виде ППОГ позволяет вычислить мнение с максимальной достоверностью. Цель состоит в том, чтобы максимизировать достоверность вычисленного мнения, а не вычислить мнение, например, о некотором значении переменной X с наибольшей прогнозируемой вероятностью. Существует компромисс между временем, которое требуется для поиска оптимального ППОГ, и тем, насколько близко к оптимальному ППОГ может быть упрощённый граф. Ниже представлены метод комплексного поиска, который гарантированно приводит к оптимальному ППОГ, и метод эвристического поиска, который приводит к ППОГ, который будет близким к оптимальному ППОГ или равным ему.

Комплексный поиск сети доверия на основе оптимального ППОГ. Комплексный поиск сети доверия на основе оптимального ППОГ включает определение всех возможных ППОГ и вычисление на их основе целевых мнений, и, в заключении, выбор ППОГ и соответствующего стандартного выражения, которое позволяет вычислить численное значение доверия с наивысшим уровнем достоверности (надёжности), т.е. с минимальной недостоверностью. Вычислительная сложность этого метода составляет $\mathrm{Comp} = l \cdot m(2^n - 1)$, где n – число возможных маршрутов, m – среднее число маршрутов в ППОГ, а l – среднее число рёбер в маршрутах.

Эвристический поиск сети доверия, близкой к оптимальному ППОГ. Эвристический поиск сети доверия, близкой к оптимальному ППОГ включает синтез графа путём пошагового включения новых маршрутов в порядке убывания достоверности. Каждый новый маршрут, который приводит к формированию не ППОГ, исключается. Этот метод требует вычисления значения доверия только для одного ППОГ и одного стандартного выражения, а его вычислительная сложность составляет $\mathrm{Comp} = l \cdot m$, где m – среднее число маршрутов в ППОГ, а l – среднее число рёбер в маршрутах.

Эвристический метод формирует ППОГ, в котором уровень достоверности вычисленных мнений равен или близок к аналогичному уровню, формируемом в оптимальном ППОГ. Причина того, что данный метод не гарантирует формирование оптимального ППОГ, заключается в следующем. Этот метод может исключить несколько маршрутов доверия с относительно низкими уровнями достоверности из-за несовместимости с ранее включённым маршрутом, обладающим более высоким уровнем достоверности. Возможно, что все маршруты с низкой степенью достоверности могут обеспечить более высокую степень достоверности, чем только один предшествующий маршрут с высокой степенью достоверности. В таких случаях, возможным оптимальным решением будет исключение маршрута с высокой достоверностью, а вместо него – включение нескольких маршрутов с низкой достоверностью. Тем не менее, в подобных случаях только метод комплексного поиска (рассмотренный ранее) гарантирует нахождение оптимального ППОГ [172].

Далее рассматривается эвристический метод при преобразовании сложной сети доверия в сеть доверия, отображаемую в ППОГ. Метод поиска является эвристическим в том смысле, что нет необходимости синтезировать оптимальный ППОГ с точки зрения максимальной достоверности вычисляемого доверия. Преимущество метода – в его эффективности [19].

5.1.4.1 Синтез сети доверия, отображаемой в форму ППОГ

Рассматриваемый ниже алгоритм позволяет упростить сложную сеть доверия, например, аналогичную той, которая представлена на рисунке 5.8, с целью синтеза сети доверия, отображаемой в форму ППОГ.

Процедура упрощения сети доверия, не отображаемой в форму ППОГ, представляет собой двухитерационный процесс. Во-первых, анализ сложной сети доверия осуществляется с целью выявления всех возможных маршрутов доверия от аналитика $\mathcal{A}$ до целевого субъекта (объекта) $\mathcal{X}$. Во-вторых, новая сеть доверия, отображаемой в форму ППОГ, синтезируется с нуля путём включения только тех маршрутов доверия из сложной сети доверия, которые не нарушают свойство ППОГ в новой синтезированной сети доверия. Таки образом, окончательный синтезированный граф между исходным аналитиком $\mathcal{A}$ и целевым узлом $\mathcal{X}$ представляет собой сеть доверия, отображаемую в форму ППОГ.

ППОГ может быть построен путём формирования последовательностей, состоящих из параллельных и последовательных структур [171]. Дадим определение ориентированной последовательной и параллельной структуры.

Определение 5.6 (ориентированная последовательная и параллельная структура).

– ориентированная последовательная структура представляет собой замену ребра $[\mathcal{A};\mathcal{C}]$ на два рёбра $[\mathcal{A};\mathcal{B}]$ и $[\mathcal{B};\mathcal{C}]$, в которых $\mathcal{B}$ – новый узел;

– ориентированная параллельная структура представляет собой замену ребра $[\mathcal{A};\mathcal{C}]$ на два ребра $[\mathcal{A};\mathcal{C}]_1$ и $[\mathcal{A};\mathcal{C}]_2$.

Принцип ориентированной последовательно-параллельной структуры представлен на рисунке 5.9.

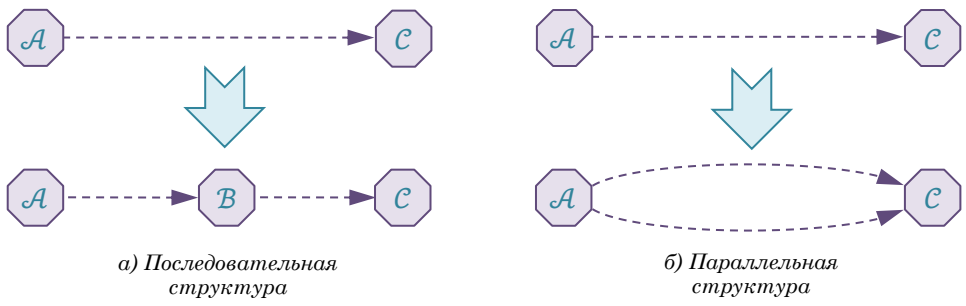

Рисунок 5.9 – Принципы формирования ориентированных последовательной и параллельной структур

На рисунке 5.10 представлена блок-схема алгоритма синтеза сети доверия, отображаемой в форму ППОГ, из сложной сети доверия в соответствие с эвристическим методом. Данный алгоритм включает следующие итерации:

(а) Подготовка к процедуре упрощения сложной сети доверия. Она включает: отображение сложной сети доверия в множество ориентированных рёбер между парами узлов; установку порогового значения $p_{\text{Т}}$ для самой минимально допустимой надёжности маршрутов доверия; формирование пустой сети доверия, отображаемой в форму ППОГ, которая должна быть синтезирована;

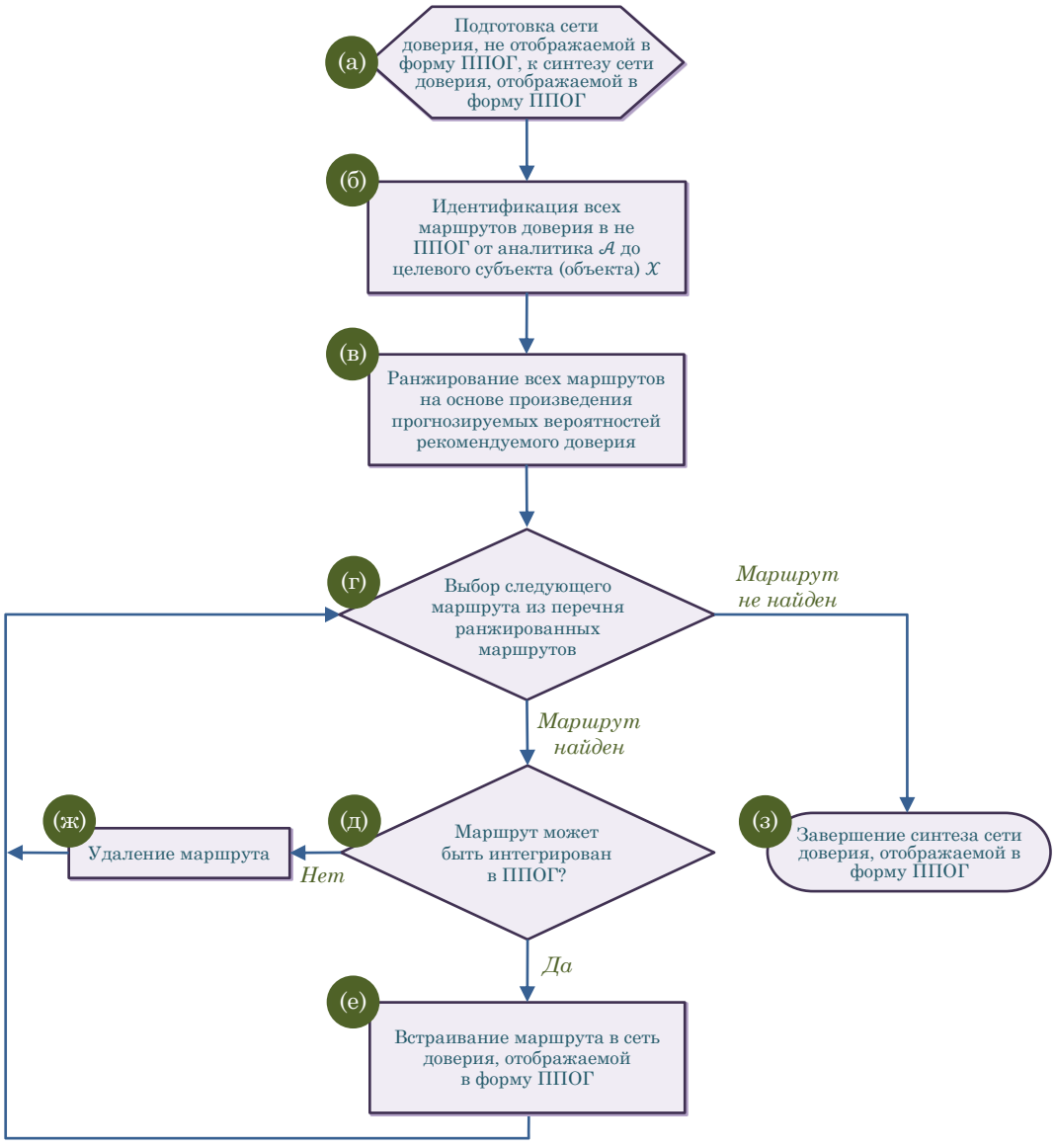

Рисунок 5.10 – Блок-схема алгоритма синтеза ППОГ из сложного не ППОГ

(б) Идентификация каждого маршрута доверия от аналитика $\mathcal{A}$ до целевого узла $\mathcal{X}$. Для каждого маршрута вычислить произведение прогнозируемых вероятностей рёбер рекомендуемого доверия. Последнее ребро функционального доверия/убеждения до целевого субъекта (объекта) $\mathcal{X}$ в произведении не участвует;

(в) Формирование перечня ранжированных маршрутов в соответствии с произведениями, вычисленными в предыдущей итерации, т.е. тому маршруту, который имеет наибольшее значение произведения, присваивается индекс 1. Встраивание маршрута 1, так чтобы начальная сеть состояла из одного маршрута. Установка значения индекса в 1;

(г) Увеличение значения индекса на единицу и выбор следующего маршрута из ранжированного перечня маршрутов. Выйти по завершении, если не осталось ни одного маршрута, или, если вычисленное рекомендуемое доверие маршрута меньше порогового значения $p_{\text{Т}}$. Продолжить, если вычисленное рекомендуемое доверие маршрута пути больше или равно пороговому значению $p_{\text{Т}}$;

(д) Проверка, выбранный маршрут доверия может быть добавлен и встроен в сеть доверия, которая отображается в форму ППОГ. Использовать критерий, представленный в §5.4.2;

(е) Добавить выбранный маршрут доверия, если он встраивается в ППОГ. Существующие ребра доверия не дублируются, только новые ребра доверия встраиваются в ППОГ

(ж) Удалить выбранный маршрут доверия, если он не встраивается в ППОГ;

(з) Синтезированный ППОГ может быть проанализирован в соответствие с алгоритмом, рассмотренным в §5.3.

5.1.4.2 Критерии синтеза ППОГ

В идеальном случае, все возможные маршруты, обнаруженные алгоритмом (рисунок 5.10), должны быть учтены при вычислении значения мнения/доверия. Как правило, ориентированный граф будет включать петлевые маршруты и зависимости (зависимые структуры). Такие ситуации можно избежать, если исключить соответствующие маршруты, однако, это может привести к потере информации. Конкретный критерий выбора необходим для поиска оптимального подмножества маршрутов с целью их включения. Если существует n возможных маршрутов, то существует $(2n-1)$ различных комбинаций при формировании графов, но все из них приемлемы для ППОГ. Назначение алгоритма, представленного на рисунке 5.10, – синтез сети доверия, отображаемой в форме ППОГ, с наименьшими потерями информации относительно первоначальной сложной сети доверия.

На рисунке 5.11 показан простой граф доверия, не отображаемый в форме ППОГ, в котором предполагается, что $\mathcal{A}$ – первоначальный аналитик, а $\mathcal{X}$ – целевой субъект (объект).

Существуют два эвристических правила, используемых для удаления маршрутов: первое – когда маршрут не согласуется с ППОГ, и второе – когда произведение прогнозируемых вероятностей падает ниже заданного порогового значения.

В алгоритме на рисунке 5.10 можно заметить, что итерация (г) обеспечивает соблюдение правила, согласно которому прогнозируемая вероятность произведения рёбер рекомендуемого доверия в графе больше или равна пороговому значению p_{T}. Небольшая величина произведения указывает на низкую достоверность маршрута доверия. После удаления маршрутов с низкой достоверностью, количество маршрутов, которые следует учитывать, снижается, а потери информации остаются незначительными. Последующая итерация (д) проверяет, что маршрут может быть последовательно включён в ППОГ.

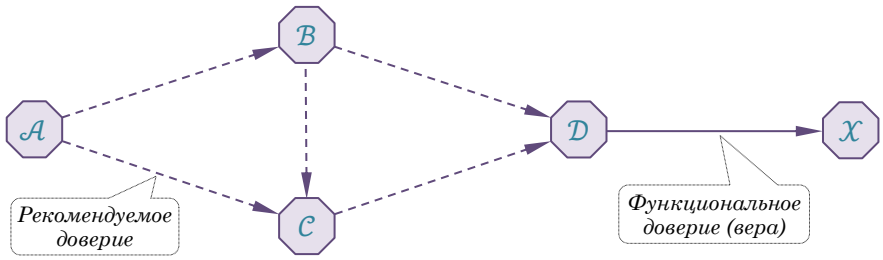

Рисунок 5.11 – Пример сложной сети доверия

В сложной сети доверия, изображённой на рисунке 5.11, представлены три возможных маршрута между субъектами $\mathcal{A}$ и $\mathcal{X}$, которые можно отобразить следующим образом:

$$\begin{aligned} \phi_1 &= ([\mathcal{A};\mathcal{B}] : [\mathcal{B};\mathcal{D}] : [\mathcal{D},\mathcal{X}]), \\ \phi_2 &= ([\mathcal{A};\mathcal{C}] : [\mathcal{C};\mathcal{D}] : [\mathcal{D},\mathcal{X}]), \\ \phi_3 &= ([\mathcal{A};B] : [\mathcal{B};\mathcal{C}] : [\mathcal{C};\mathcal{D}] : [\mathcal{D},\mathcal{X}]). \end{aligned} \tag{5.4}$$

Три маршрута могут сформировать следующие семь возможных комбинаций/графов:

$$\begin{aligned} &\gamma_1 = \phi_1, \quad && \gamma_4 = \phi_1 \diamond \phi_2, \quad && \gamma_7 = \phi_1 \diamond \phi_2 \diamond \phi_3. \\ &\gamma_2 = \phi_2, && \gamma_5 = \phi_1 \diamond \phi_3, && \\ &\gamma_3 = \phi_3, && \gamma_6 = \phi_2 \diamond \phi_3, && \end{aligned} \tag{5.5}$$

Равенство γ_7 отображает сеть доверия, которая включает все возможные маршруты между субъектами $\mathcal{A}$ и $\mathcal{X}$. Проблема равенства γ_7 состоит в том, что оно не является ППОГ, и поэтому не может быть представлено в форме стандартного выражения, в котором каждое ребро участвует в формировании маршрута только один раз. В этом примере один маршрут должен быть удалён из графа с целью получения канонического выражения. Равенства γ_4, γ_5 и γ_6 могут быть приведены к каноническому виду, равенства γ_1, γ_2 и γ_3 уже являются канони-

ческими, и это означает, что все равенства, за исключением равенства γ_7, могут использоваться в качестве основы формирования ППОГ и для вычисления мнения/доверия субъекта $\mathcal{A}$ к субъекту (объекту) $\mathcal{X}$.

Синтез ППОГ начинается с выбора первоначального маршрута, имеющего наибольшую прогнозируемую вероятность рекомендуемого доверия, вычисленную от первоначального субъекта до узла, который является ближайшим соседом конечного целевого субъекта/объекта (т.е. до узла, который имеет прямое функциональное ребро до конечного целевого субъекта/объекта). Затем, один за другим добавляются дополнительные пути в соответствие с алгоритмом, представленном на рисунке 5.10. При добавлении новых маршрутов учитывается весь маршрут от первоначального источника до конечного субъекта (объекта), но субмаршруты, которые уже существуют в синтезированном графе, игнорируются, поэтому на основе раздвоения добавляются только несуществующие субмаршруты. Каждый вновь включённый субмаршрут должен удовлетворять критерию синтеза ППОГ (Опред.5.7).

Критерии из Опред.5.7 касаются первоначального и целевого узлов каждого нового субмаршрута, предполагаемого для включения в существующий граф, а не первоначального источника и конечного целевого субъекта (объекта) графа. Необходимо отметить, что новый субмаршрут может состоять из двух или более узлов.

Определение 5.7 (критерии синтеза ППОГ при добавлении субмаршрута).

1. Целевой узел в существующем графе должен быть достижимым от первоначального узла.

2. Узлы источника и целевого субъекта (объекта) в существующем графе должны иметь одинаковые степени вложенности.

3. Степени вложенности узлов источника и целевого субъекта (объекта) в существующем графе должны быть равны или меньше степени вложенности всех промежуточных узлов.

□

Далее рассматриваются примеры использования указанных критериев. На рисунках 5.12, 5.13 и 5.14 показан способ добавления новых субмаршрутов, который сохраняет свойства ППОГ. Это означает, что новые субмаршруты включают более двух узлов, но на примерах показано добавление субмаршрутов состоящих только из одиночного ребра между источником и целевым субъектом (объектом).

На рисунках, степени вложенности узлов и рёбер обозначены целыми числами. *Раздвоение* – случай, когда узел имеет два или более входящих, или исходящих рёбер, оно обозначается скобками (в шестигранниках, обозначающих узлы). Открытая скобка «(» увеличивает степень вложенности на 1, а закрывающая скобка «)» уменьшает степень вложенности на 1. Субмаршрут – часть маршрута без раздвоений. Знак равенства «=» означает, что узел –

часть субмаршрута, и в этом случае степень вложенности ребра со стороны символа «=» равна степени вложенности узла.

Каждый раз, когда новый маршрут включается в старый граф, некоторые части субмаршрута могут уже существовать в старом графе, в таком случае они не включаются. А некоторые части субмаршрутов, которые ещё не существуют, должны быть включены в старый граф на основе процедуры раздвоения.

Первый критерий синтеза ППОГ. Рисунок 5.12 иллюстрирует первый критерий из **Опред.5.7**. Новое ребро $[\mathcal{B};\mathcal{C}]$ удаляется, так как узел $\mathcal{C}$ не достижим из узла $\mathcal{B}$ в существующем графе. С другой стороны, новое ребро $[\mathcal{A};\mathcal{D}]$ может быть включено, так как узел $\mathcal{D}$ достижим из узла $\mathcal{A}$.

Ребро $[\mathcal{A};\mathcal{D}]$, которое было включено, имеет такую же степень вложенности как и субмаршруты $([\mathcal{A};\mathcal{B}] : [\mathcal{B};\mathcal{D}])$ и $([\mathcal{A};\mathcal{C}] : [\mathcal{C};\mathcal{D}])$. Выражения существующего и вновь образованного графов, изображённых на рисунке 5.12, следующие:

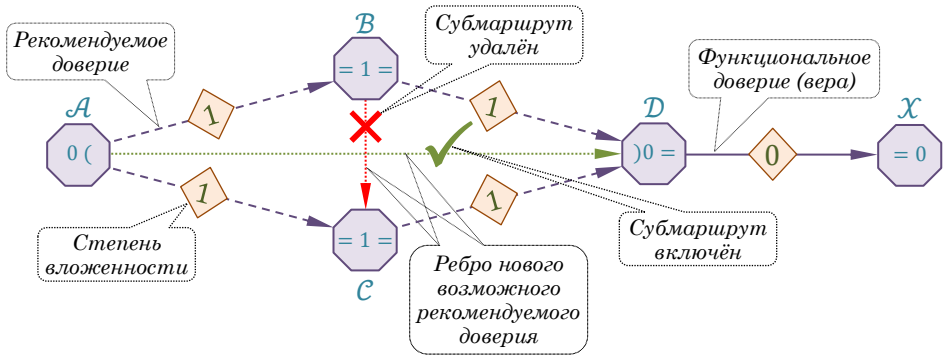

Рисунок 5.12 – Визуализация критерия обязательной достижимости целевого субъекта (объекта) от первоначального источника

$$\text{Существующий граф: } \Big(\big(([\mathcal{A};\mathcal{B}] : [\mathcal{B};\mathcal{D}])\diamond([\mathcal{A};\mathcal{C}] : [\mathcal{C};\mathcal{D}])\big) : [\mathcal{D};\mathcal{X}]\Big),$$
$$\text{Обновлённый граф: } \Big(\big(([\mathcal{A};\mathcal{B}] : [\mathcal{B};\mathcal{D}])\diamond([\mathcal{A};\mathcal{C}] : [\mathcal{C};\mathcal{D}])\diamond[\mathcal{A};\mathcal{D}]\big) : [\mathcal{D};\mathcal{X}]\Big). \quad (5.6)$$

Следует заметить, что скобки вокруг субмаршрутов, например $([\mathcal{A};\mathcal{B}] : [\mathcal{B};\mathcal{D}])$, не изображены на рисунке 5.12, так как эти скобки не отражают вложенности, а просто группируют рёбра, принадлежащие одному и тому же субмаршруту.

Второй критерий синтеза ППОГ. Иллюстрация второго критерия из **Опред.5.7** представлена на рисунке 5.13. Новое ребро $[\mathcal{B};\mathcal{D}]$ удалено, так как узлы $\mathcal{B}$ и $\mathcal{D}$ имеют различные степени вложенности, а новое ребро $[\mathcal{A};\mathcal{D}]$ включено, так как узлы $\mathcal{A}$ и $\mathcal{D}$ имеют равные степени вложенности. Узел $\mathcal{A}$, фактически, имеет степени вложенности 0, 1 и 2, соответственно, так как он является узлом источником, а также соединяет две отдельные ветви со степенями вложенности 1 и 2, которые начинаются от узла $\mathcal{A}$.

Включённое новое ребро $[\mathcal{A};\mathcal{D}]$ формирует дополнительную степень вложенности, которое также приводит к увеличению степеней вложенности субмаршрутов ($[\mathcal{A};\mathcal{B}]:[\mathcal{B};\mathcal{C}]$) и $[\mathcal{A};\mathcal{C}]$ до степени вложенности 3. Кроме того, ребро $[\mathcal{C};\mathcal{D}]$ увеличивает степень вложенности до 2. Выражения существующего и вновь образованного графов, изображённых на рисунке 5.13, следующие:

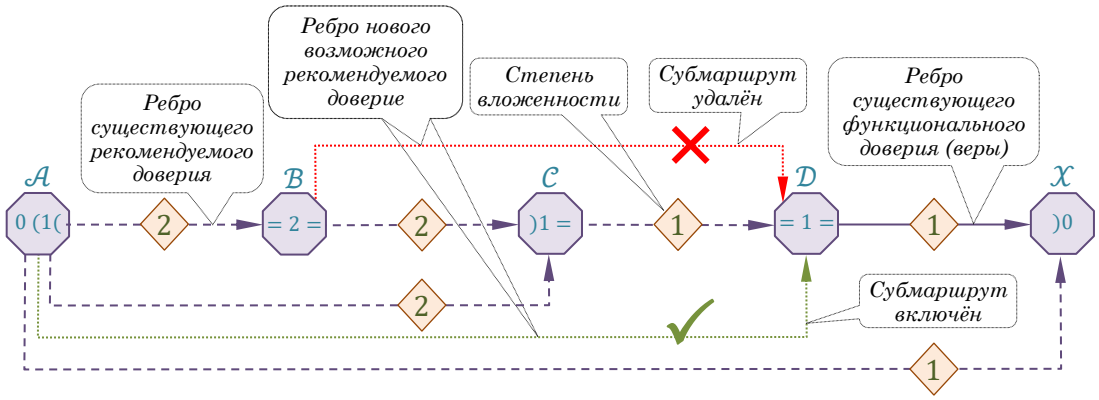

Рисунок 5.13 – Визуализация критерия обязательного равенства степеней вложенности первоначального источника и целевого субъекта (объекта)

$$\text{Существующий граф: } \Big(\big(\big(([\mathcal{A};\mathcal{B}]:[\mathcal{B};\mathcal{C}])\diamond[\mathcal{A};\mathcal{C}]\big):[\mathcal{C};\mathcal{D}]:[\mathcal{D},\mathcal{X}]\big)\diamond[\mathcal{A},\mathcal{X}]\Big),$$

$$\text{Обновлённый граф: } \Big(\big(\big(\big(([\mathcal{A};\mathcal{B}]:[\mathcal{B};\mathcal{C}])\diamond[\mathcal{A};\mathcal{C}]\big):[\mathcal{C};\mathcal{D}]\big)\diamond[\mathcal{A};\mathcal{D}]\big):[\mathcal{D},\mathcal{X}]\big)\diamond[\mathcal{A},\mathcal{X}]\Big). \quad (5.7)$$

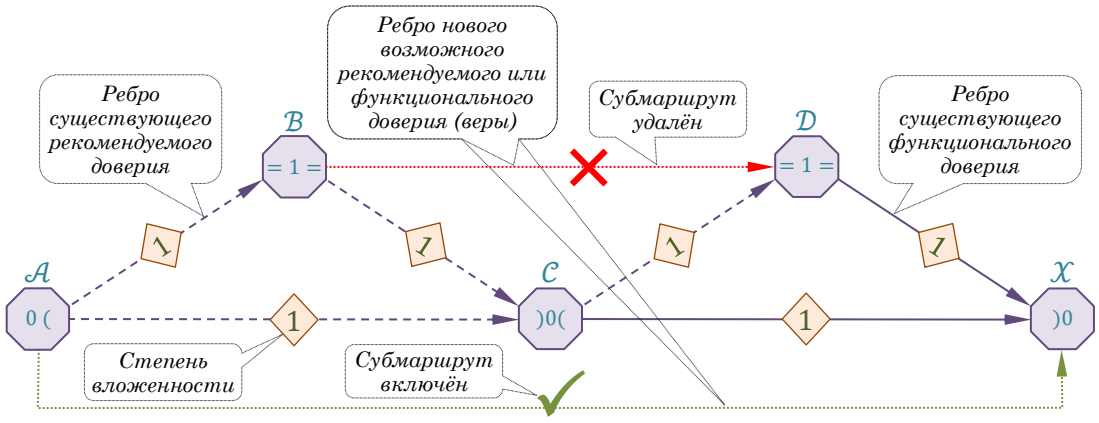

Рисунок 5.14 – Визуализация критерия, согласно которому уровни вложенности промежуточных узлов должны быть равны или превышать уровни источника и цели

Третий критерий синтеза ППОГ. Иллюстрация третьего критерия из **Опред.5.7** представлена на рисунке 5.14. Новое ребро $[\mathcal{B};\mathcal{D}]$ удалено, так как узел $\mathcal{C}$ имеет степень вложенности, который ниже степени вложенности узлов $\mathcal{B}$ и $\mathcal{D}$, а новое ребро $[\mathcal{A},\mathcal{X}]$ включено, так как степень вложенности узла $\mathcal{C}$ равна степеням вложенности узлов $\mathcal{A}$ и $\mathcal{X}$.

Вновь включённое ребро $[\mathcal{A}, \mathcal{X}]$ формирует дополнительную степень вложенности, которое также приводит к увеличению степеней вложенности существующих субмаршрутов. Выражения существующего и вновь образованного графов, изображённых на рисунке 5.14, следующие:

$$\text{Существующий граф: } \Big(\big(([\mathcal{A};\mathcal{B}] : [\mathcal{B};\mathcal{C}])\diamond[\mathcal{A};\mathcal{C}]\big) : \big(([\mathcal{C};\mathcal{D}] : [\mathcal{D},\mathcal{X}])\diamond[\mathcal{C},\mathcal{X}]\big)\Big),$$

$$\text{Обновлённый граф: } \Big(\big(\big(([\mathcal{A};\mathcal{B}] : [\mathcal{B};\mathcal{C}])\diamond[\mathcal{A};\mathcal{C}]\big) : \big(([\mathcal{C};\mathcal{D}] : [\mathcal{D},\mathcal{X}])\diamond[\mathcal{C},\mathcal{X}]\big)\big)\diamond[\mathcal{A},\mathcal{X}]\Big). \quad (5.8)$$

Следует отметить, что новые субмаршруты могут иметь произвольное количество узлов, хотя в рассмотренных выше примерах показаны только новые субмаршруты, отображаемые в виде одного ребра между источником и целевым субъектом (объектом). Используя алгоритм синтеза ППОГ (рисунок 5.10) в сочетании с критериями соответствия ППОГ из **Опред.5.7**, можно синтезировать каноническую сеть доверия. В свою очередь, такая каноническая сеть доверия может быть легко проанализирована с помощью операторов слияния и транзитивности доверия.

5.2 Синтез КЗСУ (системы доверия) на основе инфраструктуры открытых ключей

5.2.1 Ретроспектива

В Российской Федерации начало формирования КЗСУ (систем доверия) на основе ИОК относится к середине 90-х годов прошлого века. Это связано, в первую очередь, с тем, что область криптографической защиты информации стала открытой[33] и общедоступной. Появление асимметричных криптографических систем на российском рынке повлекло за собой возникновение коммерческих ЦС. Более того, этот процесс носил «стихийный» характер и практически не контролировался со стороны государства [5]. Отсутствие контроля рынка ИОК-услуг привело к созданию огромного числа (около 300) ЦС, функционирование которых до сих пор практически никак не регулируются. Причина тому – отсутствие федеральной политики (или стратегии) создания инфраструктур открытых ключей в России. Современная Национальная программа «Цифровая экономика Российской Федерации»[34] не содержит каких-либо упоминаний о создании ИОК и систем доверия на их основе.

---

[33] До конца 1991 года криптография, как наука, и её практические (реализационные) аспекты, включая производство шифровальных систем и средств, были, исключительно, в ведении специальных служб СССР.

[34] Проект «Национальная Программа «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. № 7.

5.2.1.1 Общероссийский государственный информационный центр

В 2004 году было образовано Федеральное агентство по информационным технологиям (ФАИТ), на которое были возложены функции государственного регулятора и координатора работ по созданию в Российской Федерации информационного общества (*E*-правительства). ФАИТ стал федеральным органом исполнительной власти в области использования ЭП. В частности, ФАИТ курировало реализацию Федеральной целевой программы (ФЦП) «Электронная Россия (2002… 2010 годы)». С созданием ФАИТ начался сложный процесс становления отечественной ИОК.

В рамках выполнения этой Программы был образован Общероссийский государственный информационный центр (ОГИЦ, Постановление Правительства РФ от 25.12.2007 г. №931). Цель создания ОГИЦ – 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 информационных и телекоммуникационных технологий (рисунок 5.15).

Парадигмами функционирования ОГИЦ являются предоставление государственных услуг в электронном виде в режиме «одного окна» и выполнение функций федерального удостоверяющего центра (УЦ, модель ЦС+ЦР), являющегося корневым в системе УЦ национальной ИОК России.

По своим стратегическим задачам ОГИЦ стал *информационно-технологическим ядром российского информационного общества*. Общие решаемые ОГИЦ задачи:

- обеспечение юридически значимого ЭДО и информационно-телекоммуникационного взаимодействия органов власти РФ между собой;
- предоставление технических средств и ИТ для государственных АИС;
- официальное информирование о деятельности органов государственной власти и органов местного самоуправления и предоставление населению и организациям государственных услуг в электронном виде.

Информационное взаимодействие органов власти РФ между собой и с гражданами осуществляется в рамках отдельных ИТС – межведомственного и публичного «контуров» (рисунок 5.15), каждый из которых есть совокупность взаимосвязанных информационно-технологических и телекоммуникационных объектов.

