Е. В. Ничипорчук
Московский инженерно-физический институт (государственный университет)

АРХИТЕКТУРНАЯ МОДЕЛЬ СИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ПЛАНИРОВАНИЯ ПОТОКОВ ЗАДАНИЙ

В статье представлена архитектурная модель системы криптографической защиты информации на основе планирования потоков заданий. В качестве примера приводится алгоритм решения системой задачи честного обмена цифровыми подписями.

Понятие планирования потоков заданий (secure cryptographic workflow) используется для описания криптографической системы, в которой действия должны быть выполнены в определенном порядке и при наступлении определенных условий. В системе криптографической защиты информации на основе планирования потоков заданий (СКЗИППЗ) это достигается установлением расшифрования в качестве привилегированного действия, которое может быть выполнено пользователями, обладающими определенным набором мандатов [1]. Отправитель шифрованного сообщения определяет в политике мандаты, которые должен иметь получатель сообщения для его расшифрования. У отправителя должна быть возможность выполнить зашифрование без знания того, какие мандаты получатель имеет в настоящее время. Мандаты выпускаются совокупностью центров доверия (ЦД), которые могут гарантировать, что некоторое действие будет выполнено или что некоторое событие произойдет до того, как мандаты будут предоставлены пользователям. ЦД, вступившие в сговор, не смогут расшифровать сообщение за счет использования открытого шифрования [2].

В последние годы актуальным стал вопрос создания средств массового выполнения криптографических операций в типовых задачах электронной коммерции при условии обеспечения многосторонней безопасности участников электронного взаимодействия, а также унификации средств обеспечения безопасности информации в разнородных задачах электронной коммерции и электронного документооборота.

СКЗИППЗ может быть использована в тех применениях, где требуется координация действий участников системы и назначение полномочий, в частности, в качестве универсальной системы для решения типовых задач электронной коммерции, а именно: равноправного обмена данными, электронных аукционов, электронных выборов [3] и др.

При построении СКЗИППЗ используются следующие криптографические примитивы: схема открытого шифрования, механизм инкапсуляции данных, схема идентификационного шифрования, схема разделения секрета, схема одноразовой подписи. Механизм инкапсуляции данных является схемой одноразового зашифрования с секретным ключом, где симметричный ключ используется для зашифрования единственного сообщения [2].

Приведём схему функционирования криптосистемы на основе планирования потоков заданий (Рис. 1). При построении криптосистемы на основе планирования потоков заданий участвует криптосистема с инфраструктурой открытых ключей (ИОК) и идентификационная криптосистема. При введении в систему каждого участника — возьмем для примера участника B — он должен пройти процедуру регистрации в криптосистеме с ИОК. Для этого он контактирует с удостоверяющим центром (УЦ), чтобы зарегистрировать свой открытый ключ P_B и получить от него так называемый сертификат своего открытого ключа $cert_B$. УЦ должен проверить представленные ему учетные данные, а также знание секретного ключа S_B, соответствующего представленному для регистрации открытому ключу. Чтобы зашифровать сообщение с помощью криптосистемы на основе планирования потоков заданий необходимо получить сертификат открытого ключа другого участника — возьмем для примера A —

для схемы открытого шифрования, обратившись в хранилище сертификатов или непосредственно к пользователю. Полученный сертификат подвергается проверке на действительность. С помощью открытого мастер-ключа ЦД отправитель шифрованного сообщения B создает политику и определяет в ней мандаты, которые должен иметь получатель сообщения A для его расшифрования.