5.2.1.2 Ведомственная система доверия ФНС РФ

Наиболее примечательный (и, пожалуй, единственный) пример создания системы доверия (КЗСУ на основе ИОК) – это ведомственная система доверия Федеральной налоговой службы РФ на основе ИОК, которая просуществовала с 2006 по 2014 гг. Данная система именовалась как «*Сеть доверенных удостоверяющих центров*» (СДУЦ). Функциональная схема СДУЦ (сеть доверия) представлена на рисунке 5.16.

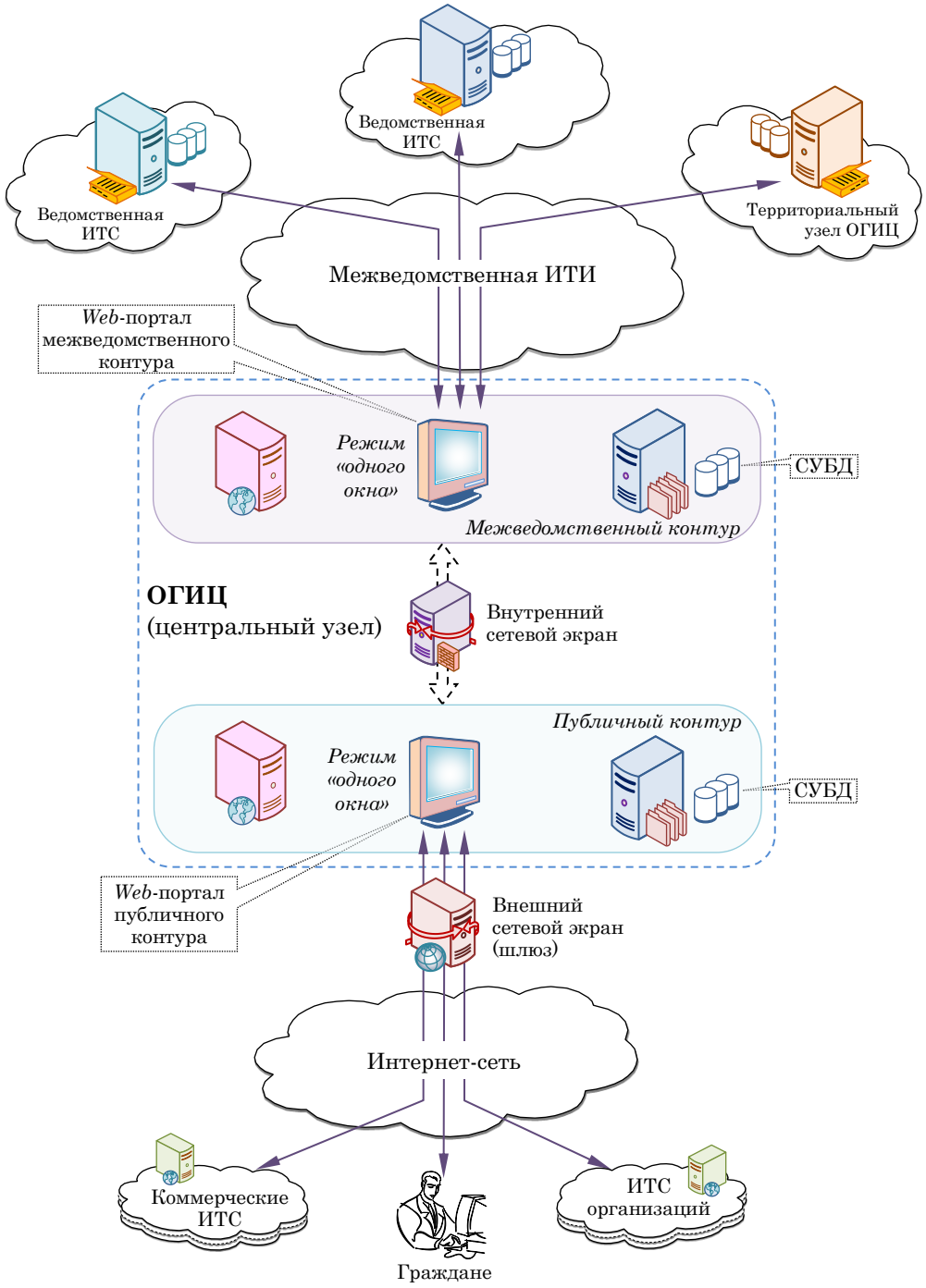

Рисунок 5.15 – Функциональная структура ОГИЦ

ФНС России была предложена государственная услуга – подача налоговой декларации в электронном виде. Данная услуга предусматривала наличие ЭП под документом налоговой отчётности. В рамках реализации указанной услуги предусматривалось:

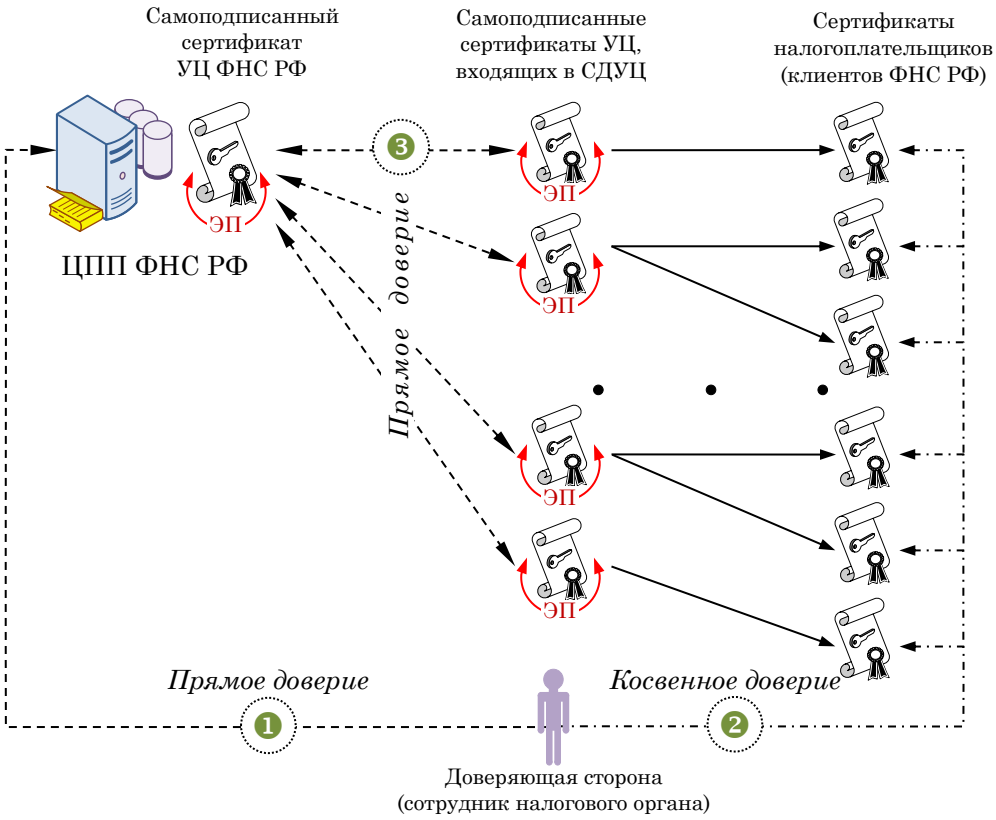

Рисунок 5.16 – Функциональная схема СДУЦ ФНС РФ (сеть доверия)

а. Создание УЦ ФНС РФ;

б. Создание сети доверенных УЦ во главе с УЦ ФНС (т.е. ИОК$_{ФНС}$);

в. Разработка единой политики сертификации (включая формат СЕРТ$_{ОК}$) для всех УЦ, входящих в СДУЦ;

г. Ведение РСДС удостоверяющим центром ФНС;

д. Заключение договоров с УЦ, кандидатами на вхождение в СДУЦ, и проведение их аккредитации;

е. Выбор и использование единого КПО для генерации ключей и выпуска СЕРТ$_{ОК}$ всеми УЦ, входящими в СДУЦ;

ж. Применение единого порядка функционального и правового взаимодействия всех УЦ, входящих в СДУЦ, с УЦ ФНС и др.

В этой системе должны были быть обеспечены следующие типы доверия:

Д1 (§4.3.2.1) – ФНС РФ и УЦ, входящий в СДУЦ и обслуживающий налогоплательщика, обеспечивают (защищают) его неприкосновенность (персональные данные налогоплательщика);

Д2 (§4.3.2.1) – ФНС РФ и УЦ, входящий в СДУЦ и обслуживающий налогоплательщика, внедрили удовлетворяющие налогоплательщика процедуры регистрации и способы аутентификации (исходя из предположений налогоплательщика);

Д3 (§4.3.2.2) – налогоплательщик обслуживает (хранит) свои параметры для аутентификации (включая закрытый ключ) адекватным способом;

Д7 (§4.5.2.3) – ФНС РФ и УЦ, входящий в СДУЦ и обслуживающий налогоплательщика, а также формирующий параметры для аутентификации, реализовали адекватные процедуры регистрации пользователей и выпуска параметров для аутентификации.

СДУЦ ФНС РФ показала свою состоятельность и эффективность. Однако, она была упразднена с принятием Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Одна из возможных причин ликвидации СДУЦ ФНС РФ – это необеспечение доверия **Д3**, так как хранение закрытого ключа предусматривает выполнение весьма жёстких требований по предотвращению налогоплательщиком НСД к его ключевой информации. Вместе с тем, налогоплательщики могли испытывать неудобство, связанное с одноразовым применением закрытого ключа и $СЕРТ_{ОК}$, т.е. только раз в год при отправке налоговой отчётности в территориальный орган ФНС РФ. А закрытый ключ и $СЕРТ_{ОК}$ необходимо было хранить в защищённом состоянии в течении всего года.

Ещё одна из возможных причин ликвидации СДУЦ ФНС РФ – это использование всеми УЦ, входящими в СДУЦ, КПО для генерации ключей и выпуска $СЕРТ_{ОК}$ только одной компании «КриптоПро», что противоречит антимонопольной политике, реализуемой Федеральной антимонопольной службой РФ.

Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» ввёл понятия «*простой*», «*неквалифицированной*» и «*квалифицированной*» ЭП. В частности, ФНС РФ перешла на использование простой ЭП[35], которая не предусматривает выпуск $СЕРТ_{ОК}$, что существенно упростило процедуры сдачи налогоплательщиками годовой налоговой отчётности в электронном виде.

В этой связи ФНС РФ самостоятельно выполняет требования по обеспечению доверия, т.е. без участия внешних УЦ. Другими словами, ФНС РФ:

---

[35] С точки зрения криптографической науки, простая ЭП электронной подписью не является, т.к. простая ЭП – это пароль и регистрационные данные. Простая ЭП обеспечивает всего лишь парольную аутентификацию и не обеспечивает целостность и авторство сообщений, а также уязвима к атакам типа «повторная передача».

i. Обеспечивает неприкосновенность налогоплательщика (защищает его персональные данные);

ii. Внедрила удовлетворяющие налогоплательщика процедуры регистрации и способы аутентификации (исходя из предположений налогоплательщика);

iii. Реализовала адекватные упрощённые процедуры регистрации пользователей и выпуска параметров для аутентификации.

Вместе с тем, налогоплательщик должен обеспечить доверие к себе со стороны ФНС РФ, т.е. обслуживать (хранить) свои параметры для аутентификации адекватным способом, который предотвращает НСД к ним.

5.2.1.3 Текущее состояние ИОК в РФ

В настоящее время структура ОГИЦ включает только корневой федеральный УЦ (ФУЦ, нулевой уровень иерархии) и несколько УЦ первого уровня (ФУЦ). А в Минцифры ведётся список аккредитованных УЦ в TSL-формате (рисунок 3.16, [93]).

Дальнейшее развитие ИОК РФ после упразднения в августе 2010 года ФАИТ практически не ведётся. Это связано с тем, что:

– отсутствует какой-либо контроль со стороны государства, дальнейшее развитие ИОК отдано «на откуп» бизнесу. Другими словами, отсутствует государственная политика информатизации. Хотя примеры других экономически развитых стран говорят об обратном: необходимо прямое активное и непосредственное участие органов государственной власти в развитии информационного общества в качестве регуляторов;

– ФЦП «Электронная Россия (2002…2010 годы)» и государственная программа Российской Федерации «Информационное общество (2011–2020 годы)» завершились провалом. Информационное общество создано не было. Все ресурсы, выделяемые на программы, были использованы, в основном, на закупку компьютеров, программного обеспечения и создание ведомственных ИТС, которые по-прежнему остаются функционально несовместимыми и потому не могут стать технологической основой современного информационного общества. В частности, по завершении ФЦП «Электронная Россия (2002…2010 годы)» было вскрыто множество фактов коррупции и т.п.;

– сегодня существует значительная нехватка профессиональных кадров в области ИОК (фактически реализацией государственных программ занимались некомпетентные госслужащие и сотрудники привлекаемых организаций). Ситуация усугубляется ещё и отсутствуем в России достаточной системы подготовки специалистов по этому направлению. В

рамках Учебно-методического объединения ВУЗов России по подготовке специалистов в области ИБ этому направлению не уделяется должного внимания, то есть, нет образовательной политики по подготовке кадров в области ИОК;

– в России существует около 100 УЦ, включённых в РСДС (аккредитованы), которые обслуживают федеральные, региональные и муниципальные органы государственной власти, конкретные организации и региональный бизнес. И большинство из них заинтересованы в государственном регулировании этой отрасли на основе единых правил с использованием государственной и частно-государственной «надстройки», которая объединит УЦ всех существующих ИТС в едином правовом и технологическом поле. Наличие большого числа независимых УЦ не позволяет им построить иерархическую или сетевую структуру доверия на основе взаимной сертификации по примеру североамериканской модели;

– все УЦ в Российской Федерации организованы на основе модели ЦС+ЦР. Данная модель является «*уязвимой*», так как предоставляет *возможность выпуска фальсифицированных СЕРТ$_{ОК}$*. Фальсифицированные СЕРТ$_{ОК}$ могут быть выпущены УЦ, сотрудники которого находятся в преступном сговоре с криминальными структурами, двумя способами. Во-первых, персональные данные «жертвы» могут быть предоставлены криминалом в УЦ, который в условиях шантажа выпустит фальсифицированный СЕРТ$_{ОК}$ на имя «жертвы». Во-вторых, «жертвой» может стать сам клиент УЦ, который предоставил УЦ свои персональные данные, а этот мошеннический УЦ (либо его злонамеренные сотрудники) может(гут) без согласия своего клиента выпустить фальсифицированный СЕРТ$_{ОК}$ на его имя.

Следовательно, переход российской экономики на «цифровые рельсы» (Национальная программа «Цифровая экономика Российской Федерации») *потребует* создания структуры доверия на основе объединения КЗСУ (ИОК) ИТС, формирующих ИТИЦЭ. Такая структура способна решить подавляющее большинство существующих проблем, связанных с обеспечением ИБ, включая защиту граждан и бизнеса.

5.2.2 Исходные условия и синтез системы управления криптографической защитой (системы доверия) на основе ИОК

В настоящее время в России существует около 100 УЦ, которые включены в РСДС Минцифры (аккредитованы) и обслуживают ИТС федеральных, региональных и муниципальных органов государственной власти, конкретных государственных и коммерческих организаций, а также их пользователей. Аккредитованные УЦ можно разделить три группы:

1. ФУЦ в составе ОГИЦ;

2. Ведомственные/корпоративные УЦ, которые составляют основу КЗСУ ИТС, и могут быть единственными внутри ведомств/организаций. Если же внутри ведомств/организаций таких УЦ несколько, то, как правило, они объединены во внутренние ИОК ИТС (иерархические структуры), возглавляемые корневыми УЦ и составляющие основу КЗСУ;

3. Коммерческие УЦ, которые не объединены в какие-либо структуры, ни в иерархические, ни в сетевые (рисунок 3.2).

Синтез. Используя аппарат СЛ и эвристический метод поиска сети доверия, можно определить *основное требование к КЗСУ (системе доверия) – это должна быть ССД, отображаемая в ППОГ*. Кроме этого, такая *ССД должна иметь минимальное число рёбер* между истоком (источником) и стоком, а также, по возможности, *не иметь параллельных маршрутов доверия*.

С точки зрения доверия, ведомственные/корпоративные ИОК (иерархии УЦ), являющиеся основой КЗСУ ИТС, используются для внутренних потребностей ЭДО и контролируются соответствующими администрациями, и поэтому считаются надёжными. В этой связи, если ведомствам/организациям потребуется объединение своих иерархий УЦ (КЗСУ своих ИТС), то данную задачу можно решить несколькими способами – с помощью взаимной сертификации корневых УЦ (§4.10.4), связующего УЦ (§4.10.5) и ЦПП (§4.10.7). Однако, первые два способа требуют большое количество процедур взаимной сертификации между корневыми УЦ и корневыми УЦ со связующим УЦ, что в реальных условиях является трудновыполнимой задачей вследствие невозможности преодоления существующих противоречий различных политик сертификации, а также по экономическим причинам.

Вместе с тем, наличие большого числа коммерческих не связанных между собой УЦ в некотором смысле «упрощает» решение задачи формирования объединённой системы доверия на основе ИОК.

С эвристической точки зрения, использование единого ЦПП для корневых УЦ ведомств/организаций (КЗСУ ИТС) и коммерческих УЦ, – наиболее приемлемое решение для формирования системы доверия на основе ИОК. Такую модель объединённой системы доверия можно проиллюстрировать с помощью рисунка 5.17.

Очевидно, в этой модели (по аналогии с ранее существовавшей системой доверия ФНС РФ, §5.2.1.2) необходимо, чтобы:

– центральный ЦПП заключил соответствующий договор с каждым УЦ (включая корневые УЦ ИТС и коммерческие УЦ), желающим присоединится к объединённой системе доверия на основе ИОК. Такие договоры должны включать необходимые правовые и технологические аспекты взаимодействия в рамках объединённой системы доверия, а также формат $СЕРТ_{ОК}$ и СОС;

– центральный ЦПП и присоединённые УЦ обеспечили (защитили) неприкосновенность (персональные данные) владельцев СЕРТ$_{ОК}$;

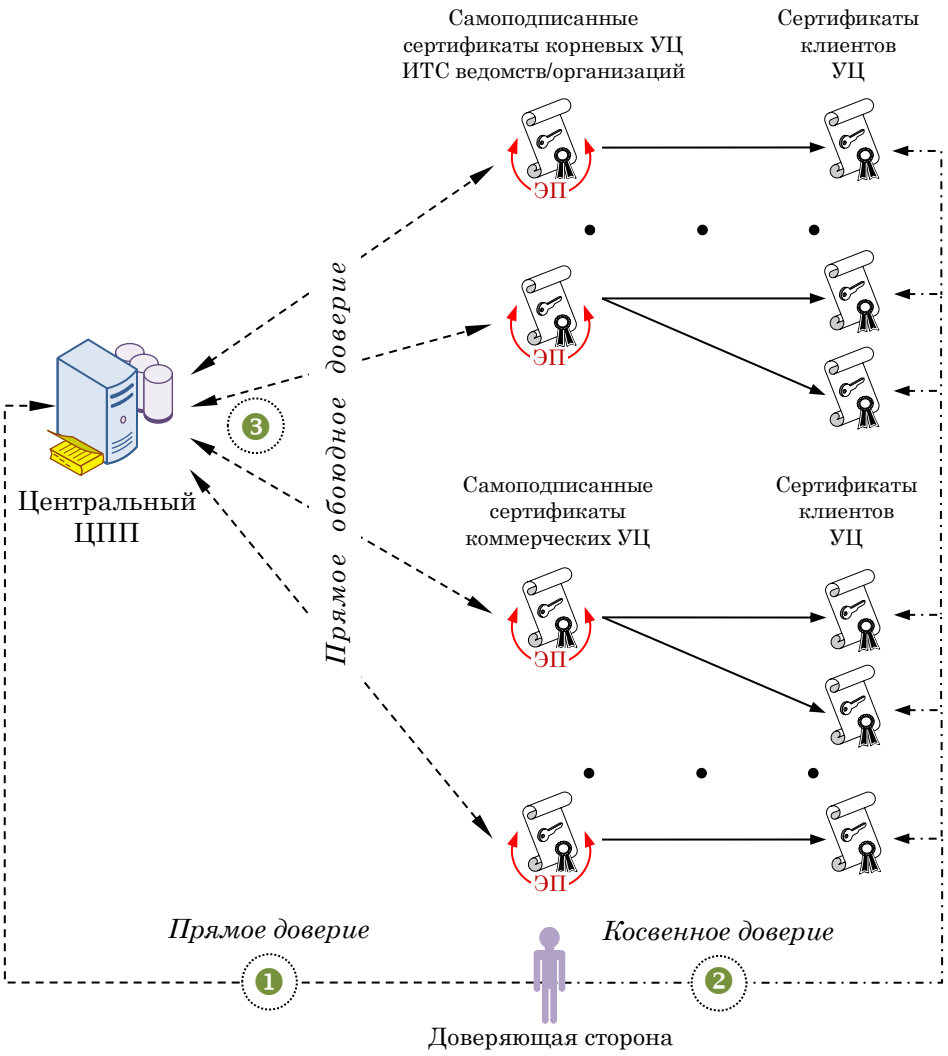

Рисунок 5.17 – Модель объединённой системы доверия на основе ИОК с единым ЦПП

– центральный ЦПП и присоединённые УЦ внедрили удовлетворяющие предполагаемых владельцев СЕРТ$_{ОК}$ процедуры регистрации и способы аутентификации (исходя из предположений будущих владельцев СЕРТ$_{ОК}$);

– владелец СЕРТ$_{ОК}$ обслуживал (хранил) свои параметры для аутентификации (включая закрытый ключ) адекватным способом;

– центральный ЦПП и присоединённые УЦ реализовали адекватные процедуры регистрации владельцев СЕРТ$_{ОК}$ и выпуска параметров для аутентификации.

Модель, изображённая на рисунке 5.17, может быть представлена как совокупность (суперпозиция) отдельных маршрутов транзитивного доверия (§2.12.3). Тогда, используя **Опред.5.1** и **Опред.5.2**, синтезируем маршруты транзитивного доверия, как ППОГ (рисунок 5.18).

На рисунке 5.18 представлены: $\mathcal{A}$ – доверяющая сторона, $\mathcal{B}$ – ЦПП, $\mathcal{C}_i$ – i-ый УЦ и $\mathcal{K}_i$ – владелец СЕРТ$_{ОК}$, изданного $\mathcal{C}_i$, где $i = \overline{1,n}$.

Теперь упростим модель, изображённую на рисунке 5.18, т.е. выделим из неё только один маршрут транзитивного доверия, соответствующий ППОГ (рисунок 5.19).

Ребро $[\mathcal{A};\mathcal{B}]$ – рекомендуемое доверие субъекта $\mathcal{A}$ к субъекту $\mathcal{B}$ (мнение $\omega_{\mathcal{B}}^{\mathcal{A}}$), которое было сформировано субъектом $\mathcal{A}$ на основе рекомендации субъекта $\mathcal{B}$ относительно субъекта $\mathcal{C}$. В данном случае, субъекту $\mathcal{A}$ известно, что субъект $\mathcal{B}$ – это ЦПП, который взаимодействует с аккредитованным УЦ на основе соответствующего заключённого с ним договора.

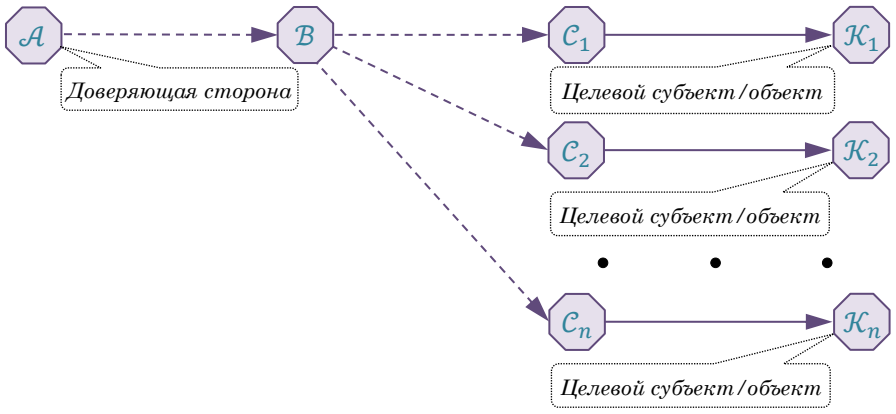

Рисунок 5.18 – Совокупность маршрутов транзитивного доверия в форме ППОГ в национальной системе доверия

Ребро $[\mathcal{B};\mathcal{C}]$ – рекомендуемое доверие субъекта $\mathcal{B}$ к субъекту $\mathcal{C}$ (мнение $\omega_{\mathcal{C}}^{\mathcal{B}}$), которое было сформировано субъектом $\mathcal{B}$ на основе рекомендации субъекта $\mathcal{C}$ относительно субъекта $\mathcal{K}$. В данном случае, ЦПП (субъект $\mathcal{B}$) взаимодействует с аккредитованным УЦ (субъекта $\mathcal{C}$) на основании соответствующего заключённого с ним договора. Кроме того, ЦПП (субъект $\mathcal{B}$) убеждён и может проверить, что аккредитованный УЦ (субъекта $\mathcal{C}$) корректно реализует политику сертификации и регулярно публикует ОДС.

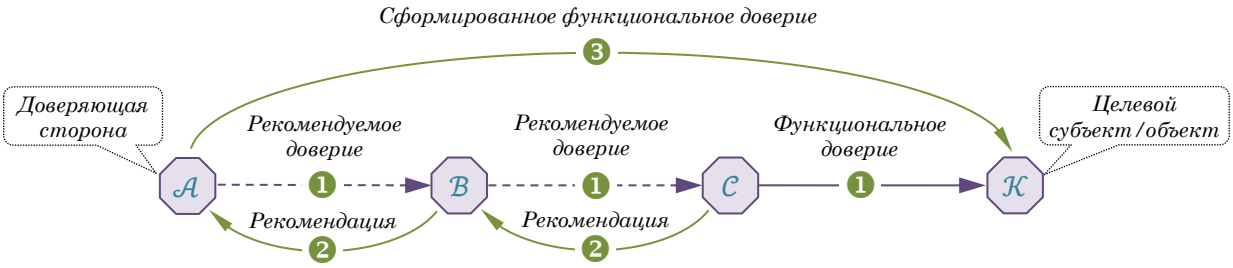

Рисунок 5.19 – Маршрут транзитивного доверия в форме ППОГ в объединённой системе доверия

Ребро $[\mathcal{C},\mathcal{K}]$ – функциональное доверие субъекта $\mathcal{C}$ к субъекту $\mathcal{K}$ (мнение $\omega_{\mathcal{K}}^{\mathcal{C}}$), которое было сформировано субъектом $\mathcal{C}$ на основе, например, анализа результатов регистрации субъекта $\mathcal{K}$, а также на основе договора на обслуживание, который был заключён с субъектом $\mathcal{K}$. А результатом такого доверия стало издание СЕРТ$_{ОК}$ для субъекта $\mathcal{K}$.

Очевидно, что маршрут транзитивного доверия (рисунок 5.19) – это простой последовательный орграф $[\mathcal{A},\mathcal{K}]$, соответствующий следующему равенству:

$$[\mathcal{A},\mathcal{K}] = [\mathcal{A};\mathcal{B}] : [\mathcal{B};\mathcal{C}] : [\mathcal{C},\mathcal{K}] = [\mathcal{A};\mathcal{B};\mathcal{C},\mathcal{K}] \quad , \qquad (5.11)$$

и который отражает сформированное мнение субъекта $\mathcal{A}$ о доверии к субъекту $\mathcal{K}$ $\omega_{\mathcal{K}}^{\mathcal{A}}$.

На рисунке 5.20 представлен пример проведения интерактивной транзакции (например, приобретение товаров) между ПЭУ (субъект $\mathcal{A}$, Интернет-магазин) и пользователем (субъект $\mathcal{K}$, покупатель), в рамках которой ПЭУ обращается в ЦПП (к субъекту $\mathcal{B}$) с целью подтверждения подлинности СЕРТ$_{ОК}$, выпущенного УЦ ($\mathcal{C}$) и предоставленного субъектом $\mathcal{K}$ в начальной фазе транзакции. Пример на рисунке 5.20 соответствует установлению прямого доверия ПЭУ к СЕРТ$_{ОК}$ покупателя на основе маршрута транзитивного доверия (через ЦПП), представленного на рисунке 5.19.

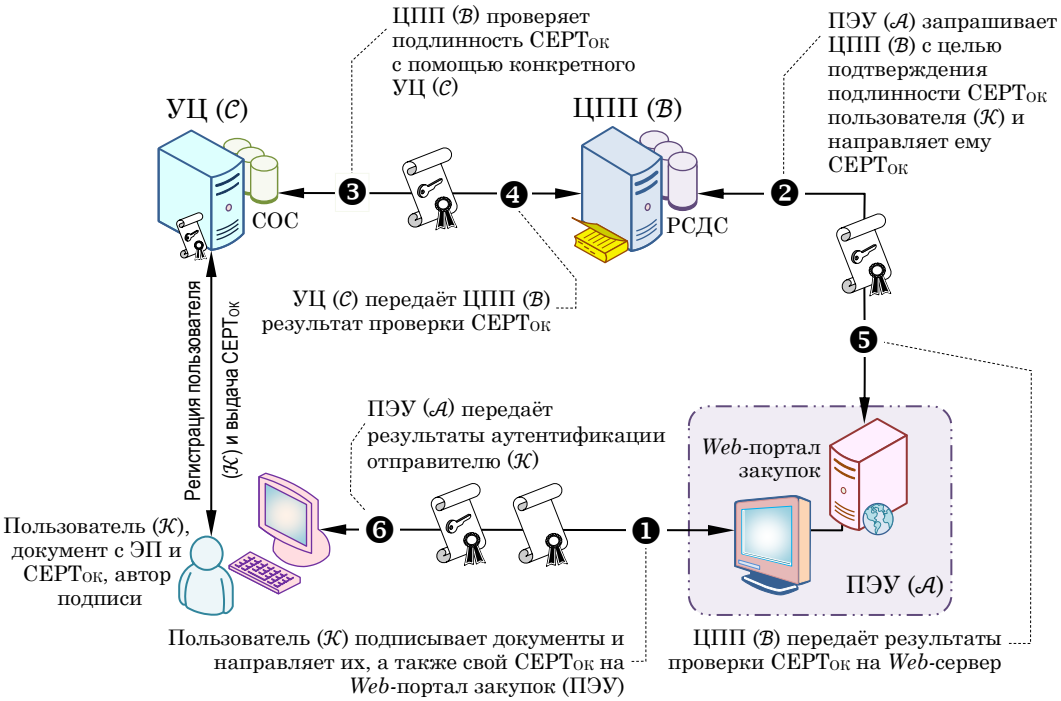

Рисунок 5.20 – Пример формирования доверия ПЭУ ($\mathcal{A}$) к СЕРТ$_{ОК}$ ($\mathcal{K}$), изданному УЦ ($\mathcal{C}$), через ЦПП ($\mathcal{B}$)

Анализ. Теперь проанализируем полученное равенство (5.11). В таблице 5.3 представлены рёбра доверия в маршруте транзитивного доверия (рисунок 5.19).

Таблица 5.3 – Рёбра доверия в маршруте транзитивного доверия, представленном на рисунке 5.19

Источник $\mathcal{A}$	**Целевой объект** $\mathcal{K}$	**Тип доверия**	**Мнение**
$\mathcal{A}$	$\mathcal{B}$	Рекомендуемое	$\omega_{\mathcal{B}}^{\mathcal{A}}$
$\mathcal{B}$	$\mathcal{C}$	Рекомендуемое	$\omega_{\mathcal{C}}^{\mathcal{B}}$
$\mathcal{C}$	$\mathcal{K}$	Функциональное	$\omega_{\mathcal{K}}^{\mathcal{C}}$

Введём произвольные значения мнений о доверии: $\omega_{\mathcal{B}}^{\mathcal{A}} = (0.90; 0.05; 0.05; 0.95)$, $\omega_{\mathcal{C}}^{\mathcal{B}} = (0.85; 0.10; 0.05; 0.80)$ и $\omega_{\mathcal{K}}^{\mathcal{C}} = (0.80; 0.20; 0.00; 0.75)$. Теперь, используя оператор понижения доверия (§2.12.4) и равенства (2.21) и (2.22) для понижения доверия в многовекторных маршрутах транзитивного доверия, получаем $\omega_{\mathcal{K}}^{[\mathcal{A};\mathcal{C}]} = (0.6766; 0.1677; 0.1557; 0.7934)$. Исходные данные для маршрута транзитивного доверия (рисунок 5.19) и результат вычисления итогового мнения о доверии к субъекту $\mathcal{K}$ с использованием оператора понижения доверия представлены в таблице 5.4.

Результаты вычислений показывают, что итоговое доверие субъекта $\mathcal{A}$ к субъекту $\mathcal{K}$ ниже, чем доверие субъекта $\mathcal{C}$ к субъекту $\mathcal{K}$. Это связано с наличием рисков, связанных с надёжностью центрального ЦПП, присоединённых УЦ и владельца $\text{СЕРТ}_{\text{ОК}}$. Например, надёжность ЦПП характеризуется частотой возникновения нештатных ситуаций (сбоев и отказов в работе) при функционировании компонентов и всей ИТС, а также вероятностью попыток персонала (сотрудников) самого ЦПП осуществить злонамеренные действия. Тоже самое относится и к функционированию УЦ, и, в частности, существует вероятность внешнего или внутреннего «давления» криминальных структур с целью принуждения сотрудников УЦ выпустить фальшивые $\text{СЕРТ}_{\text{ОК}}$.

Таблица 5.4 – Результаты понижения доверия для маршрута транзитивного доверия, представленного на рисунке 5.19

Параметры:		Входные мнения: $\omega_{\mathcal{B}}^{\mathcal{A}}$	$\omega_{\mathcal{C}}^{\mathcal{B}}$	$\omega_{\mathcal{K}}^{\mathcal{C}}$	Произведение: $\text{P}_{\mathcal{C}}^{\mathcal{A}}$	Вычисленное мнение: $\omega_{\mathcal{K}}^{[\mathcal{A};\mathcal{C}]}$
Вера/убеждённость:	b	0.9000	0.8500	0.8000		0.6766
Неверие:	d	0.0500	0.1000	0.2000		0.1677
Неопределённость:	u	0.0500	0.0500	0.0000		0.1557
Априорная вероятность:	a	0.9500	0.8000	0.3500		0.3500
Прогнозируемая вероятность:	P	0.9475	0.8900	0.8000	0.8433	0.7934

Владелец $СЕРТ_{ОК}$ также является источником риска, связанного со способностью самого владельца противостоять любым попыткам нарушителя получить НСД к ключевой информации и ПП владельца.

5.2.3 Усовершенствованная модель системы доверия на основе объединения КЗСУ (ИОК) ИТС

Создание системы доверия на основе объединения КЗСУ (ИОК) ИТС, образующих ИТИЦЭ, характеризуется следующими основными количественными показателями:

– около 100 аккредитованных УЦ, которые «разбросаны» по всей территории РФ, с учётом их принадлежности к ИТС и коммерческим организациям;

– в 2019 году на *Web*-портале «*Госуслуги*» было зарегистрировано более 100 млн. граждан РФ [173];

– отсутствуют ЦПП.

С эвристической точки зрения, это означает, что при переходе российской экономики «на цифровые рельсы» подавляющее большинство населения РФ будет пользоваться электронными услугами, включая проведение финансовых транзакций, заключение различных договоров, приобретение товаров в Интернет-магазинах и т.п. А с технологической точки зрения, это приведёт к существенному увеличению частоты транзакций в виртуальном (кибер-) пространстве (число транзакций за единицу времени) и, соответственно, увеличению нагрузки на ИТС, образующие в ИТИЦЭ.

Очевидно, что, исходя из указанных выше предположений, в модели, представленной на рисунке 5.17, единственный ЦПП будет, вероятнее всего, функционировать в состоянии «чрезмерной нагрузки», которое может перерасти в состояние «перегрузки» и далее – «блокировки», т.е. к нарушению работоспособности всей объединённой ИОК.

По этой причине, а также с эвристической точки зрения, необходимо заменить концепцию *единственного ЦПП* на *концепцию распределённого ЦПП*. Тогда модель объединённой системы доверия будет включать подсистему ЦПП (рисунок 5.21), состоящую из территориальных ЦПП (например, федерального, федеральных окружных, региональных и муниципальных уровней). В совокупности такие ЦПП образуют *единую иерархическую систему ЦПП* (ЕСЦПП). Распределённая ЕСЦПП станет *ядром системы доверия* на основе объединения КЗСУ (ИОК) ИТС, образующих ИТИЦЭ, и позволит эффективно сбалансировать (управлять) потоки(ами) данных с учётом временных поясов и географического размещения входящих в систему территориальных ЦПП.

5.3 Функционально-структурная модель системы доверия на основе объединения КЗСУ (ИОК) ИТС

Дальнейший этап разработки системы доверия на основе объединения КЗСУ (ИОК) ИТС, образующих ИТИЦЭ – это построение её функционально-структурной модели, в основе которой лежит усовершенствованная модель системы доверия на основе ЕСЦПП (архитектуры ЦПП). Функционально-структурная модель представлена на рисунке 5.22. А на рисунке 5.23 представлена географически распределённая модель ЕСЦПП в составе ЦПП федерального, федерального окружного, регионального и муниципального уровней, а также УЦ, вошедших в систему доверия на основе объединения КЗСУ (ИОК) ИТС, образующих ИТИЦЭ.

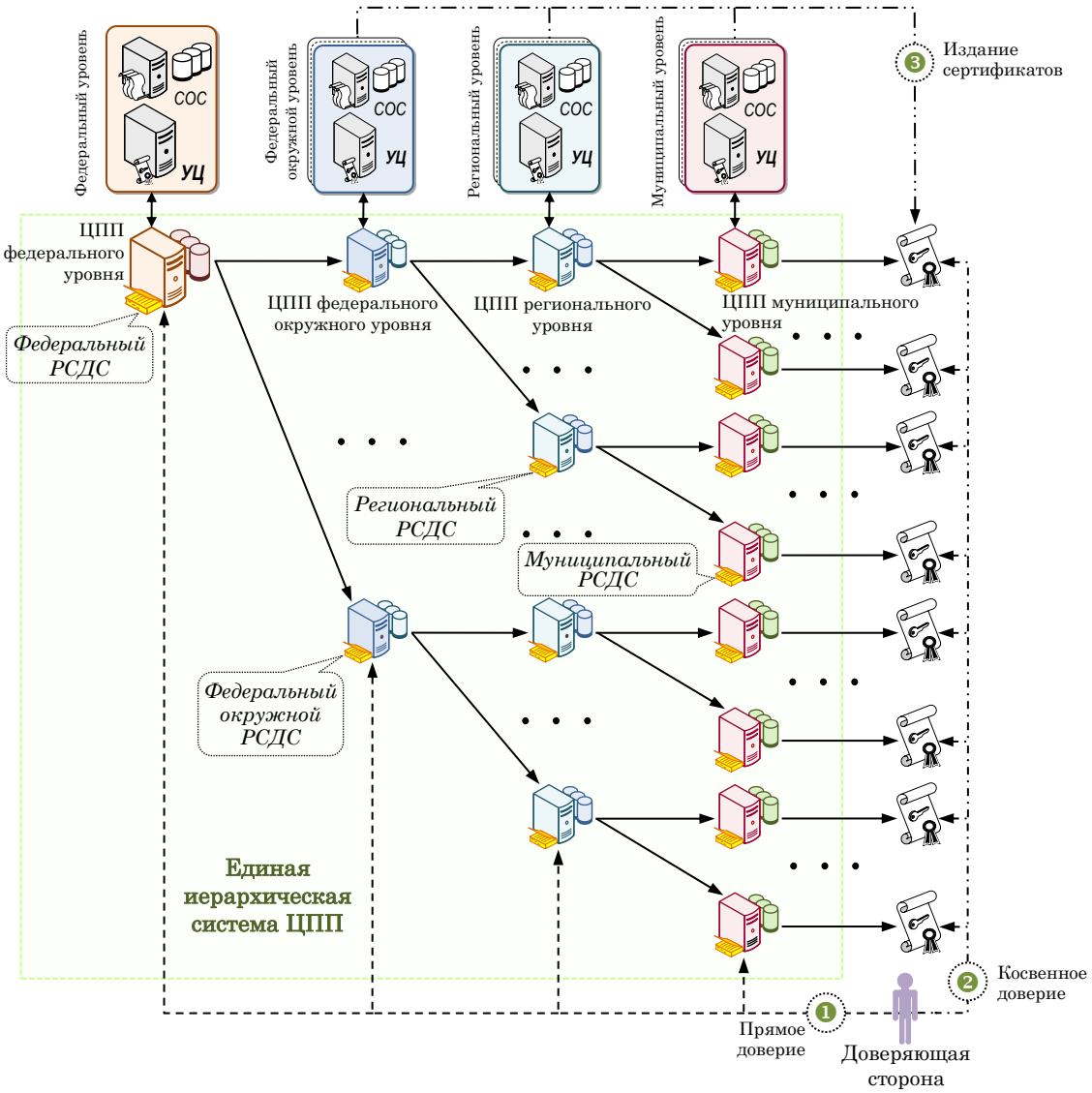

Рисунок 5.21 – Усовершенствованная модель системы доверия на основе объединения КЗСУ (ИОК) ИТС (ЕСЦПП)

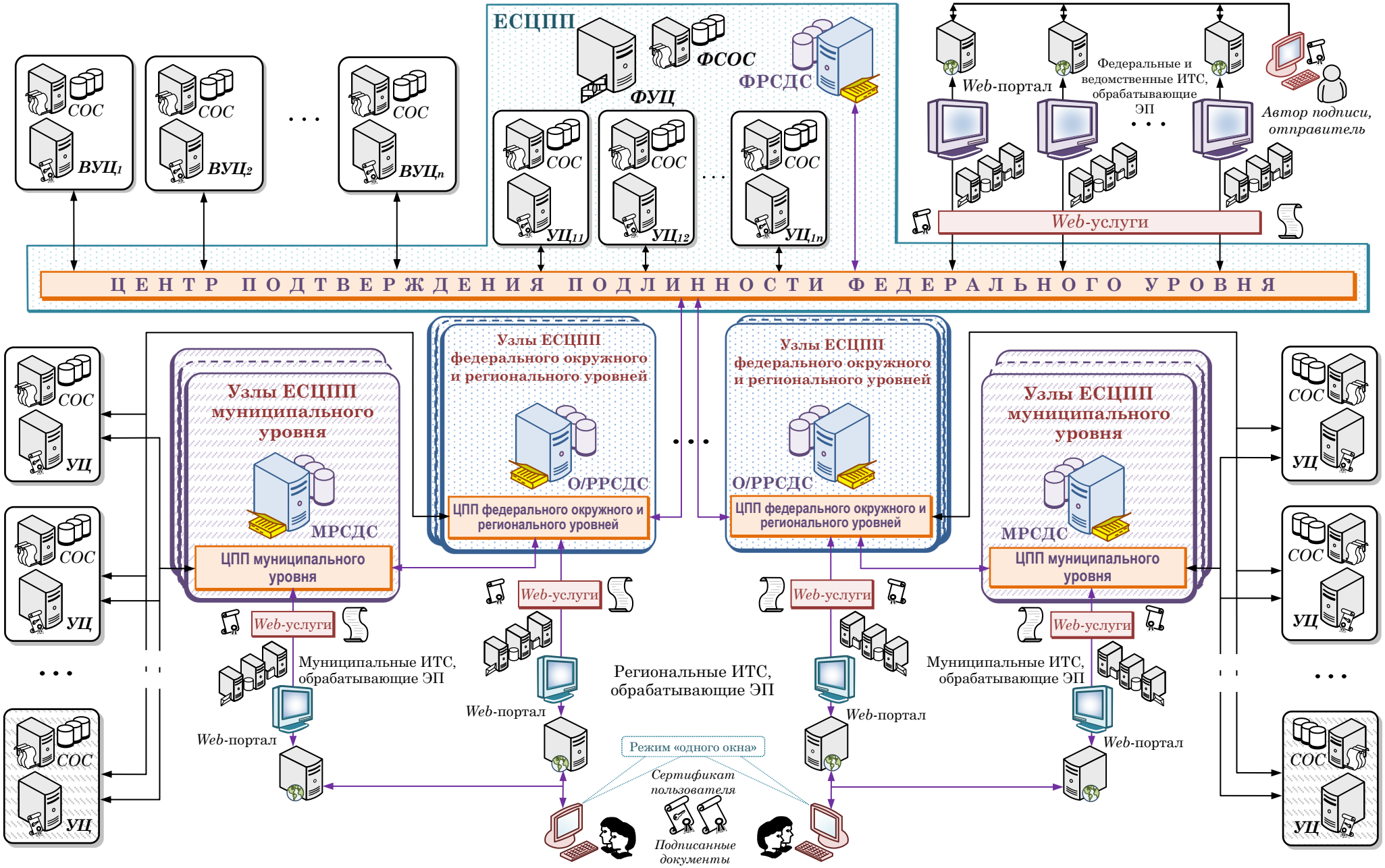

Рисунок 5.22 – Функционально-структурная модель системы доверия на основе объединения КЗСУ (ИОК) ИТС

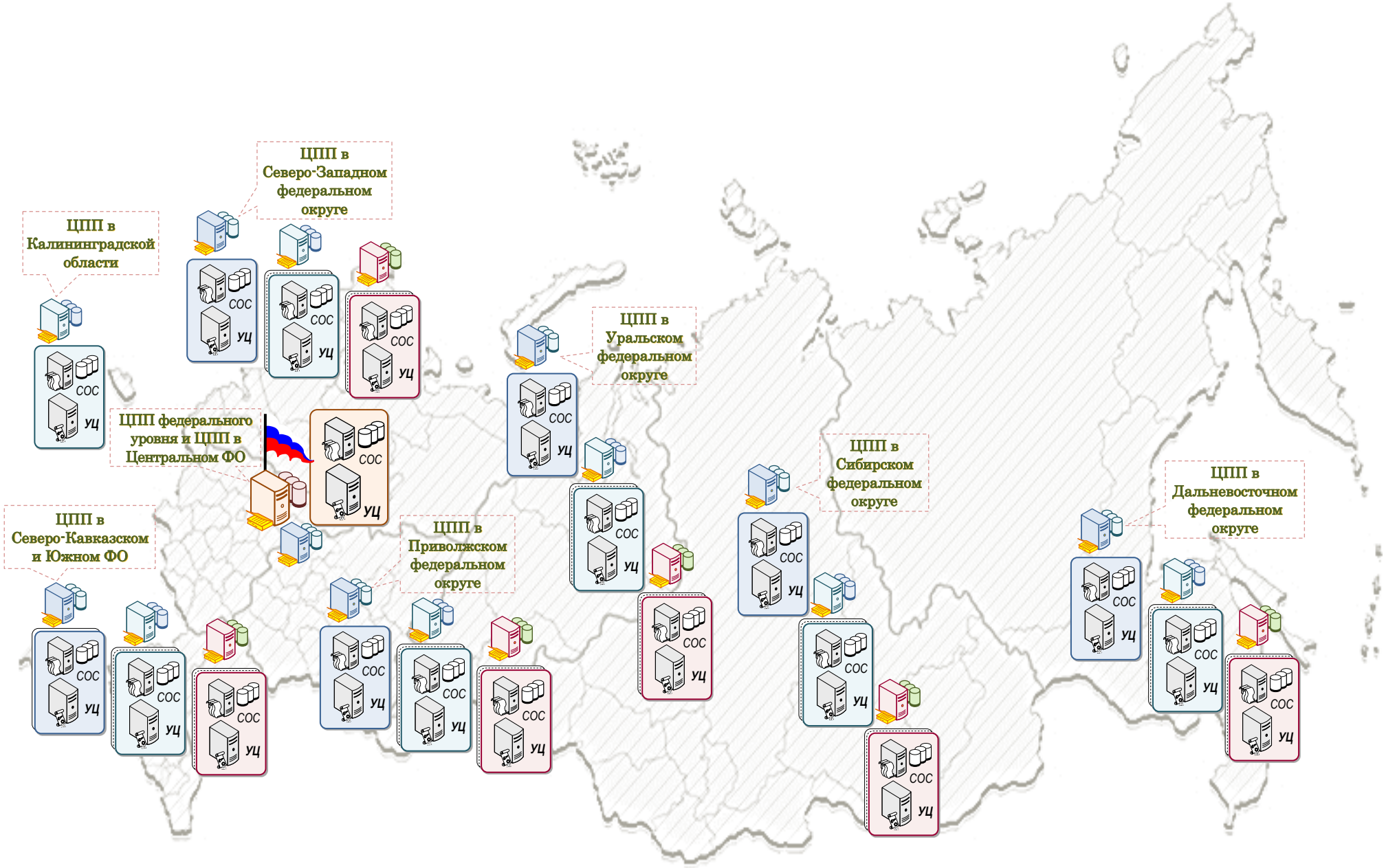

Рисунок 5.23 – Географически-распределённая модель ЕСЦПП (ядро системы доверия на основе объединения КЗСУ/ИОК)

Таким образом, в систему доверия на основе объединения КЗСУ (ИОК) ИТС входят (рисунок 5.22):

– ЦПП федерального уровня (ФЦПП), включающий УЦ федерального уровня (ФУЦ) и УЦ первого уровня и ПАК, обеспечивающий хранение, обслуживание и ведение РСДС федерального уровня (ФРСДС);

– ЦПП федерального окружного уровня (ОЦПП), которые включают ПАК, обеспечивающие в том числе хранение, обслуживание и ведение РСДС федерального окружного уровня (ОРСДС), и которые при необходимости могут включать УЦ федерального окружного уровня;

– ЦПП регионального уровня (РЦПП), которые включают ПАК, обеспечивающие хранение обслуживание и ведение РСДС регионального уровня (РРСДС), и которые при необходимости могут включать УЦ регионального уровня;

– ЦПП муниципального уровня (МЦПП), которые включают ПАК, обеспечивающие хранение обслуживание и ведение муниципальных РСДС (МРСДС), и которые при необходимости могут включать муниципальные УЦ (для обслуживания, например, муниципальных органов власти);

– Ведомственные (государственные) УЦ, которые взаимодействуют с ФЦПП;

– Коммерческие УЦ, вошедшие в состав системы доверия на основе объединения КЗСУ (ИОК) ИТС и взаимодействующие с ЕСЦПП на федеральном окружном, региональном и муниципальным уровнях;

– Ведомственные (государственные) и коммерческие ПЭУ, которые на договорных условиях подключены к ЕСЦПП;

– ИТС, обеспечивающие информационное взаимодействие:

= внутри ЕСЦПП;

= между ФЦПП и ведомственными (государственными) УЦ;

= между ЕСЦПП и коммерческими УЦ, вошедшими в состав объединённой системы доверия (КЗСУ);

= между НСЦПП и ПЭУ.

Главное требование к системе доверия на основе объединения КЗСУ (ИОК) ИТС – реализация следующих *основных функций*:

– предоставление (по запросу) услуг по *проверке ЭП* и *целостности* подписанного электронного документа;

– *подтверждение подлинности* (по запросу) предоставленного $СЕРТ_{ОК}$;

– *проверка обоснованности* выпуска $СЕРТ_{ОК}$ с целью защиты прав и свобод гражданина, на имя которого (без его согласия) мог быть издан фальсифицированный сертификат.

Метод проверки законности выпуска $СЕРТ_{ОК}$, реализуемый системой доверия на основе объединения КЗСУ (ИОК) ИТС, будет рассмотрен ниже.

5.3.1 ЦПП федерального уровня

Основные функции ФЦПП следующие:

– формирование (совершенствование) и контроль реализации политики применения объединённой ИОК, включающей формат и структуру РСДС, правила присоединения и подключения к ЕСЦПП, а также требований к ФУЦ и УЦ первого уровня;

– разработка требований к УЦ, присоединяемым к ЕСЦПП, и порядка их аккредитации, а также требований к форматам $СЕРТ_{ОК}$ и СОС;

– определение порядка информационного взаимодействия с ведомственными (государственными) УЦ и ПЭУ;

– ведение и обслуживание ФРСДС;

– разработка системы единой идентификации субъектов и объектов КЗСУ (ИОК), а также ведение, эксплуатация и обслуживание базы данных, содержащей объектные идентификаторы (*object identifier,* OID) всех участников и компонентов КЗСУ (ИОК);

– формирование и контроль реализации политики обеспечения ИБ функционирования системы доверия на основе объединения КЗСУ (ИОК) ИТС, и др.

5.3.2 ЦПП федерального окружного уровня

Основные функции федерального ОЦПП следующие:

– реализация и контроль выполнения политики применения системы доверия на основе объединения КЗСУ (ИОК) ИТС в федеральном округе;

– обеспечение информационного и технологического взаимодействия региональных ЦПП с ФЦПП и между собой;

– обеспечение информационного и технологического взаимодействия с УЦ и ПЭУ, подключённых к ЕСЦПП на федеральном окружном уровне;

– ведение и обслуживание ОРСДС;

– подготовка и заключение договоров с УЦ и ПЭУ на их подключение к ЕСЦПП на федеральном окружном уровне;

– участие в аккредитации УЦ, желающих подключиться к ЕСЦПП на федеральном окружном уровне;

– эксплуатация и сопровождение УЦ федерального окружного уровня.

5.3.3 ЦПП регионального уровня

Основные функции РЦПП следующие:

– реализация и контроль выполнения политики применения системы доверия на основе объединения КЗСУ (ИОК) ИТС в регионе;

– обеспечение информационного и технологического взаимодействия МЦПП с ОЦПП и между собой;

– обеспечение информационного и технологического взаимодействия с УЦ и ПЭУ, подключённых к ЕСЦПП на региональном уровне;

– ведение и обслуживание РРСДС;

– подготовка и заключение договоров с УЦ и ПЭУ на их подключение к ЕСЦПП на региональном уровне;

– участие в аккредитации УЦ, желающих подключиться к ЕСЦПП на региональном уровне;

– эксплуатация и сопровождение УЦ регионального уровня.

5.3.4 ЦПП муниципального уровня

Основные функции МЦПП следующие:

– реализация и контроль выполнения политики применения системой доверия на основе объединения КЗСУ (ИОК) ИТС в муниципальном образовании (муниципальном районе или городском округе);

– обеспечение информационного и технологического взаимодействия с РЦПП;

– обеспечение информационного и технологического взаимодействия с УЦ и ПЭУ, подключённых к ЕСЦПП на муниципальном уровне;

– ведение и обслуживание МРСДС;

– подготовка и заключение договоров с УЦ и ПЭУ на их подключение к ЕСЦПП на муниципальном уровне;

– участие в аккредитации УЦ, желающих подключиться к ЕСЦПП на муниципальном уровне;

– эксплуатация и сопровождение УЦ муниципального уровня.

5.4 Методы защиты пользователей ИОК

В §3.9 были рассмотрены основные проблемы и риски пользователей ИОК, которые требуют своего решения, так как переход экономики РФ на «цифровые рельсы» предусматри-

вает, в том числе, повышение благосостояния граждан, их доступности в электронным услугам и т.п., и, что немало важно, – одновременное обеспечение их защищённости в киберпространстве.

За последнее время участились случаи мошенничества в киберпространстве (обман пользователей в Интернет-сети [3,143…146]), направленные на противозаконное овладение имуществом и финансовыми средствами Интернет-пользователей. Наиболее изощрёнными способами «отъёма» имущества и денег граждан являются [200,201]:

1. *Незаконное издание фальсифицированных СЕРТ$_{ОК}$.* Наиболее вероятные причины такой деятельности: мошенническая (противоправная) деятельность сотрудников УЦ, или преступный сговор сотрудников УЦ с криминальными структурами, которые оказывают на них давление (шантажируют или угрожают физической расправой). Как показывает новейшая история, фальсифицированные СЕРТ$_{ОК}$ используются при проведении от имени «жертвы» интерактивных транзакций, связанных с продажей (приобретением) имущества, недвижимости (включая имущество и недвижимость, принадлежащие «жертве»), оплатой дорогостоящих покупок и т.п.;

2. *Создание и использование поддельных Web-сайтов* (ГАИС), которые дублируют подлинные ГАИС, принадлежащие конкретным законным ПЭУ, и тем самым вводят в заблуждение пользователей Интернет-сети. Злоумышленники, использующие поддельные *Web*-сайты, «выманивают» у пользователей их персональные данные, включая любую банковскую информацию, и в дальнейшем проводят незаконные финансовые операции от имени реальных владельцев банковских счетов. Кроме того, более изощрённой мошеннической деятельностью является продажа через поддельные *Web*-сайты железнодорожных или авиабилетов, билетов на различные культурно-спортивные мероприятия и туристических путёвок.

5.4.1 Противодействие изданию фальсифицированных СЕРТ$_{ОК}$

Система доверия на основе объединения КЗСУ (ИОК) ИТС должна выполнять *новую функцию*, которая ранее не была реализована ни в одной из известных моделей ИОК (§3.6 и §3.7). Этой функцией является *проверка законности выпуска СЕРТ$_{ОК}$* с целью защиты прав и свобод гражданина, на имя которого (без его согласия) может быть выпущен фальсифицированный сертификат (§5.3). В основе реализации этой функции лежит метод [200], который предусматривает участие специализированного государственного органа, регистрирующего заявку пользователя ИОК на получение СЕРТ$_{ОК}$.

В настоящее время в РФ государственные и муниципальные услуги предоставляются *многофункциональными центрами* «Мои документы» (МФЦ) [174,175]. В частности,

МФЦ используют защищённую БД, в которой хранятся персональные и иные данные о гражданах РФ. Следовательно, МФЦ могут выступать в роли органа регистрации заявлений граждан РФ на получение СЕРТ$_{ОК}$, а также последовательных номеров СЕРТ$_{ОК}$ (рисунок 3.9), которые были выпущены УЦ по указанным заявлениям. МФЦ могут получать подтверждения о выпуске затребованных гражданами сертификатов (с указанием их последовательных номеров) либо от самих граждан, либо от выпустивших такие сертификаты УЦ. Если УЦ попытается подтвердить выпуск не затребованного гражданином РФ (фальсифицированного) СЕРТ$_{ОК}$, то МФЦ ответит отказом, так как последний не регистрировал заявление гражданина РФ на получение такого СЕРТ$_{ОК}$. *Важным условием отправки подтверждения выпуска сертификата с его последовательным номером является своевременность*, т.е. интервал времени между получением сертификата его владельцем и получением МФЦ указанного подтверждения должен быть минимальным (и уточняется в МФЦ при подаче заявления гражданином РФ).

В этой связи, маршрут транзитивного доверия в форме ППОГ (рисунок 5.19) дополнится ещё одним субъектом $\mathcal{D}$ (МФЦ). Модифицированный маршрут транзитивного доверия отображается в сложную сеть доверия, которая представлена на рисунке 5.24.

Особенность полученной сложной сети доверия (рисунок 5.24) состоит в том, что она не отображается в форму ППОГ. Проведём анализ указанной сети доверия (рисунок 5.24). В этой сети представлены три возможных маршрута между субъектами $\mathcal{A}$ и $\mathcal{K}$, которые можно отобразить следующим образом:

$$\begin{aligned} \alpha_1 &= ([\mathcal{A};\mathcal{B}] : [\mathcal{B};\mathcal{C}] : [\mathcal{C},\mathcal{K}]), \\ \alpha_2 &= ([\mathcal{A};\mathcal{B}] : [\mathcal{B};\mathcal{D}] : [\mathcal{D},\mathcal{K}]), \\ \alpha_3 &= ([\mathcal{A};B] : [\mathcal{B};\mathcal{D}] : [\mathcal{D};\mathcal{C}] : [\mathcal{C},\mathcal{K}]). \end{aligned} \tag{5.12}$$

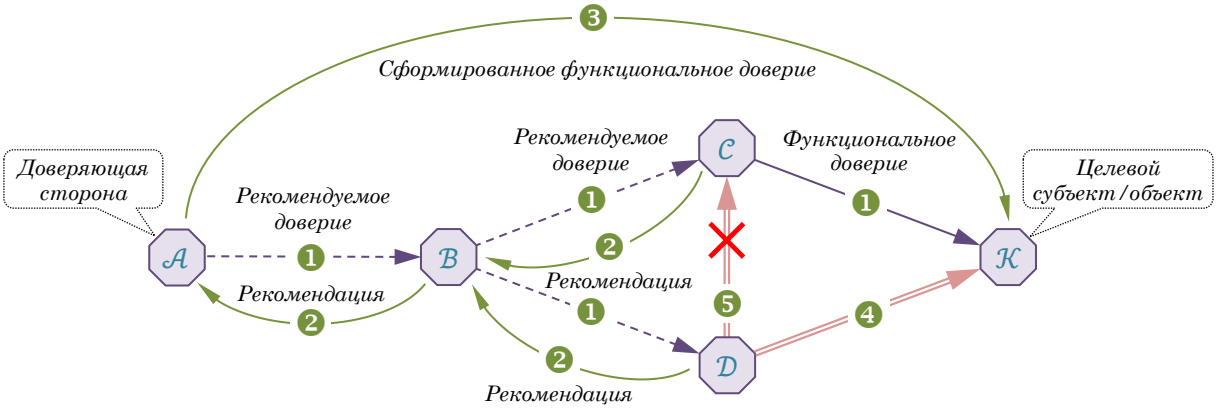

Рисунок 5.24 – Сложная сеть доверия, не отображаемая в форме ППОГ

Эти три маршрута позволяют сформировать, используя оператор слияния (§2.12.5), следующие семь возможных комбинаций/графов:

$$\begin{aligned} &\beta_1 = \alpha_1, && \beta_4 = \alpha_1 \diamond \alpha_2, && \beta_7 = \alpha_1 \diamond \alpha_2 \diamond \alpha_3. \\ &\beta_2 = \alpha_2, && \beta_5 = \alpha_1 \diamond \alpha_3, && \\ &\beta_3 = \alpha_3, && \beta_6 = \alpha_2 \diamond \alpha_3, && \end{aligned} \tag{5.13}$$

Равенство β_7 отображает сеть доверия, которая включает все возможные маршруты между субъектами $\mathcal{A}$ и $\mathcal{K}$. Проблема равенства β_7 состоит в том, что оно не является ППОГ, и поэтому не может быть представлено в форме стандартного выражения, в котором *каждое ребро участвует в формировании маршрута только один раз*. В этой сети доверия один маршрут следует удалить из графа с целью получения канонического выражения. Равенства β_4, β_5 и β_6 могут быть приведены к каноническому виду, равенства β_1, β_2 и β_3 уже являются каноническими, и это означает, что все равенства, за исключением равенства β_7, могут использоваться в качестве основы формирования ППОГ и для вычисления мнения/доверия субъекта $\mathcal{A}$ к субъекту (объекту) $\mathcal{K}$.

Необходимость удаления одного из маршрутов в сети доверия также подтверждается предназначением МФЦ (регистрация заявлений граждан РФ на получение $\text{СЕРТ}_{\text{ОК}}$), т.е. маршрут α_3 можно исключить из дальнейшего анализа, т.к. наличие ребра $[\mathcal{D}, \mathcal{K}]$ (индекс ❹, на рисунке 5.24) – *строго обязательно*. Тогда упростим равенства (5.12) и (5.13):

$$\begin{aligned} \alpha_1 &= ([\mathcal{A}; \mathcal{B}] : [\mathcal{B}; \mathcal{C}] : [\mathcal{C}, \mathcal{K}]), \\ \alpha_2 &= ([\mathcal{A}; \mathcal{B}] : [\mathcal{B}; \mathcal{D}] : [\mathcal{D}, \mathcal{K}]) \ . \end{aligned} \tag{5.14}$$

$$\beta_1 = \alpha_1, \qquad \beta_2 = \alpha_2, \qquad \beta_3 = \alpha_1 \diamond \alpha_2 \ . \tag{5.15}$$

Упрощённые равенства указывают на то, что ребро $[\mathcal{D}, \mathcal{C}]$ (индекс ❺, на рисунке 5.24) должно быть удалено. Наличие ребра $[\mathcal{D}, \mathcal{C}]$ в сети доверия (рисунок 5.24) означает, что УЦ (субъект $\mathcal{C}$) предоставляет МФЦ подтверждение о выпуске запрошенного гражданином РФ $\text{СЕРТ}_{\text{ОК}}$ вместе с его последовательным номером. Очевидно, что если в сети доверия будет отсутствовать ребро $[\mathcal{D}, \mathcal{K}]$, то наличие ребра $[\mathcal{D}, \mathcal{C}]$ – просто бессмысленно, т.е. злонамеренный УЦ пытается ввести в заблуждение МФЦ.

Таким образом, два маршрута доверия α_1 и α_2 решают две разные, но чрезвычайно важные задачи:

i. α_1 – обеспечивает подтверждение подлинности $\text{СЕРТ}_{\text{ОК}}$;

ii. α_2 – обеспечивает доказательство, что $\text{СЕРТ}_{\text{ОК}}$ – не фальсифицированный.

На рисунке 5.25 представлен пример формирования доверия ПЭУ ($\mathcal{A}$) к подлинности и законности выпуска $\text{СЕРТ}_{\text{ОК}}$ ($\mathcal{K}$), изданному УЦ ($\mathcal{C}$), через ЦПП ($\mathcal{B}$) и МФЦ ($\mathcal{D}$). В данном

примере предполагается, что пользователь ($\mathcal{K}$) заранее обратился в МФЦ и зарегистрировал своё заявление на выпуск СЕРТ$_{ОК}$ в рекомендованном или известном пользователю, либо предложенном МФЦ УЦ. Также предполагается, что после процедуры регистрации в УЦ и по получении СЕРТ$_{ОК}$ пользователь предоставил в МФЦ полученный СЕРТ$_{ОК}$ и его последовательный номер.

Рассмотрим алгоритм процедуры формирования доверия ПЭУ ($\mathcal{A}$) к подлинности и законности выпуска СЕРТ$_{ОК}$ пользователя ($\mathcal{K}$) на примере рисунка 5.25:

❶ пользователь ($\mathcal{K}$) подписывает документы и направляет их вместе со своим СЕРТ$_{ОК}$ на *Web*-портал закупок, т.е. ПЭУ ($\mathcal{A}$);

❷ ПЭУ ($\mathcal{A}$) запрашивает ЦПП ($\mathcal{B}$) с целью подтверждения подлинности и законности выпуска СЕРТ$_{ОК}$ пользователя ($\mathcal{K}$) и направляет ему СЕРТ$_{ОК}$;

❸ ЦПП ($\mathcal{B}$) проверяет подлинность СЕРТ$_{ОК}$ пользователя ($\mathcal{K}$) с помощью конкретного УЦ ($\mathcal{C}$);

❹ ЦПП ($\mathcal{B}$) передаёт МФЦ ($\mathcal{D}$) СЕРТ$_{ОК}$ пользователя ($\mathcal{K}$) для проверки законности его издания;

❺ УЦ ($\mathcal{C}$) передаёт ЦПП ($\mathcal{B}$) результат проверки СЕРТ$_{ОК}$ пользователя ($\mathcal{K}$);

❻ МФЦ ($\mathcal{D}$) передаёт ЦПП ($\mathcal{B}$) результат проверки СЕРТ$_{ОК}$ пользователя ($\mathcal{K}$);

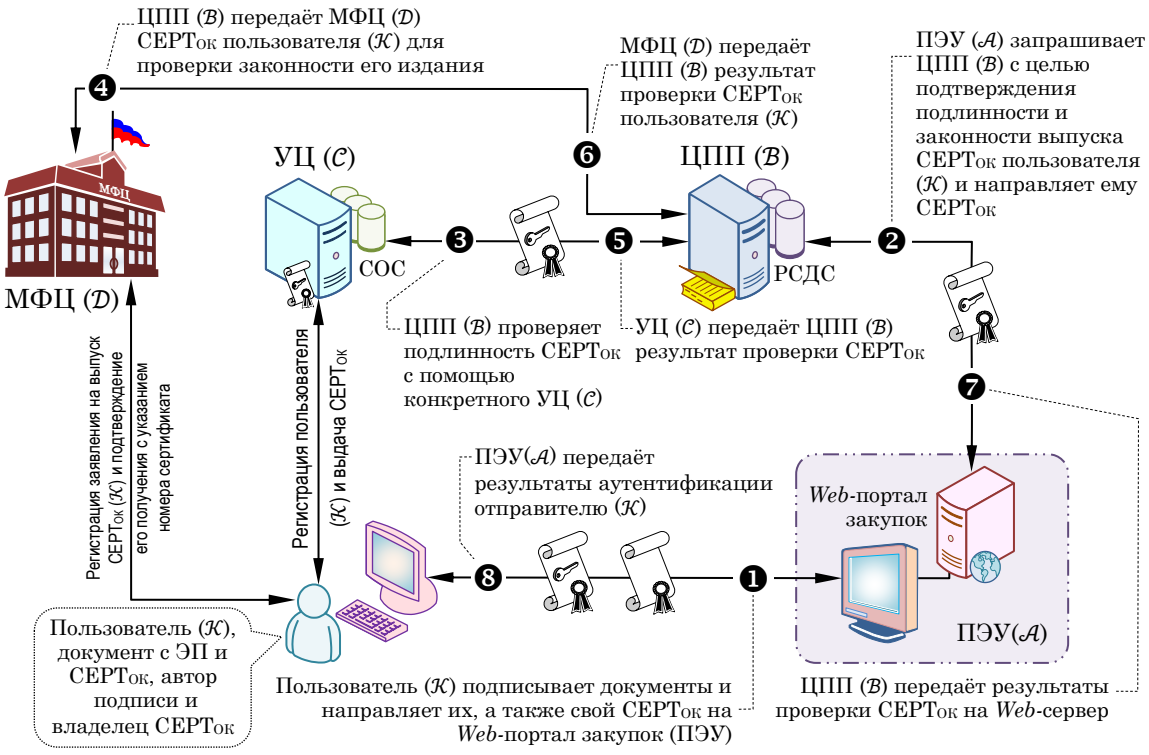

Рисунок 5.25 – Пример формирования доверия ПЭУ ($\mathcal{A}$) к подлинности и законности выпуска СЕРТ$_{ОК}$ ($\mathcal{K}$), изданного УЦ ($\mathcal{C}$), через ЦПП ($\mathcal{B}$) и МФЦ ($\mathcal{D}$)

❼ ЦПП ($\mathcal{B}$) передаёт результаты проверки СЕРТ$_{ОК}$ на *Web*-сервер, т.е. ПЭУ ($\mathcal{A}$);

❽ ПЭУ ($\mathcal{A}$) передаёт результаты аутентификации (подтверждения подлинности и законности издания СЕРТ$_{ОК}$) пользователю ($\mathcal{K}$).

Очевидно, что в случае отрицательного результата подтверждения подлинности и/или проверки законности издания СЕРТ$_{ОК}$, ПЭУ откажет пользователю в проведении транзакции. А это означает, что ПЭУ предотвратит попытку злоумышленника провести мошенническую транзакцию с использованием фальсифицированного СЕРТ$_{ОК}$.

5.4.2 Распознавание поддельных (мошеннических) Web-сайтов

В основе распознавания поддельных (мошеннических) *Web*-сайтов лежит метод [201], который реализует проверку и подтверждение подлинности СЕРТ$_{ОК}$ ПЭУ со стороны пользователя. Указанный метод предусматривает использование пользователем специализированного КПО, установленного в его компьютер или смартфон, т.е. КПО осуществляет по команде пользователя процедуры проверки и подтверждения подлинности СЕРТ$_{ОК}$ ПЭУ.

В реальных условиях возможны два варианта обнаружения мошеннических *Web*-сайтов, которые определяются тем, какой СЕРТ$_{ОК}$ ПЭУ использует злоумышленник, а именно:

(а) злоумышленник (злонамеренный ПЭУ) устраивает «маскарад», управляя поддельным *Web*-сайтом, и *использует украденный СЕРТ$_{ОК}$*♦, принадлежащий законному ПЭУ, *Web*-портал которого имитирует злоумышленник;

(б) злоумышленник (злонамеренный ПЭУ) устраивает «маскарад», управляя поддельным *Web*-сайтом, который имитирует *Web*-портал, принадлежащий законному ПЭУ, но при этом, злоумышленник *использует свой собственный СЕРТ$_{ОК}$*, полученный электронным способом в зарубежном УЦ. Было бы невообразимо полагать, что злоумышленник получит собственный СЕРТ$_{ОК}$ в российском УЦ, так как его персональные данные или данные его организации (например, ИНН, наименование и т.п.) были бы отражены в СЕРТ$_{ОК}$. А это – фактическое раскрытие злоумышленника. Вероятнее всего, злоумышленник получит СЕРТ$_{ОК}$ в зарубежном ЦС, а сам СЕРТ$_{ОК}$ не будет отражён в репозитарии российской ИОК, другими словами, подтвердить его подлинность на территории РФ не представляется возможным вследствие отсутствия трансграничного взаимодействия отечественной ИОК с ИОК других государств.

♦ Потенциальной угрозой для безопасности самого сертификата является угроза, при которой нарушитель выдаёт себя за истинного владельца сертификата, который указан в этом СЕРТ$_{ОК}$. Такое несанкционированное использование сертификата называется *кражей сертификата* [92,110].

5.4.2.1 Распознавание украденного СЕРТ$_{ОК}$

Распознавание украденного СЕРТ$_{ОК}$ осуществляется в автоматическом режиме специализированным КПО по команде пользователя, и предполагает проведение процедуры аутентификации поддельного *Web*-сайта (рисунок 5.26), включающей, как минимум, следующие четыре итерации [92,95]:

❶ пользователь инициализирует работу своего специализированного КПО, который направляет сообщение *Web*-серверу, содержащее запрос СЕРТ$_{ОК}$ владельца *Web*-сайта;

❷ *Web*-сервер направляет специализированному КПО ответное сообщение, содержащее СЕРТ$_{ОК}$ владельца *Web*-сайта;

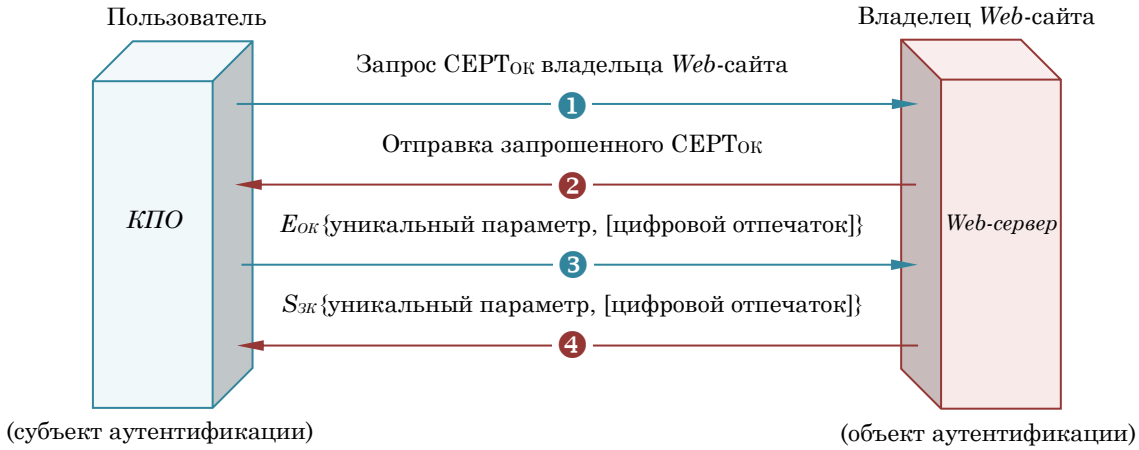

Рисунок 5.26 – Процедура аутентификации владельца *Web*-сайта с целью распознавания кражи СЕРТ$_{ОК}$

❸ специализированный КПО пользователя направляет *Web*-серверу зашифрованное с помощью открытого ключа владельца *Web*-сайта сообщение $E_{ОК}\{...\}$, содержащее уникальный параметр, цифровой отпечаток уникального параметра и алгоритм вычисления цифрового отпечатка, а также запрос на отправку ответного сообщения, которое должно содержать уникальный параметр и должно быть подписано с помощью закрытого ключа владельца *Web*-сайта $S_{ЗК}\{...\}$;

❹ *Web*-сервер направляет специализированному КПО пользователя ответное подписанное с помощью закрытого ключа владельца *Web*-сайта сообщение $S_{ЗК}\{...\}$, содержащее уникальный параметр.

Получив указанное подписанное сообщение, специализированный КПО пользователя проверяет подпись (целостность сообщения и авторство ЭП). Если проверка завершилась положительно, то пользователь переходит к проведению интерактивной транзакции с *Web*-сервером. Если же – отрицательно, то пользователь разрывает виртуальное соединение.

Последнее означает, что пользователь предотвратит попытку поддельного *Web*-сайта (сервера) провести с ним мошенническую транзакцию с использованием украденного $\text{СЕРТ}_{\text{ОК}}$.

5.4.2.2 Распознавание $\text{СЕРТ}_{\text{ОК}}$, принадлежащего владельцу Web-сайта

Распознавание $\text{СЕРТ}_{\text{ОК}}$, принадлежащего владельцу *Web*-сайта (ПЭУ), основано на построении сети субъективного доверия, аналогичной той, которая представлена на рисунке 5.24. Основное отличие состоит в том, что пользователь (доверенная сторона) и ПЭУ (доверяющая сторона) поменялись местами, т.е. пользователь – субъект $\mathcal{A}$ (доверяющая сторона), а ПЭУ – субъект $\mathcal{K}$ (его $\text{СЕРТ}_{\text{ОК}}$, доверенная сторона).

На рисунке 5.27 представлена сеть доверия, которая отображается в ППОГ, между пользователем ($\mathcal{A}$) и ПЭУ ($\mathcal{K}$).

Проведём анализ сети доверия, изображённой на рисунке 5.27. В этой сети представлены два возможных маршрута между субъектами $\mathcal{A}$ и $\mathcal{K}$, которые можно отобразить следующим образом:

$$\alpha_1 = ([\mathcal{A};\mathcal{B}] : [\mathcal{B};\mathcal{C}] : [\mathcal{C},\mathcal{K}]), \quad \alpha_2 = ([\mathcal{A};\mathcal{B}] : [\mathcal{B},\mathcal{K}]) . \tag{5.16}$$

Эти два маршрута позволяют сформировать, используя оператор слияния (§1.12.5), следующие три возможных комбинаций/графа:

$$\beta_1 = \alpha_1, \qquad \beta_2 = \alpha_2, \qquad \beta_3 = \alpha_1 \diamond \alpha_2 \ . \tag{5.17}$$

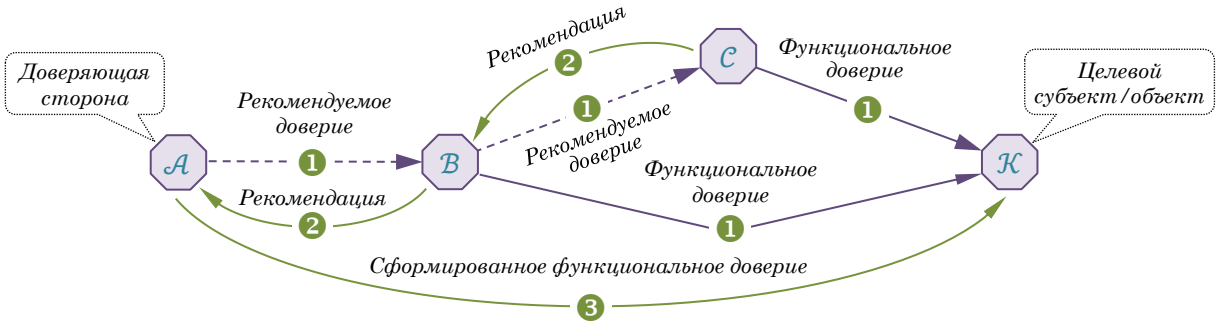

Рисунок 5.27 – Сеть доверия, отображаемая в форме ППОГ, между пользователем ($\mathcal{A}$, исток/источник) и ПЭУ ($\mathcal{K}$, сток)

Равенство β_3 отображает сеть доверия, которая включает все возможные маршруты между субъектами $\mathcal{A}$ и $\mathcal{K}$, и является ППОГ. Следовательно, β_3 может быть представлено в форме стандартного выражения, в котором *каждое ребро участвует в формировании маршрута доверия только один раз.*

Таким образом, два маршрута доверия α_1 и α_2 решают две разные, но чрезвычайно важные задачи в интересах пользователя ($\mathcal{A}$):

i. α_1 – обеспечивает подтверждение подлинности СЕРТ$_{ОК}$ ПЭУ, если указанный сертификат был выпущен российским УЦ, внесённым в РСДС;

ii. α_2 – обеспечивает доказательство надёжности ПЭУ, так как он должен быть указан в РСДС.

На рисунке 5.27 представлен пример формирования доверия пользователя ($\mathcal{A}$) к подлинности СЕРТ$_{ОК}$ ПЭУ ($\mathcal{K}$), изданному УЦ ($\mathcal{C}$), и надёжности самого ПЭУ ($\mathcal{K}$) через ЦПП ($\mathcal{B}$). В данном примере предполагается, что ПЭУ получил СЕРТ$_{ОК}$ в УЦ, аккредитованном и зарегистрированном в РСДС, и был сам аккредитован и зарегистрирован в РСДС в качестве субъекта экономической деятельности (возможно с привлечением ФНС РФ).

Рассмотрим алгоритм процедуры формирования доверия пользователя ($\mathcal{A}$) к подлинности СЕРТ$_{ОК}$ ПЭУ ($\mathcal{K}$)), изданного УЦ ($\mathcal{C}$), и надёжности самого ПЭУ ($\mathcal{K}$) через ЦПП ($\mathcal{B}$) на примере рисунка 5.28:

❶ пользователь ($\mathcal{A}$) получает СЕРТ$_{ОК}$ от ПЭУ ($\mathcal{K}$);

❷ пользователь ($\mathcal{A}$) запрашивает ЦПП ($\mathcal{B}$) с целью подтверждения подлинности СЕРТ$_{ОК}$ ПЭУ ($\mathcal{K}$), изданного УЦ ($\mathcal{C}$), и надёжности самого ПЭУ ($\mathcal{K}$) и направляет ему СЕРТ$_{ОК}$;

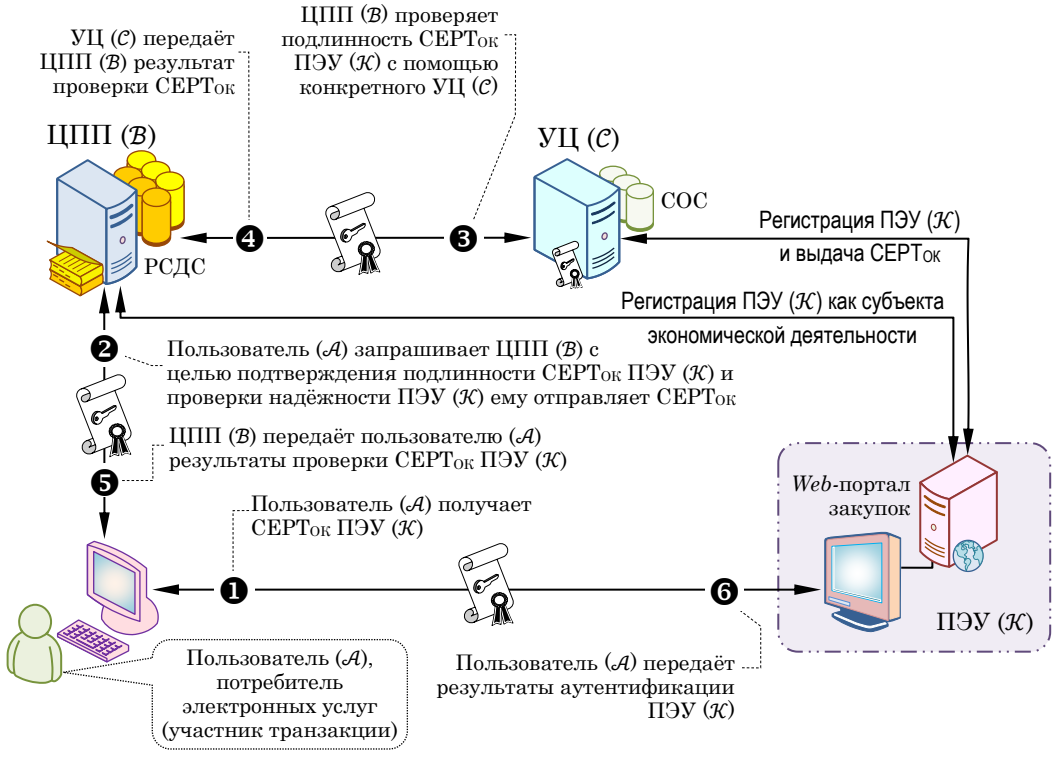

Рисунок 5.28 – Пример формирования доверия пользователя ($\mathcal{A}$) к подлинности СЕРТ$_{ОК}$ ПЭУ ($\mathcal{K}$), изданного УЦ ($\mathcal{C}$), и надёжности самого ПЭУ ($\mathcal{K}$) через ЦПП ($\mathcal{B}$)

❸ ЦПП ($\mathcal{B}$) проверяет подлинность СЕРТ$_{ОК}$ ПЭУ ($\mathcal{K}$) с помощью конкретного УЦ ($\mathcal{C}$), используя РСДС. ЦПП ($\mathcal{B}$) проверяет надёжность ПЭУ ($\mathcal{K}$), т.е. его наличие в РСДС в качестве

субъекта экономической деятельности. Следует заметить, что РСДС, в части субъектов экономической деятельности, может формироваться с участием ФНС РФ

❹ УЦ ($\mathcal{C}$) передаёт ЦПП ($\mathcal{B}$) результат проверки $СЕРТ_{ОК}$ ПЭУ ($\mathcal{K}$);

❺ ЦПП ($\mathcal{B}$) передаёт результаты проверки $СЕРТ_{ОК}$ ПЭУ ($\mathcal{K}$) пользователю ($\mathcal{A}$);

❻ пользователь ($\mathcal{A}$) передаёт результаты аутентификации (подтверждения подлинности $СЕРТ_{ОК}$) ПЭУ ($\mathcal{K}$).

Очевидно, что пользователь в случае получения отрицательного результата подтверждения подлинности $СЕРТ_{ОК}$ ПЭУ и/или проверки надёжности самого ПЭУ разорвёт виртуальное соединение с ПЭУ. А это означает, что пользователь предотвратит попытку «злонамеренного» (ненадёжного) *Web*-сайта (сервера) провести с ним мошенническую транзакцию.

5.5 Использование IPv6-адресов в качестве национальных (глобальных) ПП

Далее рассматривается метод, основанный на совместном использовании свойств IPv6-протокола [150,151] и положений стандарта Международной организации по стандартизации ISO 3166 [149]. Реализация данного способа позволит решить проблему глобальных ПП провайдеров электронных услуг и Интернет-пользователей (физических лиц и организаций), и существенно снизить остроту проблемы обеспечения безопасности ИТИЦЭ РФ. А при условии неотвратимости наказания за киберпреступления, в перспективе, можно решить проблему обеспечения ИБ государства и всего мирового сообщества. Однако, главным условием достижения победы над киберпреступностью является политическая воля мировых держав и принятие соответствующих международных актов и стандартов.

5.5.1 Свойства логической характеристики IPv6-протокола

При описании любого сетевого протокола принято выделять его логическую и процедурную характеристики [37,134]. Логическая характеристика протокола – структура (формат) и содержание (семантика) сообщений. Логическая характеристика задаётся перечислением типов сообщений и их смысла. Правила выполнения действий, предписанных протоколом взаимодействия, называются процедурной характеристикой протокола.

В связи со стремительным ростом числа пользователей и географическим расширением Интернет-сети стала проявляться нехватка IPv4-адресов, которая могла бы стать тормозом развития сети и, в конечном счёте, глобальной информатизации. По этой причине в конце 90-х годов прошлого века была предложена 16-байтовая система IPv6-адресации. Формат IPv6-пакета определяет длину IPv6-адресов, равную 128 битам. Таким образом, общая ёмкость IPv6-адресного пространства составляет: $2^{128} \approx 10^{39}$. Это число IPv6-адресов во много раз превышает численность населения Земли.

Одной из главных особенностей логической характеристики IPv6-протокола является формат кодирования глобального (общесетевого) однонаправленного (*unicast*) IPv6-адреса, который представлен на рисунке 5.29. Из этого рисунка видно, что одним из полей глобального адреса является «*префикс глобальной маршрутизации*» (обычно имеет иерархическую структуру), который присваивается группе подсетей (линий связи). Далее идёт поле «*идентификатор подсети*», в котором указывается идентификатор, присвоенный линии связи в рамках этой группы подсетей. Третье поле глобального адреса «*идентификатор интерфейса*» имеет фиксированную длину 64 бита (то есть, $n + m = 64$). В дальнейшем при рассмотрении предлагаемого способа повышения уровня защищённости национальных ИТИ будет использоваться «*префикс глобальной маршрутизации*».

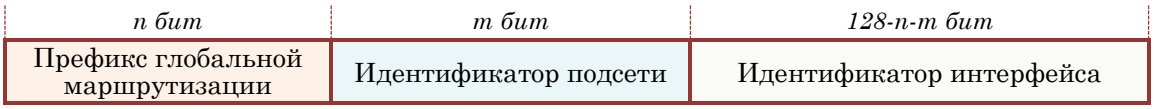

Рисунок 5.29 – Общий формат глобального однонаправленного IPv6-адреса

5.5.2 Международный стандарт ISO 3166

Международная организация по стандартизации (ISO) приняла в 1974 году первую версию Международного стандарта ISO 3166 [149]. ISO 3166 является международным стандартом кодов стран и единиц их административно-территориального деления. Его цель – установление признанных в международном масштабе кодов для указания наименований стран, территорий или мест, представляющих географический интерес, а также единиц их административно-территориального деления. Однако ISO 3166 устанавливает не наименования стран, а только их коды.

Наименования стран в ISO 3166 взяты из источников ООН. Новые наименования и коды добавляются автоматически, когда ООН публикует новые наименования в Терминологическом бюллетене наименований стран или в Кодах стран и регионов для статистического использования, которые ведут статистические отделы ООН.

В 2020 году стандарт ISO 3166 был расширен. В соответствие с этим стандартом каждая страна имеет цифровое обозначение, состоящее из трёх цифр, например, Россия – 643, США – 840, Великобритания – 826, Франция – 250.

5.5.3 Структура данных для информационного обеспечения Интернет-сети

В соответствии с Рекомендациями ITU-T• X.500 [97], любой объект реального мира может описываться несколькими классами с присвоенными этим классам атрибутами, за которыми закрепляются взаимно-однозначные уникальные идентификаторы OID и имена. Каждый класс объектов содержит определённый набор атрибутов. Порядок идентификации объектов определён международным стандартом ISO/IEC 9834-1 [176] и Рекомендацией ITU-T X.660 [177].

Все значения объектных идентификаторов имеют, по крайней мере, два субидентификатора (цифровых маркера, разделённых точкой). Значение первого субидентификатора определяет одно из следующих «известных» наименований:

(a) «0» – ITU-T;

(b) «1» – ISO;

(c) «2» – ISO/ITU-T (совместные стандарты).

Международное Интернет-сообщество поддержало указанное положение о стандартизации при построении целевых прикладных информационно-технологических систем с применением классов объектов и атрибутов, использующих объектные идентификаторы.

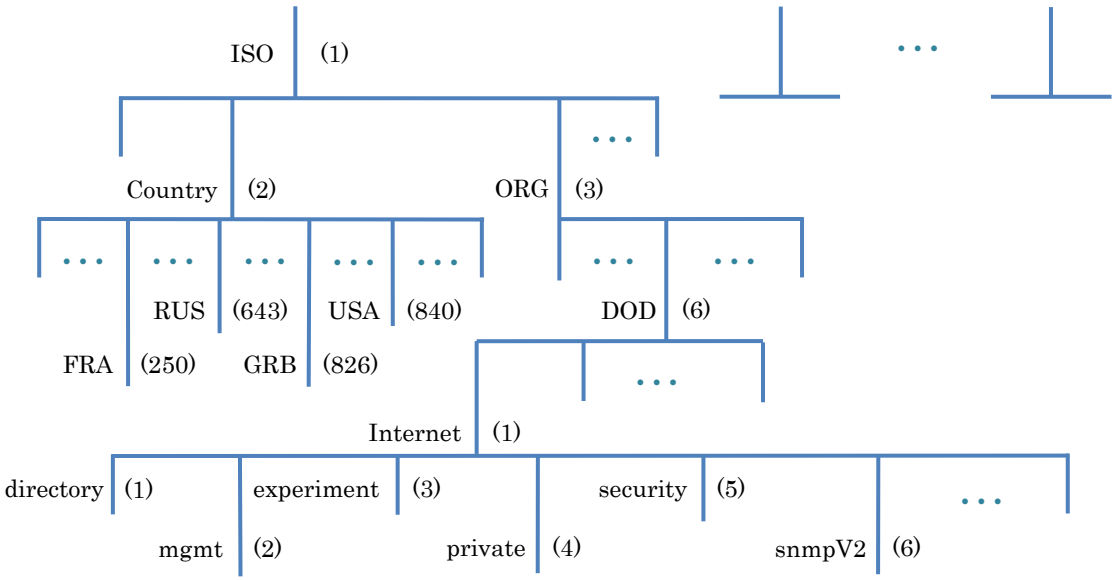

Рисунок 5.30 – Корневое дерево иерархии данных для информационного обеспечения Интернет-сети, включая объектные идентификаторы стран

• Телекоммуникационный сектор стандартизации Международного союза электросвязи (Telecommunication Standardization Sector of International Telecommunication Union) — специализированный орган ООН, с 1993 года преемник Международного Консультативного Комитета по Телеграфии и Телефонии (Comite Consultatif International Telegraphique et Telephonique) — международная организация, разрабатывающая стандарты в области связи.

Высшим уровнем иерархии (рисунок 5.30) для данных информационного обеспечения Интернет-сети является Международная организация по стандартизации, имеющая кодировку «1» («iso» = 1). Одной из ветвей корневого дерева иерархии данных общего назначения является (рисунок 5.30) ветвь объектных идентификаторов стран, которая имеет вид:

```
country     OBJECT IDENTIFIER ::= { iso 2 }  --  «iso» = 1
RUS         OBJECT IDENTIFIER ::= { country 643 }
USA         OBJECT IDENTIFIER ::= { country 840 }
GRB         OBJECT IDENTIFIER ::= { country 826 }
FRA         OBJECT IDENTIFIER ::= { country 250 } .
```

Таким образом, каждое государство (страна), фактически имеет свой объектный идентификатор, кодируемый как последовательность цифровых маркеров:

– 1 (ISO). 2 (страны). 643 (Российская Федерация). ... ;

– 1 (ISO). 2 (страны). 840 (США). ... ;

– 1 (ISO). 2 (страны). 826 (Великобритания). ... ;

– 1 (ISO). 2 (страны). 250 (Франция). ... .

Другими словами, любая трёхмаркерная последовательность вида «1.2. ... .» определяет государственную принадлежность сетевого объекта.

5.5.4 Описание метода

На основе предыдущего анализа, предлагается использовать объектные идентификаторы стран (например, 1.2.643, идентификатор России) в качестве «*префикса глобальной маршрутизации*» в IPv6-адресах. Таким образом, весь диапазон IPv6-адресов будет разделён на три больших поддиапазона:

1. Национальные поддиапазоны IPv6-адресов государств;

2. Поддиапазон специальных адресов, в который также входят локальные, групповые и все иные технологические IPv6-адреса;

3. Не используемые (запрещённые для использования) IPv6-адреса (решение об их использовании должно приниматься международной организацией и публиковаться в открытом доступе).

Примером такого глобального деления могут служить коды стран, используемые в системах фиксированной и мобильной телефонной связи (например, «+7» – Россия; «+1» – США; «+44» – Великобритания; «+33» – Франция и др.).

В шестнадцатеричном (двоичном) коде Российский диапазон IPv6-адресов будет иметь вид [147]:

1264:3000::/20 (0001 0010 0110 0100 0011 0000 0000 0000 ...) .

Диапазон IPv6-адресов США будет иметь вид:

1284::/20 (0001 0010 1000 0100 0000 0000 0000 0000 ...) .

Диапазон IPv6-адресов Великобритании (Соединённого Королевства Великобритании и Северной Ирландии) будет иметь вид:

1282:6000::/20 (0001 0010 1000 0010 0110 0000 0000 0000 ...) .

Диапазон IPv6-адресов Франции будет иметь вид:

1225::/20 (0001 0010 0010 0101 0000 0000 0000 0000 ...) .

5.5.5 Противоречие с положениями стандартов RFC-3587 и RFC-4291

Очевидно, что любой префикс глобальной маршрутизации всегда будет начинаться с октета «00010010». Однако, ввиду того, что префикс глобальной маршрутизации начинается с последовательности «000», то возникает противоречие со стандартами RFC-3587 [178] и RFC-4291 [150]. В RFC-4291 в частности говорится, что глобальные однонаправленные IPv6-адреса, которые начинаются с нулевой последовательности «000», имеют другую конструкцию и формат, отличные от тех, которые представлены на рисунке 5.29.

В таком случае, префикс глобальной маршрутизации может начинаться с любой другой последовательности их трёх бит кроме «000». С практической точки зрения это может быть одна из следующих восьми последовательностей «100», «110», «111», «011», «001», «101», «010», «101». Тогда в шестнадцатеричном (двоичном) коде Российский диапазон IPv6-адресов будет следующий:

(2 ... f)264:3000::/20 ([0010 … 1111] 0010 0110 0100 0011 0000 0000 0000 ...) .

Диапазон IPv6-адресов США будет иметь вид:

(2 ... f)284::/20 ([0010 … 1111] 0010 1000 0100 0000 0000 0000 0000 ...) .

Диапазон IPv6-адресов Великобритании (Соединённого Королевства Великобритании и Северной Ирландии) будет иметь вид:

(2 ... f)282:6000::/20 ([0010 … 1111] 0010 1000 0010 0110 0000 0000 0000 ...) .

Диапазон IPv6-адресов Франции будет иметь вид:

(2 ... f)225::/20 ([0010 … 1111] 0010 0010 0101 0000 0000 0000 0000 ...) .

Выбор конкретного вида кодирования первых четырёх бит префикса глобальной маршрутизации может быть осуществлён соответствующим органом по стандартизации в рамках Интернет-сообщества.

5.5.6 Расширение предлагаемого метода на локальные IPv6-адреса

Локальные IPv6-адреса используются в пределах одной линии связи. На рисунке 5.31 представлен формат однонаправленного IPv6-адреса для локальной линии связи.

10 бит	*54 бита*	*64 бита*
1111111010	0	Идентификатор интерфейса

Рисунок 5.31 – Формат однонаправленного IPv6-адреса для локальной линии связи

Данные адреса предназначены для обозначения интерфейсов в рамках одного канала (линии) связи в следующих целях:

1. Автоматическая настройка адресов;
2. Поиск соседних IP-узлов;
3. В условиях отсутствия маршрутизаторов.

Маршрутизаторам запрещено транслировать в другие линии (каналы) связи какие-либо пакеты, содержащие в своих полях «*адрес отправителя сообщения*» или «*адрес получателя*» IPv6-адрес для локальной линии связи.

В этой связи, национальные диапазоны однонаправленных IPv6-адресов для локальных линий связи могли бы выглядеть следующим образом:

для Российской Федерации

fe86:4300::/24 (1111 1110 1000 0110 0100 0011 0000 0000 0000 ...);

для США

fe88:4000::/24 (1111 1110 1000 1000 0100 0000 0000 0000 0000 ...);

для Великобритании

fe88:2600::/24 (1111 1110 1000 1000 0010 0110 0000 0000 0000 ...);

для Франции

fe82:5000::/24 (1111 1110 1000 0010 0101 0000 0000 0000 0000 ...).

Оставшиеся 104 бита формата адреса (рисунок 5.31) будут распределяться органом исполнительной власти государства, которому принадлежит соответствующий диапазон адресов.

Кроме этого, стандартом RFC-4193 [179] вводится формат уникальных локальных однонаправленных IPv6-адресов. Формат таких адресов представлен на рисунок 5.32.

7 бит	*1*	*40 бит*	*16 бит*	*64 бита*
Префикс	*L*	Глобальный идентификатор	Идентификатор подсети	Идентификатор интерфейса

Рисунок 5.32 – Общий формат уникальных локальных однонаправленных IPv6-адресов

В соответствие с этим стандартом IANA присвоила уникальным локальным однонаправленным IPv6-адресам префикс «fc00::/7» (1111 1100 0000 ...).

В настоящее время бит «*L*» имеет следующую кодировку:

«1» — если префикс назначается локально;

«0» — зарезервировано для дальнейшего использования.

Вместе с тем из стандарта RFC-4193 следует, что уникальность рассматриваемых адресов будет определятся их случайным выбором. Однако, в интересах каждого государства, желающего обеспечить безопасность своей национальной ИТИ, закрепить за собой на международном уровне собственный не перекрывающийся диапазон уникальных локальных однонаправленных IPv6-адресов. В таком случае, национальные диапазоны уникальных локальных однонаправленных IPv6-адресов могли бы выглядеть следующим образом:

для Российской Федерации

fc64:3000::/20 (1111 1100[1101] 0110 0100 0011 0000 0000 0000 ...);

для США

fc84:0000::/20 (1111 1100[1101] 1000 0100 0000 0000 0000 0000 ...);

для Великобритании

fc82:6000::/20 (1111 1100[1101] 1000 0010 0110 0000 0000 0000 ...);

для Франции

fc25:0000::/20 (1111 1100[1101] 0010 0101 0000 0000 0000 0000 ...).

Как и в предыдущем случае, оставшиеся биты формата адреса (рисунок 5.32) будут распределяться государственным органом страны, которой принадлежит соответствующий диапазон адресов.

5.5.7 Обоснование и следствия

1. Глобальное расширение Интернет-сети, являющейся локомотивом всемирной информационной революции, привело к формированию национальных информационных обществ и цифровых экономик (электронных правительств) во всех экономически развитых странах мира, что обусловило появление *новой социально-экономической среды*. В каждой стране такая *социально-экономическая среда (цифровая экономика) требует установления собственных границ, а также своей защиты*, как от внешнего, так и от внутреннего вмешательства (угроз безопасности).

2. Предлагаемый метод фактически позволяет реализовать указанное выше требование. По аналогии со странами Шенгенской зоны, виртуальные границы остаются открытыми и прозрачными. Однако между странами Шенгенской зоны остаются государственные и административные границы, которые определяют зоны экономической, финансовой, юридической, экологической и др. ответственности государств. Т.е. между ними остаётся «*межа*», которая разделяет сферы интересов тех или иных государств. Также, и виртуальные границы

национальных информационных обществ, фактически, являются «*межой*» в мировом виртуальном пространстве. Таким образом, предлагаемый метод разграничивает сферы интересов цифровых экономик государств в мировом виртуальном пространстве.

3. По аналогии с национальными радиочастотными диапазонами, каждый национальный поддиапазон IPv6-адресов будет являться национальным достоянием конкретной страны. Эксплуатация такого поддиапазона может стать источником пополнения государственного бюджета. Например, индивидуальные IPv6-адреса могут выдаваться гражданам Российской Федерации (по их желанию) на безвозмездной основе пожизненно. Коммерческие организации могут брать в аренду необходимые для них фрагменты (причём уникальные, не повторяющиеся и в различных объёмах) национального поддиапазона IPv6-адресов на возмездной основе. В настоящее время, операторы сотовой связи пополняют государственную казну, оплачивая аренду того или иного частотного поддиапазона.

4. Ведение базы данных (БД) национального поддиапазона IPv6-адресов и жёсткий учёт, и контроль используемых и не используемых IPv6-адресов обеспечат точное выявление киберпреступника и любого нарушителя, осуществляющего противоправную деятельность в российском сегменте мирового информационного общества. В частности, попытки потенциальных внутренних нарушителей использовать запрещённые IPv6-адреса будут пресекаться путём блокирования соответствующих IPv6-пакетов самой ИТИЦЭ государства, которая составляет основу цифровой экономики (рисунок 1.2). В основе такого утверждения лежит неукоснительное выполнение «принципа неотвратимости наказания».

5. При попытках виртуального проникновения киберпреступников с применением неиспользуемых IPv6-адресов в российскую (и любую другую национальную) социально-экономическую среду, их действия будут пресекаться на границе национальной ИТИЦЭ. А при использовании потенциальным нарушителем действующего IPv6-адреса, факт прохождения IPv6-пакета с таким адресом будет фиксироваться на виртуальной границе, и если нарушение ИБ произойдёт, то материалы расследования киберпреступления будут переданы той стране, чей IPv6-адрес использовался (т.е. входил в национальный поддиапазон IPv6-адресов этой страны).

6. По аналогии с существующей практикой, организации, предоставляющие услуги доступа в Интернет-сеть (Интернет-провайдеры), будут брать в аренду уникальные (не перекрывающиеся) фрагменты национального поддиапазона IPv6-адресов за соответствующую плату. IPv6-адреса Интернет-провайдера будут предоставляться его клиентам на основании соответствующих договоров на постоянной или временной основе. Это позволит однозначно установить клиента Интернет-провайдера, совершившего то или иное противоправное действие в киберпространстве. Это касается и организаций, и частных лиц, создающих собственные

ГАИС на основе услуг Интернет-провайдеров, содержащие запрещённую экстремистскую, порнографическую и т.п. информацию. Если же клиент Интернет-провайдера попытается использовать не допустимый IPv6-адрес, то сервер доступа в Интернет-сеть провайдера будет пресекать (блокировать) противоправные действия (попытки) нарушителя, вплоть до отключения его от Интернет-сети и аннулирования договора о предоставлении услуг.

7. Для законопослушных граждан и сотрудников организаций, пользователей Интернет-сети, практически ничего не изменится. Как они предоставляли свои персональные данные при заключении договоров с Интернет-провайдером, так и будут делать это в дальнейшем при переходе на IPv6-адресацию. За исключением одного: у них появится право выбора, т.е. пользоваться своими индивидуальными IPv6-адресами или предоставляемыми Интернет-провайдерами. В последнем случае, провайдеры будут фактически обеспечивать (условную) «анонимность» доступа клиентов в Интернет-сеть.

8. В настоящее время многие организации в целях рекламы и привлечения большего числа клиентов в сферу своего бизнеса предоставляют доступ в Интернет-сеть на безвозмездной основе. В таких зонах свободного доступа в Интернет-сеть, предоставляемого образовательными учреждениями, частными компаниями и благотворительными организациями (например, электронные библиотеки университетов, сеть ресторанов быстрого обслуживания «*McDonald's*», московский метрополитен и др.), в зависимости от политик обеспечения ИБ этих организаций, пользователи Интернет-сети смогут также пользоваться, либо своими индивидуальными IPv6-адресами, либо предоставляемыми частными организациями, полагая, что последние арендуют уникальные фрагменты национального поддиапазона IPv6-адресов. Если же пользователь Интернет-сети в такой зоне попытается использовать не допустимый IPv6-адрес, то сервер доступа в Интернет-сеть провайдера свободного доступа будет пресекать (блокировать) противоправные действия (попытки) нарушителя, вплоть до отключения его от Интернет-сети.

5.5.8 Реализационные аспекты

Международный аспект. *Первым шагом* для реализации предлагаемого метода является официальная передача управления IPv6-адресным пространством в одну из всемирно признанных международных организаций (например, Международный союз электросвязи, Международная организация по стандартизации и др.). Возможно, для этого понадобится решение ООН, или только властей США.

Вторым шагом должно быть принятие ряда международных актов и стандартов, определяющих стратегию и политику, принципы и правила использования IPv6-адресного

пространства, а также официальное закрепление за каждым государством своего уникального поддиапазона IPv6-адресов.

Третьим шагом должен быть определён период организационной и технологической адаптации (временной интервал перехода) национальных информационных обществ к полномасштабному применению своих поддиапазонов IPv6-адресов.

Четвёртым шагом может быть создание структурного подразделения «киберполиции» в рамках, например, Интерпола (Международная организация уголовной полиции), которое бы занималось расследованием международных киберпреступления, обеспечивало взаимодействие киберполицейских служб различных государств, выявляло неправомочное использование запрещённых IPv6-адресов и т.п.

Национальный аспект. Создание или назначение в каждой стране государственного органа исполнительной власти, отвечающего за разработку и реализацию стратегии и политики, принципов и правил использования национального поддиапазона IPv6-адресного пространства. В частности, в Российской Федерации указанный орган должен быть подчинён непосредственно Президенту РФ или Председателю Правительства РФ (или его Первому заместителю) и входить в состав, либо Администрации Президента РФ, либо Аппарата Правительства РФ. При этом федеральном органе должна быть образована общественная комиссия, в которой бы участвовали представители всех заинтересованных ведомств и организаций, включая общественные. Одной из задач такой комиссии могло бы стать разрешение всех возникающих конфликтов, связанных с распределением и эксплуатацией национального поддиапазона IPv6-адресного пространства, и выработка по ним соответствующих решений и рекомендаций.

Технологический аспект. Создание и ведение БД национального поддиапазона IPv6-адресов (IPv6-БД), а также жёсткий контроль и учёт используемых и не используемых IPv6-адресов. Эксплуатация IPv6-БД должна предусматривать соответствующую систему комплексной защиты базы данных. А порядок доступа к ресурсам IPv6-БД должен быть регламентирован соответствующими федеральными нормативными правовыми актами. Сама IPv6-БД, как ИТС, может быть создана на основе государственно-частного партнёрства.

Инфраструктурный аспект. ИТИЦЭ любого государства должна включать специализированные средства контроля вредоносного и криминального трафика «по принципу»: пропускать IPv6-пакеты только с разрешёнными IPv6-адресами, к которым будут относиться:

1. Национальные поддиапазоны IPv6-адресов государств;

2. Поддиапазон специальных адресов, в который, в том числе, входят локальные, групповые и все иные технологические IPv6-адреса.

Всем государственным и частным организациям, которые осуществляют эксплуатацию и развитие национальных ИТИЦЭ, также целесообразно провести настройки своих сетевых программно-аппаратных комплексов, исключающие обработку IPv6-пакетов с запрещёнными IPv6-адресами.

Кроме того, целесообразно, чтобы государственные и частные организации вели внутренний контроль и учёт обнаруженных IPv6-пакетов с запрещёнными IPv6-адресами. Данная рекомендация предусматривает ведение корпоративной IPv6-БД, в которой будут регистрироваться все случаи противоправного использования IPv6-адресов. В дальнейшем записи таких корпоративных IPv6-БД могут использоваться в качестве доказательной базы при расследовании киберпреступлений (аудиторских проверках).

Корпоративный аспект. В Интернет-сообществе был принят стандарт RFC-1918 [180], который установил разделение всего диапазона IPv4-адресов на глобальные, локальные (корпоративные) и технологические. Аналогичный стандарт был принят и для IPv6-адресов. В этой связи, порядок и правила использования локальных IPv6-адресов организациями и ведомствами должны предусматривать персональное назначение IPv6-адресов, т.е. закрепление за каждым работником своего уникального локального IPv6-адреса. Более того в локальных IPv6-адресах должен содержаться идентификатор государства и организации/ведомства. В противном случае, организации или ведомства должны использовать уникальные (неповторяющиеся) поддиапазоны локальных IPv6-адресов. Распределение и эксплуатация локальных IPv6-адресов в странах будет входить в сферу деятельности государственного органа исполнительной власти, отвечающего за разработку и реализацию стратегии и политики, принципов и правил использования национального поддиапазона IPv6-адресного пространства.

Разделение диапазонов IPv4-адресов и IPv6-адресов на глобальные, локальные (корпоративные) и технологические повлекло за собой широкомасштабное использование трансляторов сетевых адресов. Поэтому порядок и правила применения трансляторов сетевых IPv6-адресов должны затрагивать преобразования локальных адресов в глобальные и наоборот только в рамках корпоративных (ведомственных) ИТС.

И в заключении, рассмотренный метод использования IPv6-адресации в мировом информационном обществе позволит решить проблему глобальных идентификаторов ПЭУ в Интернет-сети и Интернет-пользователей (физических лиц и организаций), существенно снизить уровень киберпреступности и защитить национальные ИТИЦЭ государств без каких-либо ограничений прав и свобод граждан на получение объективной и независимой информации.

Выводы по Главе 5

1. В первой части данной главы представлены элементы СЛ, составляющие математический аппарат синтеза ССД. Рассмотрены последовательно-параллельные орграфы, используемые при построении ССД и их анализа. Даны определения ППГ, ППОГ, ВВМ, подсетей с параллельными маршрутами и степени вложенности. Сформулированы требования надёжности при определении рекомендуемых мнений о доверии.

Кроме того, описаны два типа поиска ССД: комплексный поиск сети доверия на основе оптимального ППОГ и эвристический поиск сети доверия, близкой к оптимальному ППОГ. Также представлены алгоритмы синтеза и анализа ССД, которые отображаются и не отображаются в форму ППОГ. Определены три основных критерия синтеза ППОГ.

2. Во второй части данной главы проведён синтез объединённой системы доверия (КЗСУ) на основе ИОК. Представлен исторический ракурс создания и развития российской ИОК. Определены исходные условия, количественные и качественные показатели, необходимые для синтеза объединённой системы доверия.

Описаны структура общероссийского государственного информационного центра и реализуемые им основные функции. ОГИЦ включает корневой и УЦ первого уровня и может стать прообразом центра подтверждения подлинности федерального уровня. В качестве примера российской ведомственной сети доверия рассмотрена «сеть доверенных удостоверяющих центров» Федеральной налоговой службы РФ на основе ИОК, которая показала свою состоятельность, но имела недостатки, которые были выявлены при анализе СДУЦ. При рассмотрении СДУЦ ФНС РФ были определены типы доверия (**Д1**, **Д2**, **Д3** и **Д7**), которые она обеспечивала.

Используя аппарат СЛ и эвристический метод поиска сети доверия, была синтезирована модель системы доверия на основе объединения КЗСУ (ИОК) ИТС, образующих ИТИЦЭ, и сформулировано основное требование к ней – это должна быть ССД, отображаемая в ППОГ. Кроме этого, такая ССД должна иметь минимальное число рёбер между истоком (источником) и стоком, а также, по возможности, не иметь параллельных маршрутов доверия. С эвристической точки зрения, было определено, что использование единого ЦПП для всех российских УЦ, включая корневые УЦ ведомств/организаций и коммерческие УЦ, – наиболее приемлемое решение для создания системы доверия на основе объединения КЗСУ (ИОК) ИТС. На основании разработанной модели КЗСУ (системы доверия) на основе ИОК для ИТС были определены основные требования к участникам системы.

Далее был проведён анализ системы доверия и было показано, что доверие доверяющего субъекта (источник) к доверенной стороне (сток) снижается вследствие объективного

возникновения рисков, вызванных взаимодействием участников системы между собой (наличие человеческого фактора), даже в условиях минимально возможного числа рёбер в маршруте доверия.

На основании синтезированной модели КЗСУ (системы доверия) на основе ИОК для ИТС была предложена усовершенствованная модель, в которой концепция единого (единственного) ЦПП заменена на концепцию распределённого ЦПП. Усовершенствованная модель КЗСУ (системы доверия) на основе ИОК для ИТС включает подсистему ЦПП, состоящую из ЦПП федерального, федерального окружного, регионального и муниципального уровней. В совокупности такие ЦПП образуют единую иерархическую систему ЦПП, которая является ядром системы доверия на основе объединения КЗСУ (ИОК) ИТС.

3. В третьей части данной главы разработана функционально-структурная модель системы доверия на основе объединения КЗСУ (ИОК) ИТС. Указанная модель позволила определить состав ЕСЦПП и определить функции, которые должны быть реализованы на каждом уровне иерархии. Далее была разработана географически-распределённая модель ЕСЦПП, которая определяет географические места размещения территориальных ЦПП на каждом уровне иерархии.

Было сформулировано главное требование к системе доверия на основе объединения КЗСУ (ИОК) ИТС, заключающееся в реализации следующих основных функций: (1) предоставление (по запросу) услуг по проверке ЭП и целостности подписанного электронного документа; (2) подтверждение подлинности (по запросу) предоставленного $\text{СЕРТ}_{\text{ОК}}$; (3) проверка обоснованности (законности) выпуска $\text{СЕРТ}_{\text{ОК}}$ с целью защиты прав и свобод гражданина, на имя которого (без его согласия) мог быть издан фальсифицированный сертификат.

Третья функция является новой и никогда не была реализована ранее в рамках существующих моделей доверия (североамериканской и западноевропейской).

4. В четвёртой части данной главы представлены методы защиты пользователей ИОК. Рассмотрены наиболее изощрённые способы обмана граждан (пользователей ПЭУ), которые направлены на «отъём» их материально-финансовых ресурсов. К таким мошенническим способам относятся: незаконное издание фальсифицированных $\text{СЕРТ}_{\text{ОК}}$ и создание и использование поддельных *Web*-сайтов (ГАИС).

Проведены синтез и анализ метода, который осуществляет проверку правомочности выпуска $\text{СЕРТ}_{\text{ОК}}$ удостоверяющим центром. Указанный метод предусматривает участие специализированного государственного органа (МФЦ «Мои документы»), который регистрирует заявку пользователя ИОК на получение $\text{СЕРТ}_{\text{ОК}}$. С точки зрения СЛ маршрут транзитивного доверия в форме ППОГ дополняется ещё одним субъектом $\mathcal{D}$ (МФЦ). Модифицированный

маршрут транзитивного доверия отображается в сложную сеть доверия, анализ которой подтвердил возможность формирования доверия ПЭУ к $СЕРТ_{ОК}$ пользователя ИОК.

В основе распознавания поддельных (мошеннических) *Web*-сайтов лежит метод, который реализует проверку и подтверждение подлинности $СЕРТ_{ОК}$ провайдера электронных услуг со стороны пользователя. Указанный метод предусматривает использование пользователем специализированного КПО, установленного в его компьютер или смартфон, т.е. КПО осуществляет по команде пользователя процедуры проверки и подтверждения подлинности $СЕРТ_{ОК}$ ПЭУ.

В реальных условиях возможны два варианта обнаружения мошеннических *Web*-сайтов, которые определяются тем, какой $СЕРТ_{ОК}$ ПЭУ использует злоумышленник, либо украденный $СЕРТ_{ОК}$, принадлежащий законному ПЭУ, *Web*-портал которого имитирует злоумышленник, либо свой собственный $СЕРТ_{ОК}$, полученный электронным способом в зарубежном УЦ.

Распознавание украденного $СЕРТ_{ОК}$ основано на проведении процедуры аутентификации поддельного *Web*-сайта, алгоритм которой включает как минимум четыре итерации.

Распознавание $СЕРТ_{ОК}$, принадлежащего владельцу *Web*-сайта (ПЭУ), основано на построении сети субъективного доверия, в которой были проанализированы два маршрута доверия, решающие две разные, но чрезвычайно важные задачи в интересах пользователя. Первый маршрут доверия обеспечивает подтверждение подлинности $СЕРТ_{ОК}$ ПЭУ, если указанный сертификат был выпущен российским УЦ, внесённым в РСДС, а второй обеспечивает доказательство надёжности ПЭУ, так как он должен быть указан в РСДС. В этом случае предполагается, что ПЭУ получил $СЕРТ_{ОК}$ в УЦ, аккредитованном и зарегистрированном в РСДС, и был сам аккредитован и зарегистрирован в РСДС в качестве субъекта экономической деятельности (возможно с привлечением ФНС РФ).

В заключительной части данной главы, рассмотрен предлагаемый метод решения проблемы глобальных идентификаторов ПЭУ в Интернет-сети и Интернет-пользователей (физических лиц и организаций) на основе использования IPv6-адресации в мировом киберпространстве. Данный метод позволит существенно снизить уровень киберпреступности и защитить национальные ИТИЦЭ государств без каких-либо ограничений прав и свобод граждан на получение объективной и независимой информации.

Глава 6 РЕАЛИЗАЦИОННЫЕ АСПЕКТЫ

Проблемы внедрения и реализации полученных в диссертационном исследовании результатов характеризуются многими аспектами, основными из которых являются проблемы и задачи реализации синтезированной с использованием математического аппарата субъективной логики системы управления криптографической защитой (системы доверия) на основе ИОК на федеральном (окружном федеральном), региональном и муниципальном, и корпоративном уровнях.

6.1 Федеральный уровень

Разработанная в диссертации (Глава 5) модель объединённой системы доверия (КЗСУ) на основе ИОК рекомендуется для реализации в широкомасштабных ИТС, составляющих основу ИТИЦЭ. Очевидно, что создание таких систем потребует разработки соответствующей программы и структурной перестройки, и обновления ИТС, образующих ИТИЦЭ. Для создания типовой КЗСУ на основе ИОК в ИТС (см. рисунки 5.21 и 5.22) необходима координирующая роль федерального органа исполнительной власти (возможно в структуре Минцифры), который бы синхронизировал работы по построению КЗСУ на основе ИОК в ИТС с последующим их объединением в ИТИБ ИТИЦЭ, в том числе разработку и реализацию стратегии и политики, принципов и правил использования ИОК РФ. Безусловно, деятельность такого федерального органа исполнительной власти будет основана на совместной работе российских научно-исследовательских центров, университетов и бизнеса (частно-государственного партнёрства), а также организаций, эксплуатирующих ИТС.

Ядром системы доверия (КЗСУ) на основе ИОК должна стать ЕСЦПП. При этом, необходимо определить состав ПАК, входящих в ЦПП, который будет зависеть от их территориального расположения и пропускной способности ИТС, образующих ИТИЦЭ.

6.2 Региональный и муниципальный уровни

Создание КЗСУ на основе ИОК в ИТС, формирующих основу ИТИЦЭ, должно начаться с разработки соответствующей программы, в которой будут определены необходимые мероприятия и сроки их выполнения на всех уровнях иерархии ЕСЦПП. Такая программа должна определить создание первоочередных региональных и муниципальных ЦПП, которые будут размещаться на территории Российской Федерации в конкретных городах и городских округах (см. рисунок 5.23). ПАК для ЦПП регионального и муниципального уровней по своему составу будут дублировать ПАК для ЦПП федерального и окружного уровней, и вместе с

тем они должны учитывать географические, экономические и демографические особенности региональных и муниципальных образований.

6.3 Корпоративный уровень

Полученные по итогам диссертационных исследований результаты были реализованы или использованы в научно-исследовательской и практической деятельности государственных и частных организаций. Почти все организации, в которых были реализованы (использованы) полученные результаты, в своих Актах внедрения (реализации) отметили, что большинство научных и практических результатов обладают научной новизной и оригинальностью, и имеют практическую ценность, а это позволит решить многие проблемы обеспечения безопасности цифровой экономики Российской Федерации. Кроме того, они подтвердили наличие проблемы доверия в ИТИЦЭ и необходимость модернизации самой ИОК в Российской Федерации.

Акционерное общество «Газпромбанк»

В письме Банка ГПБ указано, что представленные в диссертации способы распознавания поддельных (мошеннических) *Web*-сайтов были всесторонне проанализированы сотрудниками Блока безопасности (группа департаментов) Банка ГПБ и будут использованы при разработке перспективных комплексов программного обеспечения в интересах обеспечения безопасности Банка ГПБ.

Акционерное общество «Научно-технический и сертификационный центр по комплексной защите информации» (входит в Госкорпорацию «РОСАТОМ»)

В Акте АО Центр «Атомзащитаинформ» отмечается, что руководством организации было принято решение о целесообразности внедрения (использования) в деятельности АО Центр «Атомзащитаинформ» отдельных научных и практических результатов, в частности, модель системы доверия (КЗСУ на основе ИОК ИТС) и методы предотвращения выпуска фальсифицированных сертификатов открытых ключей, по направлениям разработки способов и средств электронной подписи и систем контроля и ограничения доступа.

Общество с ограниченной ответственность «Код безопасности»

В Акте ООО «Код Безопасности» указано, что научные результаты диссертации, относящиеся к вопросам защиты от фальсифицированных сертификатов открытых ключей, использованы в деятельности компании ООО «Код Безопасности» при построении математической модели системы доверия к сертификатам открытых ключей, составляющей основу для

разработки перспективных отечественных средств защиты информации по направлениям разработки способов и средств электронной подписи, а также систем контроля и ограничения доступа к базам данных информационных систем.

Открытое акционерной общество Фирма «АНКАД»

В Акте ООО Фирма «АНКАД» отмечается, что руководством организации было принято решение о целесообразности использования в деятельности ООО Фирма «АНКАД» отдельных научных и практических результатов. В частности, разработанные автором диссертации алгоритмы определения обоснованности (законности) выпуска сертификата открытого ключа и метод обнаружения злонамеренных провайдеров электронных услуг могут быть использованы при разработке архитектуры программных средств электронной подписи, шифрования и аутентификации субъектов информационного взаимодействия на основе асимметричных ключевых схем.

Группа компаний «МАСКОМ»

В Акте НОУ ДПО «УЦБИ «МАСКОМ» указано, что руководством ГК «МАСКОМ» принято решение о целесообразности внедрения (использования) некоторых из полученных в диссертации результатов в деятельности отдельных структурных подразделений ГК «МАСКОМ». В частности, элементы синтезированной объединённой системы доверия и методы предотвращения выпуска фальсифицированных сертификатов открытых ключей были использованы в деятельности Учебного центра при реализации учебного курса по программе «ПМ 1. Профессиональная переподготовка по направлению «Информационная безопасность», в том числе в дистанционной версии. Также, представленные в работе современные модели инфраструктур открытых ключей и базирующихся на них системы доверия включены в курс по программе повышения квалификации М 7.0 «Криптографическая защита информации» в организации НОУ УЦБИ «МАСКОМ».

Центральный Банк Российской Федерации

В 2018 году в Федеральном исследовательском центре «Информатика управление» РАН была выполнена НИР «Ключи – 2018» (Договор № 569-27-и от 24.04.2018), заказчиком которой был Центральный Банк Российской Федерации. В частности, в Разделе 5 НИР, посвящённом анализу и дальнейшему совершенствованию (оптимизации) корпоративной ИОК Банка России, были использованы результаты, которые нашли своё отражение в диссертационной работе. Например, в НИР «Ключи – 2018» представлена информационно-технологическая инфраструктура доверия (ИТИД) на основе ИОК в Российской Федерации, включающей

ЦПП, принципы присоединения корпоративной ИОК Банка России к ИТИД и создания корпоративной ИТИД Банка России, а также модели включения внешнего УЦ, обеспечивающего внутренний и внешний ЭДО, в ИТИД Банка России.

6.4 Образовательные учреждения

Основные результаты диссертационной работы отражены в *учебниках*: Мельников Д.А. Организация и обеспечение безопасности информационно-технологических сетей и систем: Учебник. – М.: IDO Press, Университетская книга, 2015. ISBN 978-5-4243-0004-2; Мельников Д.А. Информационная безопасность открытых систем: Учебник. – М.: Флинта, Наука, 2013. ISBN 978-5-9765-1613-7; *учебных пособиях*: Орлов В.А., Мельников Д.А. Современная криптография и архитектура безопасности компьютерных сетей: Учебное пособие. – М.: МГУПИ, 2009; Фомичёв В.М., Мельников Д.А. Криптографические методы защиты информации (в 2-х частях): Учебное пособие. М.: Юрайт. 2016. ISBN 978-5-9916-7089-3.

Указанные учебники и учебные пособия рекомендованы к использованию в Национальном исследовательском ядерном университете «МИФИ», Финансовом университете при Правительстве Российской Федерации и ряде других ВУЗов при подготовке бакалавров, магистров и аспирантов по направлению «Информационная безопасность», а содержащиеся в них материалы (темы) отражены в соответствующих рабочих учебных планах дисциплин по направлению «Информационная безопасность».

Выводы по Главе 6

В данной главе рассмотрены проблемы внедрения и реализации полученных в диссертационном исследовании результатов, а также практические задачи построения КЗСУ (системы доверия) на основе ИОК для ИТС, составляющих основу ИТИЦЭ. Содержание и сложность указанных задач зависят от федерального, окружного, регионального и муниципального уровней управления, а также географических, экономических и демографических особенностей той или иной территории страны.

Показано, что основные результаты диссертационных исследований были реализованы или использованы в научно-исследовательской и практической деятельности государственных и частных организаций. Почти все организации в своих Актах внедрения (реализации) указали, что большинство результатов обладают научной новизной и оригинальностью, и имеют практическую ценность, а это позволит решить многие проблемы обеспечения безопасности цифровой экономики Российской Федерации. Кроме того, они подтвердили наличие

проблемы доверия в ИТИЦЭ и необходимость модернизации самой ИОК в Российской Федерации.

В заключительной части данной главы отмечено, что результаты исследований нашли своё отражение в учебниках и учебных пособиях, которые рекомендованы к использованию во многих ВУЗах России при подготовке специалистов по направлению «Информационная безопасность», а содержащиеся в них материалы (темы) отражены в соответствующих рабочих учебных планах дисциплин по направлению «Информационная безопасность».

ЗАКЛЮЧЕНИЕ

Переход Российской Федерации на «цифровые рельсы» требует, в первоочередном порядке, создание национальной ИТИБ, которая станет составной частью ИТИЦЭ. Российской цифровой экономике нужна надёжная ИТИБ, обеспечивающая доверие между взаимодействующими сторонами: ПЭУ и их пользователями. Очевидно, что назрела проблема глубоких преобразований существующих КЗСУ (систем доверия на основе ИОК) ИТС, образующих ИТИЦЭ. Вместе с тем, на основе объединения КЗСУ (систем доверия) на основе ИОК ИТС может быть построена эффективная национальная ИТИБ (система доверия) с целью защиты прав и законных интересов личности, бизнеса и государства от угроз ИБ.

Разработанная с использованием математического аппарата субъективной логики КЗСУ на основе ИОК ИТС позволит создать единое поле (пространство) доверия ЭП (ЕПД) и $СЕРТ_{ОК}$, а именно:

– объединить все существующие УЦ ИОК ИТС в единую национальную ИОК;

– сформировать единый распределённый российский сегмент Службы единого каталога (СЕК; с использованием протоколов доступа к СЕК), состоящий из СЕК отдельных ИОК ИТС;

– обеспечить трансграничное взаимодействие с другими странами, то есть вхождение ИОК ИТС в мировую инфраструктуру открытых ключей;

– сформировать технологическую основу доверия для различных прикладных автоматизированных информационно-технологических систем (АИС), входящих в ИТС, которые образуют ИТИЦЭ (например, системы предоставления государственных услуг в электронной форме, дистанционного образования, электронного нотариата, электронные финансовые и платёжные системы, электронные торговые площадки (электронные биржи) и аукционы и т.д.);

– привлечь бизнес к дальнейшему совершенствованию и наращиванию ИОК ИТС, которые образуют ИТИЦЭ, что обеспечит ему гарантированную и стабильную прибыль;

– обеспечить «прорыв» в технологиях и социально-экономическом развитии России.

В работе были проанализированы зарубежные варианты моделей систем доверия на основе ИОК. Однако, они не приемлемы для Российской Федерации вследствие самых различных причин, основными из которых являются функционирование всех УЦ в РФ на основе чрезвычайно уязвимой модели (ЦС+ЦР), и отсутствие государственной политики создания и дальнейшего развития национальной ИОК, и, следовательно, недостаточный уровень управления и контроля со стороны государственных органов исполнительной власти РФ. Другими словами, в нашей стране государственные институты, в качестве регуляторов, недостаточно

участвуют в создании и развитии национальной ИОК и системы доверия, в то время как в зарубежных экономически развитых странах ситуация полностью противоположная – государственные органы исполнительной власти отвечают за функционирование и дальнейшее развитие национальных ИОК, которые являются технологической основой цифровизации экономик и электронных правительств иностранных государств. Таким образом, разработка и реализация модели КЗСУ (системы доверия) на основе ИОК ИТС, входящих в ИТИЦЭ, которая послужит фундаментом построения национальной ИТИБ в интересах цифровой экономики РФ, становится важнейшей стратегической задачей, решение которой носит безотлагательный характер.

Цель, поставленная в диссертационном исследовании, достигнута: в работе синтезирована и проанализирована с использованием математического аппарата субъективной логики система управления криптографической защитой (системы доверия) на основе инфраструктуры открытых ключей с целью повышения уровня защищённости ИТС, образующих ИТИЦЭ РФ.

Также в работе:

1. Проанализирована фундаментальная проблема точного понимания «доверия» в реальном мире, и в частности в ИТС, а также взаимосвязь концепций доверия и безопасности.

2. Выбран и обоснован выбор методов и средств (математического аппарата СЛ) для проведения синтеза и анализа национальной системы доверия на основе ИОК.

3. Проанализированы организация и компоненты ИОК, а также решаемые ею задачи по обеспечению безопасности. Проведён сравнительный анализ основных архитектур ИОК и современных моделей организации ИОК, реализованных за рубежом.

4. Проанализированы проблемы и риски функционирования ИОК, а также проблемы и риски пользователей ИОК. Исследованы уязвимости, характерные для российских УЦ и снижающие доверие к ним.

5. Проведён сравнительный анализ архитектур обеспечения параметрами подлинности пользователей и провайдеров электронных услуг, а также определены необходимые условия, обеспечивающие доверие пользователей к провайдерам электронных услуг, и наоборот, – провайдеров к пользователям.

6. Проанализировано использование параметров подлинности в $СЕРТ_{ОК}$ и атрибутных сертификатах ИОК. Проведён сравнительной анализ архитектур ИОК и систем (структур) доверия на основе ИОК.

7. Синтезирована модель КЗСУ (системы доверия) на основе ИОК с использованием математического аппарата субъективной логики, и, в частности, теории синтеза сетей субъективного доверия. Проведён анализ полученной модели КЗСУ (системы доверия) с точки зрения решения задач обеспечения безопасности.

8. Разработаны методы защиты граждан и бизнеса при предоставлении электронных услуг и проведении коммерческих электронных процедур (включая финансовые транзакции) на основе национальной системы доверия, а также описаны средства, реализующие указанные методы. Предложена модель международной системы идентификации Интернет-пользователей и провайдеров электронных услуг, которая позволит снизить уровень киберпреступности в мировом информационном пространстве.

Первая глава посвящена анализу проблем обеспечения безопасности цифровой экономики РФ. В частности, показано, что современное развитие российского общества направлено на *цифровизацию* (*цифровую трансформацию*) всех его сфер, включая экономику, науку, здравоохранение, образование, культуру и т.д. Определены источники концепции «*цифровая экономика*», которая получила всемирное распространение и стала предметом многочисленных научных, экономических и общественных дискуссий, которые проводятся на государственном и экспертном уровне. Начало международному обсуждению цифровой экономики было положено на Давосском форуме в 2015 году.

Анализ рекомендаций давосских экспертов показал их практическую направленность – повышение на качественно новый уровень *технологии манипуляции общественного сознания и управления обществом*, живущим в основном в виртуальном пространстве.

Вместе с тем, были выявлены очевидные недостатки и проблемы Программы «Цифровая экономика Российской Федерации». В частности, в Программе рассматриваются не различные финансово-инвестиционные «манёвры», а конкретные технологии, которые, по идее разработчиков Программы, должны изменить экономику России к лучшему. Было показано, что цели, содержащиеся в Программе, никак не конкретизируются, т.е. не определены. Авторы сами признают, что их Программа является следствием рекомендаций Давосского форума. Более того, Программа исходит не из того, чтобы что-то производить, уметь, создавать новое, а из приоритета предоставления услуг по сравнению с производством, и интересов «квалифицированного потребителя».

Далее представлен анализ угроз национальной безопасности Российской Федерации в связи с цифровой трансформацией и рассмотрены возможные пути их нейтрализации. Показано, что такими угрозами являются: кибертерроризм и кибершпионаж, ведущиеся против России США, их союзниками; угрозы со стороны внутренних преступных сообществ, террористических организаций, радикальных религиозных, нацистских и прочих экстремистских

группировок, и антигосударственных сил; уход от налогообложения, незаконный вывоз капитала, отмывание преступно полученных доходов с использованием криптовалют (систем на основе БЧ-технологии); осуществление незаконной предпринимательской деятельности посредством использования Интернет-сети, включая электронную торговлю и финансовые услуги. Фактически, речь идёт о преступлениях в киберпространстве.

Также в данной главе рассмотрена информационно-телекоммуникационная инфраструктура цифровой экономики. ИТИЦЭ представляет собой объединение ИТС (вместе с СОИБ) различных организаций на основе первичной сети электросвязи (передачи данных). Очевидно, что обязательной подсистемой ИТИЦЭ должна стать ИТИБ, включающая СОИБ (в том числе КЗСУ) ИТС, и которая должна решать задачи предоставления перечисленных выше услуг по обеспечению ИБ, защиты первичной сети электросвязи и формирования единой системы доверия в интересах цифровой экономики.

Далее рассмотрена проблема обеспечение доверия к ИТИЦЭ, включающей ИТИБ. Разработка и внедрение ИТИЦЭ должны предусматривать процедуры формирования доверия у граждан и бизнеса, которые будут её активными пользователями, а основа такого доверия – высокий уровень защищённости ИТС, образующих ИТИЦЭ. Для решения указанной проблемы желательно, чтобы разработчики ИТС (вместе с СОИБ и КЗСУ) всегда раскрывали (при необходимости и под жёстким контролем) все относящиеся к безопасности доказательства, которые пользователи объективно должны знать, а пользователи, в свою очередь, должны стараться обосновывать своё доверие, главным образом, с помощью объективных доказательств. Все объективные (прямые и косвенные) доказательства сформируют у пользователя (бизнеса) субъективное убеждение, которое и будет его доверием к ИТС, образующим ИТИЦЭ.

Опыт зарубежных экономически развитых государств (например, США и Евросоюз) показывает, что современные ИТИБ представляют собой ИОК, на основе которых строятся различные модели систем доверия в киберпространстве между взаимодействующими субъектами. ИОК обеспечивает процедуры распределения ключей и на их основе образуют *системы доверия* со стороны пользователей ИОК. Таким образом, разработка и реализация модели ИОК в РФ и создание на её основе системы доверия за счёт объединения КЗСУ (ИОК) ИТС, образующих ИТИЦЭ, в интересах цифровой экономики РФ становится *стратегической задачей*, решение которой носит безотлагательный характер.

В заключительной части данной главы рассмотрена проблема создания национальной системы уникальных ПП на основе уникальных идентификаторов. Эта задача – прямое следствие решения проблемы нейтрализации угроз безопасности цифровой экономики Российской Федерации. Показано, что в глобальном масштабе необходима международная система

идентификации Интернет-пользователей (физических лиц и организаций), которая позволит резко снизить уровень киберпреступности на основе точной идентификации злоумышленников и при условии выполнения принципа «неотвратимости наказания».

Также в результате проведённого анализа сформулирована *цель диссертационной работы,* а также *научно-технические задачи,* которые должны быть решены в диссертационной работе.

Вторая глава диссертационного исследования посвящена общетеоретическим аспектам доверия. Она сфокусирована на фундаментальной проблеме точного понимания доверия в реальном мире, и в частности в ИТС. В ней рассмотрены основные направления и результаты научных исследований в этой области. Сделан вывод о том, что появление нового научного направления – субъективной логики (СЛ) – послужило прорывом в исследовании доверия в ИТС и, что очень важно, обеспечении ИБ.

Под доверием понимается степень, с которой один субъект готов зависеть от чего-то или кого-то в конкретной ситуации, ощущая при этом относительную безопасность, даже если возможны и негативные последствия. Смысл этого определения заключается в том, что требования к обеспечению доверия напрямую коррелируют с влиянием риска. С другой стороны, показано, что доверие, затрагивающее безопасность ИТС, отражает её сопротивляемость (резистивность) по отношению к злонамеренным действиям (например, атакам).

В работе проанализированы концептуальные понятия «доверенная сторона», «доверяющая сторона» и «преступное намерение». В работе определены два класса «доверенных сторон» – «мыслящий субъект» и «логический объект». При этом первым типом доверия называется доверие к мыслящему субъекту (человек, организация), которое представляет собой веру в то (убеждённость в том), что он будет вести себя без злого умысла. А вторым типом доверия называется доверие к логическому объекту (алгоритм, протокол, комплекс технических средств и т.п.), которое представляет собой веру в то (убеждённость/уверенность в том), что он будет противодействовать вредоносным манипуляциям злонамеренного мыслящего субъекта.

Кроме того, представлен обзор основных типов доверительных взаимосвязей с точки зрения участвующих субъектов (сторон). Доверие в ИТС предусматривает участие трёх сторон: мыслящего доверяющего субъекта, логического доверенного объекта и мыслящего внешнего угрожающего (злонамеренного) субъекта. В этой связи, проанализированы многообразие и взаимозависимость доверия, а также концепция «преступное намерение», которое означает злонамеренность, т.е. сочетание нечестности и ненадёжности. Злонамеренное поведение никогда не может быть абсолютным, а может быть определено только на основе политики безопасности, морально-этических норм, контрактов/договоров и законодательства.

В заключительной части второй главы диссертационной работы исследована концепция доверия в ИТС на основе математического аппарата СЛ. Общая идея СЛ заключается в расширении вероятностной логики до формализованного подхода (формализма) за счёт прямого дополнения, т.е. включения неопределённости вероятностей и выразителя субъективной веры (убеждённости). Аргументы в СЛ называются субъективными мнениями (или просто мнениями). Показано, что доверие имеет две основные интерпретации: доверие к надёжности и доверие при принятии решения. Также проведено сравнение репутации и доверия, и проанализирована транзитивность доверия. Рассмотрены понятия рекомендуемого и функционального доверия. Представлены семантические требования (критерии) транзитивности доверия. Описаны операторы понижения, слияния и переоценки доверия.

В третьей главе диссертационного исследования рассмотрены основные различия между БДО и ЭДО, и показано, что в реальной жизни БДО невозможно полностью отобразить в ЭДО. Также показано, что глобальная информатизация позволила «перевести» БДО в ИТС («на электронные рельсы»), реализующие ЭДО, а инфраструктура открытых ключей способна ускорить и упростить переход к ЭДО, а также предоставить услуги обеспечения безопасности. К наиболее важным ИОК-услугам относятся: обеспечение целостности, конфиденциальности, неотказуемости, а также процедуры идентификации и аутентификации. А в качестве дополнительных: восстановление ключа и авторизация (определение прав доступа).

Далее рассмотрены организация и компоненты ИОК. Под инфраструктурой открытых ключей понимается совокупность ПО, технологий шифрования и служб, которые способны в интересах организаций обеспечить защиту линий и каналов связи и электронных коммерческих сделок, осуществляемых с использованием сетей передачи данных. ИОК привязывает открытые криптографические ключи к субъектам, позволяет другим субъектам проверять привязки открытых ключей и предоставляет услуги, которые необходимы при проведении соответствующих процедур обеспечения ключами в распределённой ИТС. Функциональными элементами ИОК являются: центры сертификации (включая центры атрибутных сертификатов), центры (пункты) регистрации, репозитарии и архивы.

Далее представлен анализ основных архитектур ИОК, а также форматы данных, используемых в ИОК. Существуют две общепринятые используемые в организациях ИОК-архитектуры, которые обеспечивают такую проверку (подтверждение) подлинности $СЕРТ_{ОК}$: иерархическая и сетевая. В случае иерархической архитектуры, ЦС «выстраиваются иерархически» под корневым ЦС, который выпускает $СЕРТ_{ОК}$ для «подчинённых» ЦС. Последние могут выпускать $СЕРТ_{ОК}$ для своих «подчинённых» ЦС или для пользователей. В случае сетевой архитектуры, независимые ЦС взаимно сертифицируются каждый с каждым (т.е. выпускают и доставляют $СЕРТ_{ОК}$ друг другу), в результате чего формируется сеть доверенных

связей между «равноправными» ЦС. Затем рассматриваются современные типы ИОК-архитектур, к которым относятся «строгая иерархия», «общая иерархия», «произвольная структура», «изолированные иерархии» и «взаимно-сертифицированные иерархии».

В дальнейшем проанализированы североамериканская и западноевропейская модели организации ИОК, которые по своей сути неприемлемы для реализации в Российской Федерации.

В заключительной части третьей главы проанализированы проблемы и риски функционирования ИОК, а также проблемы и риски пользователей ИОК. Показана несостоятельность и уязвимость модели УЦ, состоящего из двух частей: ЦР и ЦС, которая характерна для УЦ в Российской Федерации.

Четвёртая глава диссертационной работы посвящена исследованию проблемы обеспечения параметрами подлинности. Показано, что одним из фундаментальных понятий, используемых в системах аутентификации на основе ИОК, является ПП. Наличие возможности отображать и распознавать объекты в компьютерных сетях имеет основополагающее значение для систем электронного взаимодействия и сотрудничества, и является функциональным фундаментом практически всех систем обеспечения безопасности, например, системы авторизации и управления доступом, а также обеспечения репутации. Кроме того, проанализированы концепции «субъекты/объекты», «параметры подлинности» (включая цифровые ПП), «идентификаторы» и «атрибуты». Также рассмотрены системы обеспечения пользователей параметрами подлинности. В частности, были проанализированы изолированная, федеративная, централизованная СОПП, а также система персональной аутентификации. Для каждой из указанных СОПП были описаны их архитектуры, проблемы доверия (клиента к ПЭУ и ПЭУ к клиенту) и определены восемь типов функционального доверия.

Показано, что для обоюдной аутентификации между пользователями и ПЭУ необходим специализированный ПАК – персональное устройство аутентификации (ПУА). Функциональность ПУА способна интегрировать его с другими устройствами, например, мобильные телефоны (смартфоны), которые в настоящее время получили массовое распространение. Использование смартфона позволило внедрить самые передовые технологии, например, регистрацию и аутентификацию на основе запросно-ответного способа информационного взаимодействия («клиент-сервер») по дополнительному каналу мобильной связи. Однако, современные системы аутентификации при предоставлении электронных услуг не обеспечивают аутентификацию ПЭУ.

Также отмечено, что ПЭУ, которые функционируют в глобальных ИТС, например, Интернет-сети, нуждаются в глобальных идентификаторах. К сожалению, не существует надёжных и реальных глобальных пространств имён для людей и организаций, и поэтому весьма

сомнительна значимость аутентификации ПЭУ с учётом нынешней парадигмы обеспечения безопасности во всемирной ГИТС.

В заключительной части четвёртой главы проанализированы модели архитектур ИОК, среди которых одиночная иерархическая, многоиерархическая ИОК, модель избираемого прямого доверия, модель со взаимной сертификацией корневых ЦС, модель со связующим ЦС, *PGP*-модель, модель на основе центра подтверждения подлинности и модель на основе защищённой DNS-системы. Для каждой из них указаны проблемы обеспечения доверия, их преимущества и недостатки. Сделан вывод о том, что в современных условиях модель с ЦПП является наиболее перспективной и востребованной. И в завершении главы рассмотрены основные направления развития и совершенствования ИОК.

В пятой главе диссертации представлены элементы СЛ, составляющие математический аппарат синтеза ССД. Рассмотрены последовательно-параллельные орграфы, используемые при построении ССД и их анализа. Даны определения ППГ, ППОГ, ВВМ, подсетей с параллельными маршрутами и степени вложенности. Сформулированы требования надёжности при определении рекомендуемых мнений о доверии. Кроме того, описаны два типа поиска ССД: комплексный поиск сети доверия на основе оптимального ППОГ и эвристический поиск сети доверия, близкой к оптимальному ППОГ. Также представлены алгоритмы синтеза и анализа ССД, которые отображаются и не отображаются в форму ППОГ. Определены три основных критерия синтеза ППОГ.

Далее проведён синтез КЗСУ (системы доверия) на основе ИОК для ИТС. Представлена ретроспектива создания и развития ИОК в РФ. Определены исходные условия, количественные и качественные показатели, необходимые для синтеза системы доверия. Используя аппарат СЛ и эвристический метод поиска сети доверия, была синтезирована модель КЗСУ (системы доверия) на основе ИОК для ИТС, образующих ИТИЦЭ, и сформулировано основное требование к ней – это должна быть ССД, отображаемая в ППОГ. Кроме этого, такая ССД должна иметь минимальное число рёбер между истоком (источником) и стоком, а также, по возможности, не иметь параллельных маршрутов доверия. С эвристической точки зрения, было определено, что использование единого ЦПП для всех российских УЦ, включая корневые УЦ ведомств/организаций и коммерческие УЦ, – наиболее приемлемое решение для создания национальной системы доверия на основе ИОК. На основании разработанной модели системы доверия были определены основные требования к участникам системы.

Затем был проведён анализ КЗСУ (системы доверия) на основе ИОК для ИТС, образующих ИТИЦЭ, и было показано, что доверие доверяющего субъекта (источник) к доверенной

стороне (сток) снижается вследствие объективного возникновения рисков, вызванных взаимодействием участников системы между собой (наличие человеческого фактора), даже в условиях минимально возможного числа рёбер в маршруте доверия.

На основании синтезированной модели КЗСУ (системы доверия) на основе ИОК для ИТС была предложена усовершенствованная модель, в которой концепция единого (единственного) ЦПП заменена на концепцию распределённого ЦПП. Усовершенствованная модели КЗСУ (системы доверия) на основе ИОК включает подсистему ЦПП, состоящую из ЦПП федерального, федерального окружного, регионального и муниципального уровней. В совокупности такие ЦПП образуют единую иерархическую систему ЦПП, которая является ядром системы доверия на основе ИОК.

Далее была разработана функционально-структурная модель КЗСУ ИТС. Указанная модель позволила определить состав ЕСЦПП (архитектуру ЕСЦПП) и определить функции, которые должны быть реализованы на каждом уровне иерархии. Также была разработана географически-распределённая модель ЕСЦПП, которая определяет географические места размещения ЦПП на каждом уровне иерархии.

Было сформулировано главное требование к КЗСУ ИТС, заключающееся в реализации следующих трёх основных функций: предоставление (по запросу) услуг по проверке ЭП и целостности подписанного электронного документа; подтверждение подлинности (по запросу) предоставленного $СЕРТ_{ОК}$; проверка обоснованности (законности) выпуска $СЕРТ_{ОК}$ с целью защиты прав и свобод гражданина, на имя которого (без его согласия) мог быть издан фальсифицированный сертификат. При этом третья функция является новой и никогда не была реализована ранее в рамках существующих моделей доверия (североамериканской и западноевропейской).

Также представлены методы защиты пользователей ИОК ИТС и описаны средства, реализующие указанные методы. Рассмотрены наиболее изощрённые способы обмана граждан (пользователей ПЭУ), которые направлены на «отъём» их материально-финансовых ресурсов. К таким мошенническим способам относятся: незаконное издание фальсифицированных $СЕРТ_{ОК}$ и создание и использование поддельных *Web*-сайтов (ГАИС). Проведены синтез и анализ метода, который осуществляет проверку правомочности выпуска $СЕРТ_{ОК}$ удостоверяющим центром. В основе распознавания поддельных (мошеннических) *Web*-сайтов (ГАИС) лежит метод, который реализует проверку и подтверждение подлинности $СЕРТ_{ОК}$ провайдера электронных услуг со стороны пользователя.

В завершении пятой главы была рассмотрена модель (метод) глобальной идентификации Интернет-пользователей (физических лиц и организаций) и ПЭУ в Интернет-сети. В ос-

нове этой модели (способа) лежит использование объектных идентификаторов (OID) государств, которые размещаются в субполе «префикс глобальной маршрутизации» поля IPv6-адреса в заголовке IPv6-пакета (128-битовые сетевые идентификаторы,), а также разбиение всего пространства таких адресов на национальные поддиапазоны в соответствие с OID государств и запрет использования IPv6-адресов из оставшейся части адресного пространства. Предложенная модель (метод) позволит существенно снизить уровень киберпреступности и защитить национальные ИТИ цифровых экономик государств без каких-либо ограничений прав и свобод граждан на получение объективной и независимой информации, и ведение экономической деятельности в киберпространстве.

В шестой главе диссертации рассмотрены проблемы внедрения и реализации полученных в диссертационном исследовании результатов, а также практические задачи построения объединённой КЗСУ (системы доверия) на основе интеграции ИОК для ИТС, образующих ИТИЦЭ РФ. Содержание и сложность таких задач зависят от федерального, окружных федеральных, региональных и муниципальных уровней управления, а также географических, экономических и демографических особенностей той или иной территории страны.

Показано, что основные результаты диссертационных исследований были реализованы или использованы в научно-исследовательской и практической деятельности государственных и частных организаций. Почти все организации в своих Актах внедрения (реализации) указали, что большинство результатов обладают научной новизной и оригинальностью, и имеют практическую ценность, а это позволит решить многие проблемы обеспечения безопасности цифровой экономики РФ. Кроме того, они подтвердили наличие проблемы доверия в ИОК РФ и необходимость модернизации самой ИОК на основе объединения КЗСУ (ИОК) ИТС, входящих в ИТИЦЭ.

В заключительной части данной главы отмечено, что результаты исследований нашли своё отражение в учебниках и учебных пособиях, которые рекомендованы к использованию во многих ВУЗах России при подготовке специалистов по направлению «Информационная безопасность», а содержащиеся в них материалы (темы) отражены в соответствующих рабочих учебных планах дисциплин по направлению «Информационная безопасность».

ВЫВОДЫ ПО ДИССЕРТАЦИИ

По итогам проведённого научного исследования можно сделать следующие выводы:

1. Анализ Национальной Программы «Цифровая экономика Российской Федерации» показал, что она является следствием рекомендаций давосских экспертов, реализация которых может привести к повышению на качественно новый уровень *технологии манипуляции общественного сознания и управления обществом*, живущим в основном в виртуальном пространстве. Вместе с тем, Программа обладает очевидными недостатками, среди которых отсутствие её конечных целей и данных об ожидаемом экономическом эффекте от мероприятий, описанных в Программе. Цифровая трансформация экономики повлечёт за собой угрозы национальной безопасности Российской Федерации. Основной путь их нейтрализации – разработка и внедрение ИТИБ. Современная форма реализации ИТИБ – это объединение КЗСУ (ИОК) ИТС, образующих ИТИЦЭ, которое обеспечивает процедуры распределения ключей и на их основе образует *систему доверия* со стороны пользователей ИОК. Таким образом, актуальной научно-технической проблемой является построение КЗСУ (системы доверия) на основе ИОК ИТС с целью парирования угроз ИБ, связанных с созданием цифровой экономики Российской Федерации, и защиты прав и законных интересов личности, бизнеса и государства.

2. Впервые, используя математический аппарат СЛ и эвристический метод поиска сети доверия, была синтезирована новая (ранее не известная) модель КЗСУ (системы доверия) на основе ИОК для ИТС и сформулировано основное требование к ней – это должна быть сеть субъективного доверия (ССД), отображаемая в форму последовательно-параллельного орграфа (ППОГ). Синтезированная модель КЗСУ (системы доверия) ИТС полностью удовлетворяет указанному требованию, позволяет сформировать маршруты доверия с минимальным числом рёбер в ППОГ, и, таким образом, напрямую соединить УЦ, ПЭУ и ИОК-пользователей с ЦПП, т.е. обеспечить прямую транзитивность доверия. Кроме того, указанная модель не требует группирования УЦ в иерархическую структуру с корневым УЦ или сетевую структуру с главным УЦ, но включает ЕСЦПП, во главе которой ЦПП федерального уровня.

3. На основе анализа модели КЗСУ (системы доверия) на основе ИОК для ИТС, образующих ИТИЦЭ в РФ, было сформулировано главное функциональное требование к ней, заключающееся в реализации следующих основных функций: предоставление (по запросу) услуг по проверке ЭП и целостности подписанного электронного документа; подтверждение подлинности (по запросу) предоставленного $СЕРТ_{ОК}$; (впервые) проверка обоснованности (законности) выпуска $СЕРТ_{ОК}$ с целью защиты прав и свобод гражданина, на имя которого (без его согласия) мог быть издан фальсифицированный сертификат.

4. На основе синтезированной модели КЗСУ (системы доверия) ИТС был предложена усовершенствованная (функционально-структурная) модель, в которой концепция единого (единственного) ЦПП заменена на концепцию распределённого ЦПП. Усовершенствованная модель КЗСУ (системы доверия) ИТС включает подсистему ЦПП, состоящую из ЦПП федерального, федерального окружного, регионального и муниципального уровней, и устанавливает требования к ним. В совокупности такие ЦПП образуют ЕСЦПП, которая является ядром системы доверия на основе объединения КЗСУ (ИОК) ИТС. Также была разработана географически-распределённая модель системы доверия на основе объединения КЗСУ (ИОК) ИТС, которая определяет географические места размещения ЦПП на каждом уровне иерархии.

5. Впервые, с теоретической точки зрения, был обнаружена и проанализирована глобальная уязвимость современной национальной ИОК Российской Федерации – чрезвычайно уязвимая модель построения всех без исключения российских УЦ (ЦС+ЦР). Следствием этого является невозможность национальной ИОК Российской Федерации предотвратить выпуск фальсифицированных $СЕРТ_{ОК}$, которые, в свою очередь являются источниками многочисленных рисков для граждан и организаций различных форм собственности.

6. Как следствие предыдущего вывода, была определена новая функция (задача), реализуемая (решаемая) разработанной системы доверия на основе объединения КЗСУ (ИОК) ИТС, образующих ИТИЦЭ, – определение обоснованности (законности) выпуска $СЕРТ_{ОК}$, которая дополнила перечень известных функций (задач) обеспечения безопасности, реализуемых (решаемых) ИОК. Следует отметить, что существующие модели зарубежных систем (структур) доверия на основе ИОК, эту задачу не решают. Таким образом, были расширены научные представления о возможностях различных архитектур ИОК, выполняющих функции инфраструктуры обеспечения безопасности.

7. С целью практического решения задачи определения обоснованности (законности) выпуска $СЕРТ_{ОК}$ и парирования угроз безопасности, связанных с выпуском фальсифицированных $СЕРТ_{ОК}$ УЦ, был впервые разработан метод, который предусматривает совместные процедуры подтверждения подлинности и проверки законности выпуска $СЕРТ_{ОК}$. В рамках разработки указанного метода были предложены алгоритм и вариант его реализации, предусматривающий участие специализированного государственного органа (многофункционального центра «Мои документы»), который регистрирует заявку пользователя ИОК на получение $СЕРТ_{ОК}$ и в последующем подтверждает наличие такой заявки и $СЕРТ_{ОК}$, полученного в УЦ пользователем ИОК, и последовательный номер которого соответствует («привязан» к) номеру заявки.

8. С целью защиты граждан и организаций различных форм собственности разработан метод распознавания поддельных (мошеннических) *Web*-сайтов, который включает процедуры проверки и подтверждение подлинности $СЕРТ_{ОК}$ ПЭУ со стороны пользователя (организации) с целью предотвращения (блокирования) мошеннических транзакций. Указанный метод предусматривает использование пользователем (организацией) специализированного программного средства (КПО), установленного в его компьютер или смартфон, т.е. КПО, который по команде пользователя осуществляет указанные процедуры. Предложенный метод включает два варианта обнаружения мошеннических *Web*-сайтов, которые определяются тем, какой $СЕРТ_{ОК}$ ПЭУ использует злоумышленник, либо украденный $СЕРТ_{ОК}$, принадлежащий законному ПЭУ, *Web*-портал которого имитирует злоумышленник, либо свой собственный $СЕРТ_{ОК}$, полученный электронным (удалённым) способом в зарубежном УЦ. Этот метод также предусматривает проверку наличия регистрации ПЭУ в РСДС, который может формироваться и обслуживаться совместно с ФНС России.

9. Впервые на основе анализа понятия «доверия» и «взаимосвязей/взаимоотношений» были разработаны новые структурные модели доверительных взаимосвязей: первая – модель взаимодействия с поддельным (мошенническим) *Web*-сайтом; вторая – модель компьютерного шпионажа. Эти модели позволили определить и конкретизировать содержание метода обнаружения поддельных (мошеннических) *Web*-сайтов (злонамеренных ПЭУ), способных ввести в заблуждение их пользователей (граждан и организаций).

10. Впервые предложен(а) метод (модель) глобального обеспечения ПП Интернет-пользователей (физических лиц и организаций) и провайдеров электронных услуг на основе логической характеристики IPv6-протокола. Всеобъемлющая реализация этого(ой) метода (модели) позволит значительно упростить распознавание (аутентификацию) Интернет-объектов, а также парировать возможные попытки проведения атак или распознавать источники таких атак. А в дальнейшем обеспечит существенное снижение уровня киберпреступности при строгом выполнении принципа «неотвратимости наказания».

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

АИС – автоматизированная информационно-технологическая система
АКС – ассиметричная криптографическая система
БДО – бумажный документооборот
БСК – барицентрическая система координат
БФПВ – функция плотности вероятности бета(β)-распределения
ВВМ – выходное-входное множество
ВПО – вредоносное ПО
ГА – гипероблась анализа
ГАИС – гипертекстовая АИС (World Wide Web)
ГСА – грамматико-синтаксический анализатор
ГЦС – главный ЦС
ДЗЦС – доверенный замыкающий ЦС (anchor)
ДТС – доверенная третья сторона
ДФПВ – функция плотности вероятности распределения Дирихле
ЕС – Европейский союз (или Евросоюз)
ИБ – информационная безопасность
ИОК – инфраструктура открытых ключей
ИНН – индивидуальный номер налогоплательщика
ИТИ – информационно-технологическая инфраструктура
ИТС – широкомасштабная информационно-телекоммуникационная система
ИТСЭП – ИТС, которая обрабатывает сообщения, содержащие ЭП
КИК – категорический императив И. Канта
КПО – комплекс программного обеспечения
КТС – комплекс техническихсредств
МРСДС – РСДС муниципального уровня
МФЦ – многофункциональный центр «Мои документы»
НСД – несанкционированный доступ
ЕСЦПП – единая иерархическая система ЦПП
ОА – область анализа
ОГИЦ – Общероссийский государственный информационный центр
ОДС – отчёт о текущей деятельности в области сертификации (certificate practice statement)
ОРСДС – РСДС федерального окружного уровня
ПАК – программно-аппаратный комплекс
ПИН – персональный идентификационный номер
ПО – программное обеспечение

ПП – параметр подлинности
ППГ – последовательно-параллельный граф
ППОГ – последовательно-параллельный ориентированный граф (орграф)
ПРП – процедура подтверждения параметра подлинности
ПУА – персональное устройство аутентификации
ПЭМИН – побочные электромагнитные излучения и наводки
ПЭУ – провайдер электронных услуг
РСДС – реестр состояния доверенных служб
РРСДС – РСДС регионального уровня
РФ – Российская Федерация
СДУЦ – сеть доверенных УЦ ФНС РФ
СЕК – служба единого каталога (The Directory)
$СЕРТ_{АТ}$ – атрибутный сертификат
$СЕРТ_{ОК}$ – сертификат открытого ключа
СКУД – система контроля и УД
СЛ – субъективная логика
СОПП система обеспечения ПП
СОС – список отозванных сертификатов
ССБ – сетевой сегмент безопасности
СПП – система подтверждения подлинности
СПБЗ – субпротокол «блочной защиты» (record protocol)
СППР – субпротокол «приветствие» (handshake protocol)
ССД – сеть субъективного доверия
ССС – сервер, предоставляющий информацию о состоянии сертификатов
СУБД – система управления базой данных
СЦС – связующий ЦС
США – Соединённые Штаты Америки
УД – управления доступом
УИД – уникальный идентификатор
УЦ – удостоверяющий центр
ФАИТ – Федеральное агентство по информационным технологиям
ФНС – Федеральная налоговая служба РФ
ФПС – федеральная политика сертификации США
ФРСДС – РСДС федерального уровня
ФСД – федеральный совет IT-директоров США
ФСЦС – федеральный СЦС США
ФУЦ – удостоверяющий центр федерального уровня
ФЦОР – федеральный центр обеспечения и регулирования национальной ИОК США

ФЦРП – федеральный центр разработки и реализации политики развития национальной ИОК США

ФЦП – федеральная целевая программа

ЦПП – центр подтверждения подлинности

ЦС – центр сертификации

ЦР – центр регистрации

ЦРПС – центр реализации политики сертификации США

ЭВМ – электронная вычслительная машина (компьютер)

ЭДО – электронный документооборот

ЭП – электронная подпись

BAN – первые буквы авторов логики для аутентификации: **B**urrows M., **A**badi M. и **N**eedham R.

CC – conjunctive certainty (конъюнктивная достоверность)

DAP – directory access protocol (протокол доступа к СЕК-серверу)

DC – degree of conflict (степень противоречия)

DNS – domain name system (система именования сетевых сегментов/областей в Интернет-сети)

DNSSEC – DNS Security Extension (защищённая DNS-система)

IANA – Internet Assigned Numbers Authority (центр распределения адресов и идентификаторов в Интернет-сети)

IETF – Internet Engineering Task Force (технический комитет по стандартизации в Интернет-сети)

ISO – International Standardization Organization (Международная организация по стандартизации)

ITU-T – International Telecommunications Union, Standardization Sector (Международный союз электросвязи, сектор стандартизации)

LDAP – lightweight directory access protocol (протокол упрощённого доступа к СЕК-серверу)

NL – nesting level (степень вложенности)

OCSP – online certificate status protocol (протокол интерактивной проверки состояния СЕРТ$_{ОК}$)

OID – object identificator (идентификатор объекта)

PD – projected probability distance (расстояние между прогнозируемыми вероятностями)

PGP – pretty good privacy (буквально «хорошее средство обеспечения неприкосновенности» – КПО, реализующий различные критографические функции)

RF – revision factor (показатель (причина) переоценки)

SDSI – simple distributed security infrastructure (простая распределённая инфраструктура безопасности)

SPKI – simple PKI (простая PKI)

TCP – transmission control protocol (протокол управления передачей на транспортном (3ем) уровне Интернет-архитектуры)

TLS – transport layer security (протокол обеспечения безопасности на транспортном (3ем) уровне Интернет-архитектуры)

UD – uncertainty differential (различие неопределённости)

URI – uniform resource identifier (универсальный идентификатор ресурсов)

UTC – coordinated universal time (всеобщее скоординированное время)

X.500 – Рекомендация ITU-T X.500

X.509 – Рекомендация ITU-T X.509

XML – расширенный язык гипертекстовой разметки документов

$\mathcal{A}$ – мыслящий субъект

A – логический объект

ω – (субъективное) мнение

$\omega_X^{\mathcal{A}}$ – мнение субъекта $\mathcal{A}$ о логическим объекте X

b_X – распределение множества убеждений о логическим объекте X

d_x распределение множества неверия в логический объект X

u_X – множество неопределённостей относительно логического объекта X

a_X – распределение априорной вероятности

$\mathcal{R}(\mathbb{X})$ – ГА

$\mathrm{P}(x)$ – прогнозируемая (апостореорная) вероятность двоичного мнения о величине x

$\mathrm{Var}(x)$ – дисперсия двоичных мнений

$\mathcal{K}_3$ – закрытый криптографический ключ

$\mathcal{K}_0$ – открытый криптографический ключ

$\deg_{in}(\mathcal{B})$ – число рёбер, входящих в узел $\mathcal{B}$

$\deg_{out}(\mathcal{B})$ – число рёбер, исходящих из узла $\mathcal{B}$

СЛОВАРЬ ТЕРМИНОВ

Атрибут – информационный объект, который включает два компонента (поля): наименование параметра/признака и значение этого параметра/признака, например, ФИО: Иванов Пётр Сергеевич.

Аутентификация – процедура, которая подтверждает, что объект действительно является тем, за кого себя выдаёт.

Доверие – это степень, с которой один субъект готов зависеть от чего-то или кого-то в конкретной ситуации, ощущая при этом относительную безопасность, даже если возможны и негативные последствия.

Доверие к мыслящему субъекту – вера в то (убеждённость в том), что он будет вести себя без злого умысла.

Доверие к логическому объекту – вера в то (убеждённость/уверенность в том), что он будет противодействовать вредоносным манипуляциям мыслящего субъекта.

Инфраструктура открытых ключей – совокупность программного обеспечения, технологий шифрования и служб, которые способны в интересах организаций обеспечить защиту линий и каналов связи и электронных коммерческих сделок, осуществляемых с использованием сетей передачи данных.

Конфиденциальность – это свойство информации, которое обеспечивает её недоступность или нераскрываемость для неавторизованных пользователей, объектов и процессов.

Криптографический ключ – секретная последовательность символов, используемая криптографическими алгоритмами для зашифрования и расшифрования данных.

Мнение – суждение, выражающее оценку чего-нибудь, отношение к чему-нибудь, взгляд на что-нибудь.

Неотказуемость (обеспечение неотказуемости) – невозможность отказаться от чего-либо, которая обеспечивается путём проведения процедур сбора, обработки, обеспечения доступности и признании неопровержимости доказательства (свидетельства) относительно заявленного события или действия с целью урегулирования споров о произошедшем или не произошедшем событии или действии.

Преступное намерение (злонамеренность) – это сочетание нечестности и ненадёжности.

Репозитарий – база данных, в которой хранятся действующие цифровые сертификаты системы центров сертификации.

Репутация – создавшееся общее мнение людей о достоинствах и недостатках кого-либо или о чего-либо, т.е. как люди думают о ком-то или о чём-то.

Целостность – это свойство информации, которое предотвращает её изменение или разрушение неавторизованным способом.

Центр регистрации – объединение программно-аппаратного комплекса и обслуживающего его персонала, доверенный субъект центра сертификации для регистрации или подтверждения параметров подлинности клиентов, пользующихся услугами этого центра сертификации.

Центр сертификации – это объединение комплекса технических, программно-аппаратных средств и обслуживающего персонала, которое формирует, подписывает и издаёт $СЕРТ_{ОК}$ для своих пользователей.

Электронное сообщение – последовательность двоичных чисел (единиц и нулей), которые кодируют информацию в определённом формате.

Эпистемология – раздел философии, изучающий сущность познания и критерии его истинности.

СПИСОК ЛИТЕРАТУРЫ

[1] Мельников Д.А. и др. Практическая реализация различных моделей инфраструктуры открытых ключей // Безопасность информационных технологий. Т. 23, № 1. 2016. С. 100 – 114. ISSN 2074-7128. URI: https://bit.mephi.ru/index.php/bit/article/view/38.

[2] Перечень аккредитованных удостоверяющих центров сайт Министерства цифрового развития, связи и массовых коммуникаций РФ. URI: https://digital.gov.ru/ru/activity/govservices/certification_authority/.

[3] 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». URI: https://www.garant.ru/products/ipo/prime/doc/71715542/.

[4] Счётная палата Российской Федерации. Бюллетень Счётной палаты №12 (декабрь) 2017 г. Пресс-центр счётной палаты Российской Федерации, URI: http://audit.gov.ru/activities/bulleten/bulletin-of-the-accounting-chamber-12-2017.php.

[5] Аракелян Е., Хожателова Ю. Новый вид мошенничества: Оставили без квартиры, подделав электронную подпись. // Комсомольская правда, 2019. URI: https://www.kp.ru/daily/26979/4038526/.

[6] Мельников Д.А., Хоменок А.В. Современное состояние отечественной инфраструктуры электронной коммерции // Экономика, статистика и информатика. – 2012. – № 1. – С. 169-173.

[7] Постановление Правительства РФ от 30.06.2004 г. № 319 «Об утверждении положения о Федеральном агентстве по информационным технологиям». URI: http://www. consultant.ru.

[8] Баушев С.В., Кузьмин А.С. и др. Удостоверяющие автоматизированные информационные системы и средства. Введение в теорию и практику: Учебное пособие / под ред. С.В. Баушева, А.С. Кузьмина. – СПб.: БХВ-Петербург, 2016. – 304 с.: ил. ISBN 978-5-9775-3733-9.

[9] Melnikov D.A., et al. 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. URI: https://www.researchgate.net/publication/322288892_Russian_Model_of_Public_Keys_ and_ Validation_Infrastructure_as_Base _of_the_Cloud_Trust.

[10] Фомичёв В.М., Мельников Д.А. Криптографические методы защиты информации (в 2-х частях): Учебное пособие. М.: Юрайт. 2016. ISBN 978-5-9916-7089-3.

[11] Мельников Д.А. и др. Модель доверия для цифровой экономики Российской Федерации // Безопасность информационных технологий. Т. 27, № 2. 2020. С. 47 – 64. ISSN 2074-7128. URI: https://bit.mephi.ru/index.php/bit/article/view/1270.

[12] Zimmermann P. The Official PGP User's Guide. MIT Press, 1995.

[13] Schneider F.B., et al. Trust in Cyberspace. National Academies Press, 1999, 352 p. ISBN: 0309-51970-5. URI: http://www.nap.edu/catalog/6161.html.

[14] Ellison C., et al. SPKI Certification Theory, RFC 2693, September 1999. URI: http:// www.ietf.org/rfc/rfc2693.txt.

[15] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures. Official Journal of the European Communities 19.01.2000. P. 0012 – 0020. URI: https://eur-lex.europa.eu/eli/dir/ 1999/93/oj.

[16] National Institute of Standards and Technology. Introduction to Public Key Technology and the Federal PKI Infrastructure. NIST Special Publication 800-32, 26 February 2001.

[17] Cooper D., et al. «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile», RFC 5280, May 2008. URI: https://www.rfc-editor.org/rfc/ rfc5280.txt.

[18] Jøsang A. PKI Trust Models. In Atilla Elçi et al. (editors), Theory and Practice of Cryptography Solutions for Secure Information Systems (CRYPSIS). IGI Global, May 2013. ISBN13: 9781466640306.

[19] Jøsang A. Subjective Logic. A Formalism for Reasoning Under Uncertainty. – Springer International Publishing, Switzerland, 2016. – 337 p. ISBN 978-3-319-42335-7(1). DOI 10.1007/ 978-3319-42337-1.

[20] Jøsang A. The right type of trust for distributed systems. In C. Meadows, editor, Proc. Of the 1996 New Security Paradigms Workshop. ACM, New York, 1996.

[21] Knapskog S.J. and Jøsang A. A metric for trusted systems (full paper). In Proceedings of the 21st National Information Systems Security Conference. NSA, October 1998.

[22] Jøsang A. An algebra for assessing trust in certification chains. In J. Kochmar, editor, Proceedings of the Network and Distributed Systems Security Symposium (NDSS'99). The Internet Society, 1999.

[23] Lo Presti S. and Jøsang A. Analysing the relationship between risk and trust. In T. Dimitrakos, editor, Proceedings of the Second International Conference on Trust Management (iTrust), volume 2295 of LNCS, p.p. 135–145. Springer, Berlin, 2004.

[24] Haller J. and Jøsang A. Dirichlet reputation systems. In The Proceedings of the International Conference on Availability, Reliability and Security (ARES 2007), Vienna, Austria, April 2007.

[25] Lance K. and Jøsang A. Principles of subjective networks. In Proceedings of the 19th International Conference on Information Fusion (FUSION 2016). IEEE, Los Alamitos, 2016.

[26] Иванов В.В., Малинецкий Г.Г. Цифровая экономика: мифы, реальность, перспектива. – М.: РАН, 2017. 64 с. ISBN 978-5-906906-04-5.

[27] Шваб К. Четвёртая промышленная революция. М.: Издательство «Э», 2016. 138 с. ISBN 978-5-699-90556-0.

[28] National Institute of Standards and Technology. Blockchain Technology Overview. NISTIR 8202, October 2018. URI: https://doi.org/10.6028/NIST.IR.8202

[29] Будзко В.И., Мельников Д.А. Информационная безопасность и блокчейн // Системы высокой доступности. 2018. Т. 14. № 3. с. 5–11.

[30] Будзко В.И., Мельников Д.А. Исторический ракурс технологии «Blockchain». «Всё новое – хорошо забытое старое» // Безопасность информационных технологий. 2018. Том 25, № 4. с. 23–33.

[31] Будзко В.И., Горбатов В.С., Жуков Ю.И. и Мельников Д.А. К вопросу универсальности технологии «Blockchain» // Проблемы информационной безопасности. Компьютерные системы. – 2019, №1, стр. 45-54. ISSN 2071-8217. URI: http://jisp.ru/o-zhurnale/arxiv-nomerov/.

[32] Глазьев С.Ю. Великая цифровая революция: вызовы и перспективы для экономики XXI века // Электронный ресурс, 14 сентября 2017 года. URI: https://glazev.ru/articles/6-jekonomika/54923-velikaja-tsifrovaja-revoljutsija-vyzovy-i-perspektivy-dlja-jekonomiki-i-veka.

[33] Асаул В.В., Михайлова А.О. Обеспечение информационной безопасности в условиях формирования цифровой экономики // Теория и практика сервиса: экономика, социальная сфера, технологии, № 4 (38). СПбГЭУ, Санкт-Петербург, 2018. С.5-9. URI: https://unecon.ru/sites/default/files/tips_438_2018.pdf. ISSN 2078-5852.

[34] Белл Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования/ Перевод с английского. Изд. 2-е, испр. и доп. – М.: Academia, 2004. CLXX. – С. 788. ISBN 5-87444-203-0.

[35] Кастельс М. Информационная эпоха: экономика, общество и культура: Пер. с англ. под науч. ред. О.И Шкаратана. – М.: ГУ ВШЭ, 2000. – С.608. ISBN 5-75-98-0069-8.

[36] Постановление Правительства Российской Федерации от 25 декабря 2007 года № 931 «О некоторых мерах по обеспечению информационного взаимодействия государственных органов и органов местного самоуправления при оказании государственных услуг гражданам и организациям». Собрание законодательства Российской Федерации, 2007, № 53, ст. 6627. URI: https://base.garant.ru/192518/.

[37] Мельников Д.А. Системы и сети передачи данных: Учебник. – М.: РадиоСофт, 2015. – С. 624. ISBN 978-5-93037-294-6.

[38] Мельников Д.А. Интернет. Информатизация. Иллюзии. // Статья в электронном журнале «Компьютерра», 2001, С. 8. URI: https://b-ok.global/book/3232362/57593a.

[39] Presidential Decision Directive «Public Encryption Management». 15 April 1993. URI: https://fas.org/irp/offdocs/pdd/pdd-5.pdf.

[40] Новикова А. Очередной «слив» от Сноудена: Спецслужбы США следили за гражданами с помощью соцсетей и GPS. // Комсомольская правда, 29 сентября 2013 года. URI: https://www.kp.ru/online/news/1547595/.

[41] Соловьева О. Доля цифрового криминала в России превысила 25%. Кибервымогателей ловить всё сложнее. // Независимая газета, 3 августа 2021 года. URI: https://www.ng.ru/economics/2021-08-03/1_8215_economics2.html.

[42] Токарева Н.Н. Об истории криптографии в России. // Прикладная дискретная математика, 2012, № 4(18), С. 82–107. URI: http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=pdm&paperid=391&option_lang=rus.

[43] Столпаков Б.В. Время создания первого отечественного учебного пособия по криптографии – 1633 год. // Открытое образование. М., 2012. №4. С.82-88. URI: https://cyberleninka.ru/article/n/vremya-sozdaniya-pervogo-otechestvennogo-uchebnogo-posobiya-po-kriptografii-1633-god.

[44] Грибанов Ю.И. Цифровая трансформация социально-экономических систем на основе развития института сервисной интеграции. Диссертация на соискание учёной степени доктора экономических наук, СПбГЭУ, Санкт-Петербург, 2019. URI: https://unecon.ru/sites/default/files/dissgribanovui.pdf.

[45] Днепровская Н.В. Исследование перехода предприятия к цифровой экономике // Вестник Российского экономического университета имени Г.В. Плеханова. – 2019. – № 4 (106). – С. 54-56. URI: https://doi.org/10.21686/2413-2829-2019-4-54-65.

[46] Будзко В.И., Мельников Д.А., Фомичёв В.М. Способы доставки ключей пользователям информационно-технологических систем высокой доступности на основе асимметричных криптографических методов // Системы высокой доступности. 2015. Т. 11. № 4. С. 32−44.

[47] Specification for the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197 November 26, 2001. URI: https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf.

[48] Diffie W., Hellman M.E. New Directions in Cryptography. // IEEE Trans. Inf. Theory / F. Kschischang – IEEE, 1976. – Vol. 22, Iss. 6. – P. 644-654. – ISSN 0018-9448; 1557-9654 – DOI:10.1109/TIT.1976.1055638

[49] Будзко В.И., Мельников Д.А., Фомичёв В.М. Способы согласования ключей пользователями информационно-технологических систем высокой доступности на основе асимметричных криптографических методов // Системы высокой доступности. 2015. Т. 11. № 4. С. 17−31.

[50] Yahalom R., Klein B., and Beth T. Trust relationships in secure systems – a distributed authentication perspective. In Proceedings of the 1993 IEEE Symposium on Research in Security and Privacy, p.p. 150-164, 1993.

[51] Yahalom R., Klein B., and Beth T. Trust-based navigation in distributed systems. Computing Systems, 7(1):45-73, 1994.

[52] Beth T., Borcherding M., and Klein B. Valuation of trust in open networks. In D. Gollmann, editor, ESORICS 94. Brighton, UK, November 1994.

[53] Denning D. A new paradigm for trusted systems. In Proceedings 1992-1993 ACM SIGSAC New Security Paradigms Workshop, p.p. 36-41, New York, NY, USA, 1993. ACM.

[54] EC. Information Technology Security Evaluation Criteria (ITSEC). The European Commission, 1992.

[55] USDoD. Trusted Computer System Evaluation Criteria (TCSEC). US Department of Defence, 1985.

[56] Simmons G. and Meadows C. The role of trust in information integrity protocols. Journal of Computer Security, 3(1):71-84, 1995.

[57] Campbell E., Safavi-Naini R., and Pleasants P. Partial belief and probabilistic reasoning in the analysis of secure protocols. In Proceedings. Computer Security Foundations Workshop V, p.p. 84-91. IEEE Comput. Soc. Press, Los Alamitos, CA, USA, 1992.

[58] Burrows M., Abadi M., and Needham R. A logic of authentication. Technical report, DEC Systems Research Center, February 1989. Research Report 39.

[59] Jøsang A. Artificial reasoning with subjective logic. In Abhaya Nayak and Maurice Pagnucco, editors, Proceedings of the 2nd Australian Workshop on Commonsense Reasoning, Perth, December 1997. Australian Computer Society.

[60] Jøsang A. A logic for uncertain probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 9(3):279–311, June 2001.

[61] Ismail R. and Jøsang A. The beta reputation system. In Proceedings of the 15th Bled Electronic Commerce Conference, June 2002.

[62] Pope S., Marsh S., and Jøsang A. Exploring different types of trust propagation. In K. Stølen, W.H. Winsborough, F. Martinelli, and F. Massacci, editors, Proceedings of the 4th International Conference on Trust Management (iTrust), volume 3986 of LNCS, p.p. 179–192. Springer, Berlin, 2006.

[63] Boyd C., Ismail R., and Jøsang A. A survey of trust and reputation systems for online service provision. Decision Support Systems, 43(2):618–644, 2007.

[64] Ažderska T., Marsh S., and Jøsang A. Trust transitivity and conditional belief reasoning. In T. Dimitrakos, R. Moona, D. Patel, and D.H. McKnight, editors, Proceedings of the 6th IFIP International Conference on Trust Management (IFIPTM 2012), volume 374 of IFIP Advances in Information and Communication Technology, p.p. 68–83. Springer, Berlin, 2012.

[65] Costa P.C.G., Blash E., and Jøsang A. Determining model correctness for situations of belief fusion. In Proceedings of the 16th International Conference on Information Fusion (FUSION 2013), p.p. 1225–1232. IEEE, Los Alamitos, 2013.

[66] McKnight D.H. and Chervany N.L. The Meanings of Trust. Technical Report MISRC Working Paper Series 96-04, University of Minnesota, Management Information Systems Research Center, 1996.

[67] Kant I. Kritik der praktischen Vernunft. 1788. Translated and edited by Lewis W. Beck, Critique of Practical Reason and Other Writings in Moral Philosophy. The University of Chicago Press, Chicago, 1949.

[68] ISO. «Evaluation Criteria for IT Security (Common Criteria)», documents N-2052, N-2053, N-2054. ISO/IEC JTC1/SC 27, May 1998.

[69] Laprie J. Dependability: Basic concepts and Terminology. Springer, 1992.

[70] de Finetti B. The value of studying subjective evaluations of probability. In C.-A. Staël von Holstein, editor, The concept of probability in psychological experiments, pages 1-14, Dordrecht, Holland, 1974. D.Reidel Pablishing Company.

[71] Marsh S. Formalising Trust as a Computational Concept. PhD thesis, University of Stirling, 1994.

[72] Gärdenfors P. and Sahlin N.-E. Unreliable probabilities, risk taking, and decision making. Synthese, 53(3):361–386, 1982.

[73] Sundgren D. and Karlsson A. Uncertainty levels of second-order probability. Polibits, 48:5–11, 2013.

[74] Ожегов С.И. Толковый словарь русского языка. Под ред. проф. Л.И. Скворцова. – 27-е изд., испр. – М.: АСТ, Мир и образование, 2013. – 1360 с.

[75] Dempster A. New Methods for Reasoning Towards Posterior Distributions Based on Sample Data. Annals Math. Stat. 37, 355-374, 1966.

[76] Shafer G. A Mathematical Theory of Evidence. Princeton University Press, 1976.

[77] Möbius A.F. Der barycentrische Calcul. Leipzig, 1827. Re-published by Georg Olms Verlag, Hildesheim, New York, 1976.

[78] Fitting M. Kleene's three-valued logics and their children. Fundamenta Informaticae, 20:113–131, 1994.

[79] Castelfranchi C. and Falcone R. Trust Theory: A Socio-cognitive and Computational Model. Wiley Series in Agent Technology. Wiley, New York, 2010.

[80] Falcone R. and Castelfranchi C. How trust enhances and spread trust. In Proceedings of the 4th Int. Workshop on Deception, Fraud and Trust in Agent Societies, in the 5th International Conference on Autonomous Agents (AGENTS'01), May 2001.

[81] Gambetta D. Can we trust trust? In D. Gambetta, editor, Trust: Making and Breaking Cooperative Relations, p.p. 213–238. Basil Blackwell. Oxford, 1990.

[82] ISO. ISO 31000:2009 – Risk Management Principles and Guidelines. International Organization for Standardization, 2009.

[83] Falcone R. and Castelfranchi C. Social trust: A cognitive approach. In C. Castelfranchi and Y.H. Tan, editors, Trust and Deception in Virtual Societies, p.p. 55–99. Kluwer, Dordrecht, 2001.

[84] Freeman L.C. Centrality in social networks. Social Networks, 1:215–239, 1979.

[85] Marsden P.V. and Lin N., editors. Social Structure and Network Analysis. Sage Publications, Beverly Hills, 1982.

[86] Tadelis S. Firm Reputation with Hidden Information. Economic Theory, 21(2):635–651, 2003.

[87] Christianson B. and Harbison W.S. Why isn't trust transitive? In M. Lomas, editor, Proceedings of the Security Protocols International Workshop, volume 1189 of LNCS, p.p. 171–176. Springer, Berlin, 1996.

[88] Pope S., and Jøsang A. Semantic constraints for trust transitivity. In S. Hartmann and M. Stumptner, editors, Proceedings of the Asia-Pacific Conference of Conceptual Modelling (APCCM) (Volume 43 of Conferences in Research and Practice in Information Technology), Newcastle, Australia, February 2005.

[89] Jøsang A. Categories of Belief Fusion. Journal of Advances in Information Fusion (JAIF), December 2018, Volume 13, Number 2, ISSN 1557-6418.

[90] Sensoy M., et al. Using subjective logic to handle uncertainty and conflicts. In Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, TRUSTCOM'12, p.p. 1323– 1326, Washington, DC, USA, 2012. IEEE Computer Society.

[91] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». URI: http://www.consultant.ru/document/cons_doc_LAW_61801/.

[92] ITU-T. Recommendation X.810, Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Overview (ISO/IEC 10181-1: 1996), 1995.

[93] ITU-T. Recommendation X.815, Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Integrity Framework (ISO/IEC 10181-6: 1996), 1995.

[94] ITU-T. Recommendation X.814, Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Confidentiality Framework (ISO/IEC 10181-5: 1996), 1995.

[95] ITU-T. Recommendation X.811, Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Authentication Framework (ISO/IEC 10181-2: 1996), 1995.

[96] ITU-T. Recommendation X.813, Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Non-repudiation Framework (ISO/IEC 10181-4: 1996), 1995.

[97] ITU-T. Recommendation X.500, Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services (ISO/IEC 9594-1, 2005), 2005.

[98] ITU-T. Recommendation X.501, Information technology – Open Systems Interconnection – The Directory: Models (ISO/IEC 9594-2, 2005), 2005.

[99] Sermersheim J. Lightweight Directory Access Protocol (LDAPv3): The Protocol, RFC 4511, June 2006. URI: https://www.rfc-editor.org/rfc/rfc4511.txt.

[100] ITU-T. Recommendation X.509, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks (ISO/IEC 9594-8, 2016), 2016.

[101] Zimmermann P. The Official PGP User's Guide. MIT Press, 1995.

[102] Lucas M.W. PGP & GPG: Email for the Practical Paranoid. No Starch Press Inc., 2006. ISBN: 978-1-59327-071-1.

[103] Callas J., Donnerhacke L., Finney H., Shaw D., and Thayer R. OpenPGP Message Format, RFC 4880, November 2007. URI: http://www.rfc-editor.org/rfc/rfc4880.txt.

[104] ITU-T. Recommendation X.509, The Directory: Authentication Framework, 1993.

[105] ITU-T. Recommendation X.500, Data Communication Network Directory, 1993.

[106] ITU-T. Recommendation X.509, The Directory: Abstract Service Definition (ISO/IEC 9594-3, 1995), 1993.

[107] ITU-T. Recommendation X.812, Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Access Control Framework (ISO/IEC 10181-3: 1996), 1995.

[108] Farrell S., Housley R. and Turner S. An Internet Attribute Certificate Profile for Authorization, RFC 5755, January 2010. URI: https://www.rfc-editor.org/rfc/rfc5755.txt.

[109] ITU-T. Recommendation X.810, Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Overview (ISO/IEC 10181-1: 1996), 1995.

[110] Мельников Д.А. Информационная безопасность открытых систем: Учебник. – М.: ФЛИНТА, Наука, 2013. – 448 с. ISBN 978-5-9765-1613-7.

[111] The Health Insurance Portability and Accountability Act of 1996. HIPAA; Pub. L. 104–191, 110 Stat. 1936, enacted August 21, 1996.

[112] The Government Paperwork Elimination Act. GPEA, Pub. L. 105-277, Approved October 21, 1998.

[113] Federal Public Key Infrastructure Policy Authority (FPKIPA). X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework. Version 1.31. February 8, 2019. URI: https://fpki.idmanagement.gov/.

[114] Santesson S. et al. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, RFC 6960, June 2013. URI: http://www.ietf.org/rfc/rfc6960.txt.

[115] European Telecommunications Standards Institute. ETSI TS 119 612 Electronic Signatures and Infrastructures (ESI); Trusted Lists, Technical Specification, V2.2.1, April 2016. URI: https:// www.etsi.org/deliver/etsi_ts/119600_119699/119612/02.02.01_60/ts_119612v020201p.pdf.

[116] Berners-Lee T. et al. Uniform Resource Identifier (URI): Generic Syntax, RFC 3986, January 2005. URI: http://www.ietf.org/rfc/rfc3986.txt.

[117] ISO 8601:2019: Date and time – Representations for information interchange. URI: https:// www.iso.org/obp/ui/#iso:std:iso:8601:-1:ed-1:v1:en.

[118] Phillips A., Davis M. Tags for Identifying Languages, RFC 5646, September 2009. URI: http://www.ietf.org/rfc/rfc5646.txt.

[119] ISO/IEC 10646:2017: Information technology – Universal Coded Character Set (UCS). URI: https://standards.iso.org/ittf/PubliclyAvailableStandards/c069119_ISO_IEC_10646_ 2017.zip.

[120] European Telecommunications Standards Institute. ETSI TS 102 853 Electronic Signatures and Infrastructures (ESI); Signature validation procedures and policies, Technical Specification, V1.1.2, October 2011. URI: https://www.etsi.org/deliver/etsi_ts/102800_102899/102853/01.01.02_60/ts_102853v010102p.pdf.

[121] Dalziel J., et al. Trust Requirements in Identity Management. Proceedings of the Australasian Information Security Workshop (AISW'05), Newcastle, Australia, January-February 2005. URI: https://folk.universitetetioslo.no/josang/papers/ JFHDP2005-AISW.pdf

[122] Pope S., and Jøsang A. User Centric Identity Management. Proceedings of AusCERT, Gold Coast, May 2005. URI: https://folk.universitetetioslo.no/josang/papers/JP2005-AusCERT.pdf.

[123] NIST. Electronic Authentication Guideline. NIST Special Publication SP 800-63, June 2004.

[124] US OMB. E-Authentication Guidance for Federal Agencies. Memorandum M-04-04 to the heads of all departments and agencies, US Office of Management and Budget, 16 December 2003.

[125] Cranor L. et al. The Platform for Privacy Principles 1.1 (P3P1.1) Specification. W3C, 2004. www.w3.org/TR/2004/WD-P3P11-20040427/.

[126] OASIS. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. Organization for the Advancement of Structured Information Standards, OASIS Standard, 15 March 2005.

[127] Liberty-Alliance. Liberty ID-FF Architecture Overview. Version: 1.2-errata-v1.0. URI: http://www.projectliberty.org/specs/liberty-idff-arch-overview-v1.2.pdf, 2003.

[128] Wong R., Berson T., and Feiertag R. Polonius: an identity authentication system. Proceedings of the 1985 IEEE Symposium on Security and Privacy, p.p. 101-107, 1985. URI: http://www.anagram.com/berson/abspolo.html.

[129] Mobile Electronic Transactions Ltd. Personal Transaction Protocol Version 1.0, Draft Specification 01-11-2002. MeT, 2002.

[130] Lannerstrom S. Mobile Authentication. Technical Report MPM 02:0041, SmartTrust/Sonera, 9 August 2002.

[131] Melnikov D.A., Jones A. «Masquerade» Attacks and a Process for Their Detection. In the Proceedings of the 3rd European Conference on Information Warfare and Security. – Royal Holloway University of London, UK. - 28-29 June 2004. – p.p. 269-278. URI: https://www. researchgate.net/publication/288280730_Masquerade_Attacks_and_the_process_of_their_ detection.

[132] Gieseke E. and McLaughlin J. Secure Web Authentication with Mobile Phones Using Keyed Hash Authentication. Technical report, Harward University, 11 January 2005.

[133] Мельников Д.А., Савельев М.С. Скрытые под маской// PCWeek. – 2005. - №6.

[134] Мельников Д.А. Организация и обеспечение безопасности информационно-технологических сетей и систем: Учебник. – М.: IDO Press, Университетская книга, 2012. ISBN 978-5-4243-0004-2.

[135] Rescorla E. «The Transport Layer Security (TLS) Protocol Version 1.3», RFC 8446, August 2018. URI: https://www.rfc-editor.org/rfc/rfc8446.txt.

[136] American National Standards Institute. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), ANSI ANS X9.62-2005, November 2005.

[137] Moriarty K. et al. PKCS #1: RSA Cryptography Specifications Version 2.2, RFC 8017, DOI 10.17487/RFC8017, November 2016, URI: https://www.rfc-editor.org/info/rfc8017.

[138] Josefsson S. and Liusvaara I. Edwards-Curve Digital Signature Algorithm (EdDSA), RFC 8032, DOI 10.17487/RFC8032, January 2017, URI: https://www.rfc-editor.org/info/rfc8032.

[139] Rescorla E., Korver B. «Guidelines for Writing RFC Text on Security Considerations», RFC 3552, DOI 10.17487/RFC3552, July 2003, URI: https://www.rfc-editor.org/info/rfc3552.

[140] Cheung E. et al. Web Security: The Emperors New Armour. In The Proceedings of the European Conference on Information Systems (ECIS2001), Bled, Slovenia, June 2001.

[141] Ho A., Povey. D, and Jøsang A. What You See is Not Always What You Sign. Proceedings of the Australian UNIX and Open Systems Users Group Conference (AUUG2002), Melbourne, September 2002.

[142] Kumar R., et al. Service Provider Authentication Assurance. 10th Annual Conference on Privacy, Security and Trust (PST 2012). Paris, July 2012.

[143] Гладких А. Россиян предупредили о мошеннических сайтах по продаже авиабилетов. // LIFE, 2020. URI: https://life.ru/p/1340555/.

[144] Вердина Н. Разводы-2019. Как мошенники обманывали россиян в этом году? // Аргументы и факты, 2019. URI: https://aif.ru/money/mymoney/razvody-019_kak_moshenniki_obmanyvali_rossiyan_v_etom_godu.

[145] Вахрушева Я. Развод чистой воды: Как обманывают мошенники в 2020 году? // Пятый канал, 2020. URI: https://www.5-tv.ru/news/284761/razvod-cistoj-vody-kak-obmanyvaut-mosenniki-v2020-godu/.

[146] Россиянка узнала о продаже своей квартиры из квитанции за услуги ЖКХ. // РИА Новости, 29.01.21. URI: https://ria.ru/20210129/kvitantsiya-1595122839.html.

[147] Melnikov D.A., et al. Concept for Increasing Security of National Information Technology Infrastructure and Private Clouds. Proceedings of the 5rd International Conference on Future Internet of Things and Cloud (FiCloud 2017). – 2017. – p.p. 155-160. DOI: 10.1109/ FiCloud. 2017.11. URI: https://ieeexplore.ieee.org/document/8114477.

[148] ISO 3166-1: 2020: Codes for the representation of names of countries and their subdivisions – Part 1: Country codes. URI: https://www.iso.org/standard/72482.html.

[149] Deering S., and Hinden R. IP Version 6 Addressing Architecture, RFC 4291, DOI 10.17487/ RFC4291, February 2006, URI: https://www.rfc-editor.org/info/rfc4291.

[150] Hinden R. Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, DOI 10.17487/ RFC2460, December 1998, URI: https://www.rfc-editor.org/info/rfc2460.

[151] 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.

[152] Microsoft. Microsoft Security Bulletin MS01-017 (March 22, 2001): Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard. URI: http://www.microsoft.com/technet/ security/bulletin/MS01-017.asp, 2001.

[153] UK e-Envoy. Registration and Authentication. UK Office of the e-Envoy, under the Cabinet Office, URI: http://e-government.cabinetoffice.gov.uk/assetRoot/04/00/09/60/04000 960.pdf, September 2002.

[154] Clarke D. et al. Certificate Chain Discovery in SPKI/SDSI. Journal of Computer Security, 2001, 9(4):285–322.

[155] 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.p. 306–313. CAUSA Proceedings, IEEE Computer Society, Palo Alto, June 17-19 1998.

[156] Soghoian C. and Stamm S. Certified lies: Detecting and defeating government interception attacks against SSL (short paper). In Financial Cryptography, p.p. 250–259, 2011.

[157] Mills E. Fraudulent Google certificate points to Internet attack. URI: http://news.cnet.com/, August 29, 2011.

[158] Shakarian P. Stuxnet: Cyberwar revolution in military affairs // Small Wars Journal, April 2011.

[159] Netcraft Ltd. Certification Services. Netcraft Report. URI: https://ssl.netcraft.com/ssl-sample-report/CMatch/certs, 2010.

[160] 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.

[161] Li N., Grosof B., and Feigenbaum J. Delegation Logic: A Logic Based Approach to Distributed Authorization. ACM Transactions on Information and System Security, 6(1):128–171, 2003.

[162] Blaze M. et al. The KeyNote Trust Management System Version 2, RFC 2704, September 1999. URI: http://www.ietf.org/rfc/rfc2704.txt.

[163] Bellovin S.M. Using the domain name system for system break-ins. In Proceedings of the Fifth Usenix Unix Security Symposium, 1995.

[164] Kaminsky D. Details. Dan Kaminsky's blog at dankaminsky.com. URI: http://dankaminsky.com/ 2008/07/24/details/, 24 July 2008.

[165] Arends R. et al. DNS Security Introduction and Requirements, RFC 4033, March 2005. URI: http://www.rfc-editor.org/rfc/rfc4033.txt.

[166] Hoffman P. and Schlyter J. The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA, RFC 6698, August 2012. URI: http://www.ietf.org/ rfc/rfc6698.txt.

[167] White R. A Look at the Current State of DNSSEC in the Wild // CircleID.com, September 06, 2018. URI: http://www.circleid.com/posts/20180906_a_look_at_current_state_of_dnssec_in_the_wild.

[168] Омельченко А. В. Теория графов. – М.: МЦНМО, 2018. – 416 с. ISBN 978-5-4439-1247-9.

[169] Duffin R.J. Topology of series-parallel networks. Journal of Mathematical Analysis and Applications, 10(2):303–313, 1965.

[170] Flocchini P. and Luccio F.L. Routing in series parallel networks. Theory of Computing Systems, 36(2):137–157, 2003.

[171] Park Y. On the optimality of trust network analysis with subjective logic. Advances in Electrical and Computer Engineering, 14(3):49–54, 2014.

[172] Проектный офис национальной программы «Цифровая экономика Российской Федерации» Аналитического центра при Правительстве Российской Федерации. На портале «Госуслуги» свыше ста миллионов зарегистрированных пользователей. 26 ноября 2019 года. URI: https://digital.ac.gov.ru/news/1621/.

[173] Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг». URI: http://www.consultant.ru/document/cons_doc_LAW_103023/.

[174] Постановление Правительства РФ от 22.12.2012 № 1376 «Об утверждении Правил организации деятельности многофункциональных центров предоставления государственных и муниципальных услуг». URI: http://www.consultant.ru/document/cons_doc_LAW_139747/.

[175] ISO/IEC 9834-1:2012 Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree – Part 1. URI: https://www.iso.org/obp/ui/#iso:std:iso-iec:9834:-1:ed-4:v1:en.

[176] ITU-T. Recommendation X.660: Information technology - Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree. URI: https://www.itu.int/rec/T-REC-X.660-201107-I/en.

[177] Hinden R., et al. IPv6 Global Unicast Address Format. RFC 3587, August 2003. URI: http:// www.ietf.org/rfc/rfc3587.txt.

[178] Hinden R., and Haberman B. Unique Local IPv6 Unicast Addresses. RFC 4193, October 2005. URI: http:// www.ietf.org/rfc/rfc4193.txt.

[179] Rekhter Y. et al. Address Allocation for Private Internets. RFC 1918, February 1996. URI: http:// www.ietf.org/rfc/rfc1918.txt.

[180] Encyclopedia of Cryptography and Security, Edited by Henk van Tilborg. Springer, USA, 2005, p. 740. ISBN-10: (eBook) 0-387-23483-7.

[181] Jones A., Melnikov D.A. Static Image Data Hiding and Encryption Method. Proceedings of the 3rd European Conference on Information Warfare and Security. – Royal Holloway University of London, UK. – 28-29 June 2004. – p.279. ISBN 0954709624, 9780954709624.

[182] Мельников Д.А. и др. К вопросу об использовании свойств логической характеристики IPv6-протокола в целях повышения уровня защищённости национальной информационно-технологической инфраструктуры Российской Федерации // Безопасность информационных технологий. – 2014. – №1. с. 30-35.

[183] Будзко В.И., Мельников Д.А., Фомичёв В.М. Протоколы обеспечения ключами пользователей информационно-технологических систем высокой доступности с использованием симметричной криптографии // Системы высокой доступности. 2014. Т. 10. № 3. С. 36−51.

[184] Мельников Д.А. и др. Криптографический способ документирования покадровых изображений. Научная визуализация. – 2016. – Том №8 - №4. (Эл. журнал). С. 13-25. URI: https://sv-journal.org/2016-5/02.php?lang=ru.

[185] Melnikov D.A., et al. Analysis of the level of security provided by advanced information and communication technologies. 2019 Actual Problems of Systems and Software Engineering (APSSE 2019). 2019, BMS Part Number: CFP19T94-ART, pp. 29-34. ISBN: 978-1-7281-6062-7. URI: https://dx.doi.org/10.1109/APSSE47353.2019.00010.

[186] Мельников Д.А. К вопросу обнаружения атак типа «Маскарад». Экономика, статистика и информатика. – 2010. – № 1. – С. 127-133.

[187] Мельников Д.А. и др. Обнаружение уязвимостей информационно-технологических систем на основе анализа сетевого трафика // Безопасность информационных технологий. – 2013 – Т.20, №4. С. 83-87.

[188] Melnikov D.A., et al. IPv6-protocol the logical characteristic used to increase the security level of national information technology infrastructures. In the Proceedings of the International Conference on eBusiness, eCommerce, eManagement, eLearning and eGovernance (IC5E 2014). - University of Greenwich, London, UK. - 30-31 July 2014. – p.p.15-20. URI: https://archive.org/details/ic5e2014/ic5e2014002/page/n5/mode/2up.

[189] Мельников Д.А. и др. Использование логической характеристики IPv6-протокола для защиты IT инфраструктуры // Информационная безопасность банков (BIS Journal). – 2014. - №1(12). URI: https://ib-bank.ru/bisjournal/post/296.

[190] Melnikov D.A., et al. Access Control Mechanism Based On Entity Authentication With IPv6 Header «Flow Label» Field. In the Proceedings of the 3rd International Conference on Future Internet of Things and Cloud (FiCloud 2015). – 2015. – p.p. 158-164. DOI: 10.1109/ FiCloud. 2015.41. URI: https://ieeexplore.ieee.org/document/7300813.

[191] Melnikov D.A., et al. Cybertrust in e-Learning Environment based on Network Time Synchronization. In the Proceedings of the 8th International Conference on Computer Supported Education (CSEDU 2016) – Volume 2, p.p. 402-407. ISBN: 978-989-758-179-3. URI: https:// dblp.org/rec/conf/csedu/MelnikovPMDK16.html.

[192] Будзко В.И., Мельников Д.А., Фомичёв В.М. Базовые требования к подсистемам обеспечения криптоключами в информационно-технологических системах высокой доступности // Системы высокой доступности. – 2016. Т.12, № 3. С. 73-81.

[193] Будзко В.И., Мельников Д.А., Фомичёв В.М. Политики безопасности в подсистемах обеспечения криптоключами информационно-технологических систем высокой доступности // Системы высокой доступности. – 2016. Т.12, № 3. С. 82-90.

[194] Будзко В.И., Мельников Д.А., Фомичёв В.М. Способ управления доступом к системе обработки больших данных на основе использования маркера потока в заголовке IP-пакета шестой версии // Системы высокой доступности. – 2017. Т. 13. № 4. С. 39-48.

[195] Мельников Д.А. и др. К вопросу о цели и задачах национальной образовательной инициативы США в области кибербезопасности // Безопасность информационных технологий. – 2018. – №2. С. 23-37.

[196] Melnikov D.A., et al. Architecture solutions for the metadata extraction toolkit, taking into account the built-in privacy extracts. CEUR Workshop Proceedings, Vol-2514, 2019, p.p. 3-9. ISSN 1613-0073. URI: http://ceur-ws.org/Vol-2514/.

[197] Будзко В.И., Мельников Д.А., Фомичёв В.М. Основы организации обеспечения информационной безопасности и киберустойчивости в централизованных информационно-телекоммуникационных системах высокой доступности. // Системы высокой доступности. – 2019. Т. 15. № 1. С. 70-77.

[198] Мельников Д.А. и др. Реализация способа защиты неподвижных изображений в «квантовом мире». // Безопасность информационных технологий. – 2019. – №2, С. 21-43. ISSN: 2074-7136. http://dx.doi.org/10.26583/bit.2019.2.02.

[199] Melnikov D.A., et al. About the cybersecurity of automated process control systems. Procedia Computer Science. 2020 Annual International Conference on Brain-Inspired Cognitive Architectures for Artificial Intelligence: Eleventh Annual Meeting of the BICA Society, Edited by Alexei V. Samsonovich, Valentin V. Klimov, Volume 190, Pages 1-868 (2021), p.p. 217-225. ISSN: 1877-0509. https://www.sciencedirect.com/science/article/pii/ S1877050921012709.

[200] Мельников Д.А. О проблеме доверия к удостоверяющим центрам в Российской Федерации. // Системы высокой доступности. – 2022. Т. 18. № 1. С. 5-15. DOI: https://doi.org/10. 18127/j20729472-202201-01.

[201] Мельников Д.А. К вопросу распознавания мошеннических Web-сайтов. // Системы высокой доступности. – 2022. Т. 18. № 1. С. 16-25. DOI: https://doi.org/10. 18127/j20729472-202201-02.

Приложение 1

О государственном регулировании в области шифрования информации

(Директива президента США от 15 (16) апреля 1993 года)

Президент США утвердил директиву «О государственном регулировании в области шифрования информации». Директива предусматривает следующее.

Современные системы информационного обмена и доступные коммерческие криптографические системы являются частью стремительно развивающихся новых компьютерных и телекоммуникационных технологий. Криптографические системы шифруют информацию с целью обеспечения неприкосновенности информационного обмена и данных на основе предотвращения несанкционированного доступа. Современные телекоммуникационные системы используют цифровые технологии с целью быстрой и качественной обработки больших объёмов данных, которые транслируются во время процедур информационного обмена. Такие новейшие телекоммуникационные системы интегрированы в инфраструктуру, которая необходима для обеспечения гарантий экономической конкурентоспособности в эпоху информатизации.

Несмотря на свои преимущества, новые технологии электронного информационного взаимодействия могут также препятствовать законному ведению государством электронной разведки. Передовые криптографические системы могут негативно воздействовать на деятельность федеральных органов власти США. Когда такие системы вывозятся за границу, их можно использовать для воспрепятствования деятельности органов внешней разведки, имеющей решающее значение для наших национальных интересов. Раньше правительство было способно вести электронную разведку с целью обеспечения законных интересов правоохранительных органов и национальной безопасности, и одновременно с этим обеспечивало неприкосновенность частной жизни и защиту гражданских свобод всех граждан. Теперь, в условиях совершенствования криптографических методов и технологий защиты информации, потребуются новые инновационные способы и решения.

В области шифрованной связи, правительством США разработана микросхема, которая не только обеспечивает неприкосновенность данных за счёт их шифрования, являющегося существенно более надёжным, чем текущий государственный стандарт, но также позволяет хранить ключи, необходимые для расшифрования. Система хранения ключей позволит правительству получить доступ к зашифрованной информации только на основе соответствующих законных полномочий.

Для оказания помощи правоохранительным органам и другим государственным ведомствам при добывании и расшифровке ими информации, передаваемой в электронном виде, на основании санкций уполномоченных органов, настоящим я предписываю следующее:

Внедрение микросхем, разработанных правительством

Генеральный прокурор США или его представитель должны обратиться к производителям телекоммуникационных программно-аппаратных комплексов и соответствующего оборудования, включающих подсистемы шифрования, с просьбой установить в своих изделиях разработанные правительством США микросхемы для хранения ключей. Факты доступа правоохранительных органов к хранящимся ключам не будут скрыты от американской общественности. Должны быть приняты все необходимые меры по обеспечению полной доступности любых существующих или будущих версий микросхемы хранения ключей для американских производителей телекоммуникационных программно-аппаратных комплексов и соответствующего оборудования с целью обеспечения гарантированной защиты системы хранения ключей. Принимая это решение, я не намерен препятствовать развитию частного сектора или одобрению правительством других микросхем или алгоритмов, которые одинаково эффективны для обеспечения неприкосновенности и защищённости системы хранения ключей.

Хранение ключей

Генеральный прокурор должен заключить все необходимые соглашения с соответствующими организациями о размещении ключей в микросхемах для хранения ключей, которые встроены в телекоммуникационные программно-аппаратные комплексы и соответствующее оборудование. В каждом случае, владелец (держатель) ключа должен согласиться строго выполнять процедуры обеспечения безопасности с целью предотвращения несанкционированного формирования ключей. Ключи должны передаваться только тем правительственным ведомствам, которым были предоставлены (или которые обладают) соответствующие(ими) полномочия(ми) для получения содержания тех сообщений, которые транслировались в течение информационного обмена и были зашифрованы устройствами, содержащими микросхемы. Генеральный прокурор проверяет обоснованность юридических процедур и нормативных правовых актов, на основании которых ведомство определяет свои (или ведомству предоставляются) полномочия для получения содержания таких сообщений.

Приобретение и использование средств шифрования

Министр торговли по результатам консультаций с другими соответствующими ведомствами США должен начать процесс разработки и написания стандарта с целью упрощения процедур приобретения и использования средств шифрования, оснащённых микросхемами для хранения ключей, в федеральных системах связи, которые обрабатывают уязвимую, но неклассифицированную информацию. Я полагаю, что этот процесс будет идти по графику, который позволит обнародовать окончательный стандарт по окончании шести месяцев после опубликования данной директивы.

Генеральный прокурор будет утверждать приобретение и применение устройств шифрования в том объёме, который необходим для обеспечения деятельности правительства по законному ведению электронной разведки и удовлетворения потребностей правоохранительных органов в защищённых системах связи. Кроме того, для осуществления указанного приобретения генеральный прокурор будет использовать средства из фонда дополнительных средств, полученных за счёт конфискации криминальных активов, министерства юстиции.

20321

THE WHITE HOUSE

WASHINGTON

April 15, 1993

PRESIDENTIAL DECISION DIRECTIVE/NSC-5

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF COMMERCE
THE DIRECTOR OF THE OFFICE OF MANAGEMENT & BUDGET
THE ASSISTANT TO THE PRESIDENT FOR ECONOMIC POLICY
THE DIRECTOR OF CENTRAL INTELLIGENCE
THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
THE DIRECTOR OF THE NATIONAL SECURITY AGENCY

SUBJECT: Public Encryption Management

Advanced telecommunications and commercially available encryption are part of a wave of new computer and communications technology. Encryption products scramble information to protect the privacy of communications and data by preventing unauthorized access. Advanced telecommunications systems use digital technology to rapidly and precisely handle a high volume of communications. These advanced telecommunications systems are integral to the infrastructure needed to ensure econ[illegible]titiveness in the

PROCUREMENT AND USE OF [illegible]ION DEVICES

The Secretary of Commerce, in consultation with other appropriate U.S. agencies, shall initiate a process to write standards to facilitate the procurement and use of encryption devices fitted with key-escrow microcircuits in federal communications systems that process sensitive but unclassified information. I expect this process to proceed on a schedule that will permit promulgation of a final standard within six months of this directive.

The Attorney General will procure and utilize encryption devices to the extent needed to preserve the government's ability to conduct lawful electronic surveillance and to fulfill the need for secure law enforcement communications. Further, the Attorney General shall utilize funds from the Department of Justice Asset Forfeiture Super Surplus Fund to effect this purchase.

William J. Clinton

William J. Clinton

Приложение 2

Операторы, используемые в СЛ

Ниже представлена таблица, в которой содержатся используемые в СЛ операторы и их описание, а также показано сравнение с операторами, используемыми в двоичной логике (ДЛ).

Таблица П.2 – Сравнение операторов, используемых в субъективной и двоичной логиках

Оператор СЛ	**Символ**	**Оператор ДЛ**	**Символ**	**Обозначение в СЛ**
Сложение	$+$	Объединение	$\cup$	$\omega_{x\cup y} = \omega_x + \omega_y$
Вычитание	$-$	Разность	$\setminus$	$\omega_{x\setminus y} = \omega_x - \omega_y$
Дополнение	$\neg$	NOT (Отрицание)	$\bar{x}$	$\omega_{\bar{x}} = \neg\omega_x$
Умножение	$\cdot$	AND (Конъюнкция)	$\wedge$	$\omega_{x\wedge y} = \omega_x \cdot \omega_y$
Коумножение	$\sqcup$	OR (Дизъюнкция)	$\vee$	$\omega_{x\vee y} = \omega_x \sqcup \omega_y$
Деление	$/$	UN-AND (Неконъюнкция)	$\widetilde{\wedge}$	$\omega_{x\widetilde{\wedge}y} = \omega_x / \omega_y$
Коделение	$\widetilde{\sqcup}$	UN-OR (Недизъюнкция)	$\widetilde{\vee}$	$\omega_{x\widetilde{\vee}y} = \omega_x \widetilde{\sqcup} \omega_y$
Полиномиальное произведение	$\cdot$	Декартово произведение	$\times$	$\omega_{XY} = \omega_X \cdot \omega_Y$
Дедукция	$\circledcirc$	Условный конструктивный силлогизм	$\Vert$	$\omega_{Y\Vert X} = \omega_X \circledcirc \boldsymbol{\omega}_{Y\vert X}$
Абдукция (обратная дедукция)	$\widetilde{\circledcirc}$	Условный деструктивный силлогизм	$\widetilde{\Vert}$	$\omega_{X\widetilde{\Vert}Y} = \omega_Y \widetilde{\circledcirc} \left(\boldsymbol{\omega}_{Y\vert X}, \boldsymbol{a}_X\right)$
Теорема Байеса	$\widetilde{\phi}$	Противопоставление	$\tilde{\mid}$	$\omega_{X\tilde{\Vert}Y} = \widetilde{\Phi}\left(\boldsymbol{\omega}_{Y\vert X}, \boldsymbol{a}_X\right)$
Объединённые мнения	$\cdot$	Декартово произведение	$\times$	$\omega_{YX} = \boldsymbol{\omega}_{Y\vert X} \cdot \omega_X$
Ограниченное слияние	$\odot$	–	&	$\omega_X^{A\&B} = \omega_X^A \odot \omega_X^B$
Суммарное слияние	$\oplus$	–	$\diamond$	$\omega_X^{A\diamond B} = \omega_X^A \oplus \omega_X^B$
Усреднённое слияние	$\underline{\oplus}$	–	$\underline{\diamond}$	$\omega_X^{A\underline{\diamond}B} = \omega_X^A \underline{\oplus} \omega_X^B$
Взвешенное слияние	$\widehat{\oplus}$	–	$\hat{\diamond}$	$\omega_X^{A\hat{\diamond}B} = \omega_X^A \widehat{\oplus} \omega_X^B$
Компромиссное слияние	ⓒⓒ	–	♥	$\omega_X^{A\heartsuit B} = \omega_X^A$ ⓒⓒ ω_X^B
Неслияние	$\ominus$	–	$\overline{\diamond}$	$\omega_X^{A\bar{\diamond}B} = \omega_X^A \ominus \omega_X^B$
Понижение доверия	$\otimes$	Транзитивность доверия	:	$\omega_X^{[A;B]} = \omega_X^A \otimes \omega_X^B$

Приложение 3

Акты внедрения/использования полученных результатов

Акционерное общество «Газпромбанк»

ГАЗПРОМБАНК

«Газпромбанк»
(Акционерное общество)
Банк ГПБ (АО)
ОКПО/БИК 09807684/044525823
ИНН/КПП 7744001497/997950001
ОГРН 1027700167110
117420, г. Москва, ул. Наметкина, д. 16, корпус 1
ТЕЛЕФОН: +7 (495) 719-1763
ФАКС: +7 (495) 913-7319
S.W.I.F.T.: GAZPRUMM
ТЕЛЕКС: 412027 GAZ RU
www.gazprombank.ru

25.03.2021 № 13-727

На № _____ от _____

Для предоставления в
диссертационный совет
Д 002.073.02 при ФИЦ ИУ РАН

119333, Москва, Вавилова, 44/2

Об использовании научных
результатов диссертации Д.А. Мельникова

Уважаемый диссертационный совет!

Блоком безопасности Банка ГПБ (АО) были изучены результаты диссертации Д.А. Мельникова на соискание учёной степени доктора технических наук на тему «Методы и средства построения системы управления криптографической защитой на основе инфраструктуры открытых ключей для широкомасштабных информационно-телекоммуникационных систем».

Так, представленные в работе научные и практические результаты обладают научной новизной и оригинальностью, что позволит решить многие проблемы обеспечения безопасности в сети Интернет не только для граждан РФ, но и для развивающейся цифровой экономики на территории России.

Представленные в диссертации способы распознавания поддельных (мошеннических) Web-сайтов были всесторонне проанализированы работниками Департамента, их использование при разработке перспективных комплексов программного обеспечения в интересах обеспечения безопасности будет рассмотрено совместно с профильными подразделениями Банка.

Вместе с этим, подтверждаем существующую проблематику доверия в инфраструктуре открытых ключей РФ и отмечаем необходимость её модернизации.

Начальник Департамента Банка ГПБ (АО) Е.М. Монисов

С.Д. Арестов
(495) 287-61-00, вн. 2-9652

Акционерное общество «Научно-технический и сертификационный центр по комплексной защите информации» (входит в Госкорпорацию «РОСАТОМ»)

АТОМЗАЩИТАИНФОРМ
РОСАТОМ

Акционерное общество
«Научно-технический
и сертификационный центр
по комплексной защите информации»
(АО Центр «Атомзащитаинформ»)

Большая Ордынка, д.24,
Москва, 119017
Телефон (499) 949-46-33, факс (499) 949-48-68
E-mail: VVAgafonkina@rosatom.ru
ОКПО 36931085, ОГРН 1197746219747
ИНН 7706469319, КПП 770601001

03.03.2021 № 2/9-127

На № _____ от _____

Для предоставления в диссертационный совет Д 002.073.02 при ФИЦ ИУ РАН

УТВЕРЖДАЮ

Заместитель генерального директора

_____ А.В. Клименко

Акт внедрения

АКТ

о внедрении (использовании) результатов диссертационного исследования Мельникова Дмитрия Анатольевича на тему: «Методы и средства построения систем управления криптографической защитой на основе инфраструктуры открытых ключей для широкомасштабных информационно-телекоммуникационных сетей»

Комиссия в составе:
Председатель: Тимонин Виталий Альбертович - начальник отдела;
Члены: Егоров Сергей Николаевич – главный специалист;
Шеин Анатолий Васильевич – главный специалист

настоящим Актом удостоверяет, что всесторонне проанализировала научные результаты диссертации Д.А. Мельникова на соискание учёной степени доктора технических наук и приняла решение о целесообразности внедрения (использования) в деятельности АО Центр «Атомзащитаинформ» отдельных научных и практических результатов, в частности, модель национальной системы доверия и способы предотвращения выпуска фальсифицированных сертификатов открытых ключей, по направлениям разработки способов и средств электронной подписи и систем контроля и ограничения доступа.

Следует отметить, что большинство научных и практических результатов, полученных Д.А. Мельниковым, обладают научной новизной и оригинальностью, что позволит решить многие проблемы обеспечения безопасности цифровой экономики Российской Федерации.

Председатель: _____ В.А. Тимонин

Члены: _____ С.Н. Егоров

_____ А.В. Шеин

Общество с ограниченной ответственность «Код безопасности»

115127, Россия, Москва а/я 66
+7 (495) 982-30-20
info@securitycode.ru
www.securitycode.ru

Для предоставления в
диссертационный совет
Д 002.073.02 при ФИЦ ИУ РАН
119333, Москва, Вавилова, 44/2

А К Т
о внедрении (использовании) результатов диссертационного исследования Мельникова Дмитрия Анатольевича на тему: «Методы и средства построения системы управления криптографической защитой на основе инфраструктуры открытых ключей для широкомасштабных информационно-телекоммуникационных систем»

Комиссия ООО «Код Безопасности» в составе:

Председатель: Задорожный Д.И., *руководитель Службы сертификации, ИБ и криптографии*;

Члены: Фомичев В.М., *научный консультант Службы сертификации, ИБ и криптографии*;
Коренева А.М., *начальник отдела криптографического анализа Службы сертификации, ИБ и криптографии*

настоящим Актом удостоверяет, что научные результаты диссертации Д.А. Мельникова на соискание учёной степени доктора технических наук, относящиеся к вопросам защиты от фальсифицированных сертификатов открытых ключей, использованы в деятельности компании ООО «Код Безопасности» при построении математической модели системы доверия к сертификатам открытых ключей, составляющей основу для разработки перспективных отечественных средств защиты информации по направлениям разработки способов и средств электронной подписи, а также систем контроля и ограничения доступа к базам данных информационных систем.

Комиссия:
Председатель: _____ (Задорожный Д.И.)
(подпись)

Члены: _____ (Фомичев В.М.)
(подпись)

_____ (Коренева А.М.)
(подпись)

«УТВЕРЖДАЮ»
Генеральный директор
ООО «Код Безопасности»:

_____ А.В. Голов
(подпись)

«Код Безопасности» Общество с ограниченной ответственностью ОГРН 5087746212241 г. Москва

___.___.2021 г.

Открытое акционерной общество Фирма «АНКАД»

Для предоставления
в диссертационный совет
Д 002.073.02 при ФИЦ ИУ РАН

119333, Москва, Вавилова, 44/2

А К Т

о внедрении (использовании) результатов диссертационного исследования Мельникова Дмитрия Анатольевича на тему: «Методы и средства построения системы управления криптографической защитой на основе инфраструктуры открытых ключей для широкомасштабных информационно-телекоммуникационных систем»

Комиссия в составе:

Председатель: Дударев Д. А., исполнительный директор, к. т. н.

Члены: Панасенко С. П., заместитель генерального директора, к. т. н.;

Мазуркин Н. С., криптограф, к. т. н.

Настоящим Актом удостоверяет, что комиссия всесторонне изучила научные результаты диссертации Д. А. Мельникова на соискание учёной степени доктора технических наук и приняла решение о целесообразности использования в деятельности ООО Фирма «АНКАД» отдельных научных и практических результатов. В частности, разработанные автором диссертации алгоритмы определения обоснованности (законности) выпуска сертификата открытого ключа и способ обнаружения злонамеренных провайдеров электронных услуг могут быть использованы при разработке архитектуры программных средств электронной подписи, шифрования и аутентификации субъектов информационного взаимодействия на основе асимметричных ключевых схем.

Следует также отметить, что большинство научных и практических результатов, полученных Д. А. Мельниковым, обладают научной новизной и оригинальностью и имеют практическую ценность; их применение позволит значительно повысить уровень информационной безопасности цифровой экономики Российской Федерации.

Комиссия:
Председатель: _____ Д. А. Дударев

Члены: _____ С. П. Панасенко

_____ Н. С. Мазуркин

22.11.2021 г.

«УТВЕРЖДАЮ»
Генеральный директор
ООО Фирма «АНКАД»

_____ Ю. В. Романец

М.П.

ООО Фирма «АНКАД», ИНН 7735081665, КПП 773501001, ОГРН 1027739013356,
124527 г. Москва, г. Зеленоград, Солнечная аллея, дом 8, Фирма «АНКАД»
Тел. +7 (499) 731-0000, +7 (499) 731-2050. Факс: +7 (499) 731-2060.
E-mail: marketing@ancud.ru
www.ancud.ru

МАСКОМ
УЧЕБНЫЙ ЦЕНТР
НОУ ДПО "УЦБИ "МАСКОМ"
Г. МОСКВА, СТАРОКАЛУЖСКОЕ ШОССЕ, Д. 62, СТР. 1, 117630
+7 (495) 136-40-10 (доб.1310), +7 (495) 136-40-20 (доб.1310)
MASCOM-UC@MASCOM-UC.RU, WWW.MASCOM-UC.RU
ОГРН 1047796070596 ИНН 7729503196/КПП 772901001

_____ №_____

На №_____ от_____

Для предоставления в диссертационный совет Д 002.073.02 при ФИЦ ИУ РАН
119333, Москва, Вавилова, 44/2

«УТВЕРЖДАЮ»
Директор НОУ ДПО
«УЦБИ «МАСКОМ»
_____М.И. Лобанов
(подпись)

А К Т

о внедрении (использовании) результатов диссертационного исследования Мельникова Дмитрия Анатольевича на тему: «Методы и средства построения системы управления криптографической защитой на основе инфраструктуры открытых ключей для широкомасштабных информационно-телекоммуникационных систем»

Комиссия в составе:

Председатель: Васильев А.А. – заместитель директора;

Члены: Лобашев А.К. – заведующий кафедрой технической защиты информации и защиты государственной тайны;

Позднякова А.С. – заместитель директора по учебной работе

настоящим Актом удостоверяет, что комиссия внимательно и всесторонне изучила научно-технические и практические результаты диссертации Д.А. Мельникова на соискание учёной степени доктора технических наук и приняла решение о целесообразности внедрения (использования) некоторых из них в деятельности отдельных структурных подразделений ГК «МАСКОМ». В частности, элементы синтезированной системы управления криптографической защиты (системы доверия) и способы предотвращения выпуска фальсифицированных сертификатов открытых ключей были использованы в деятельности Учебного центра при реализации учебного курса по программе «ПМ 1. Профессиональная переподготовка по направлению «Информационная безопасность» и при разработке комплекса программного обеспечения «…», используемого в СКУД. Также, представленные работе современные модели инфраструктур открытых ключей и базирующихся на них системы доверия включены в курс по программе повышения квалификации «М 7.0. Криптографическая защита информации в организации НОУ УЦБИ «МАСКОМ».

Вместе с этим следует отметить, что полученные Д.А. Мельниковым научно-технические и практические результаты, обладают научной новизной и оригинальностью, а их реализация позволит решить многие проблемы защиты прав и законных интересов граждан, бизнеса и государства от угроз ИБ.

Комиссия:

Председатель: _____ А.А. Васильев (подпись)

Члены: _____ А.К. Лобашев (подпись)

_____ А.С. Позднякова (подпись)

« 15 » сентября 2021г.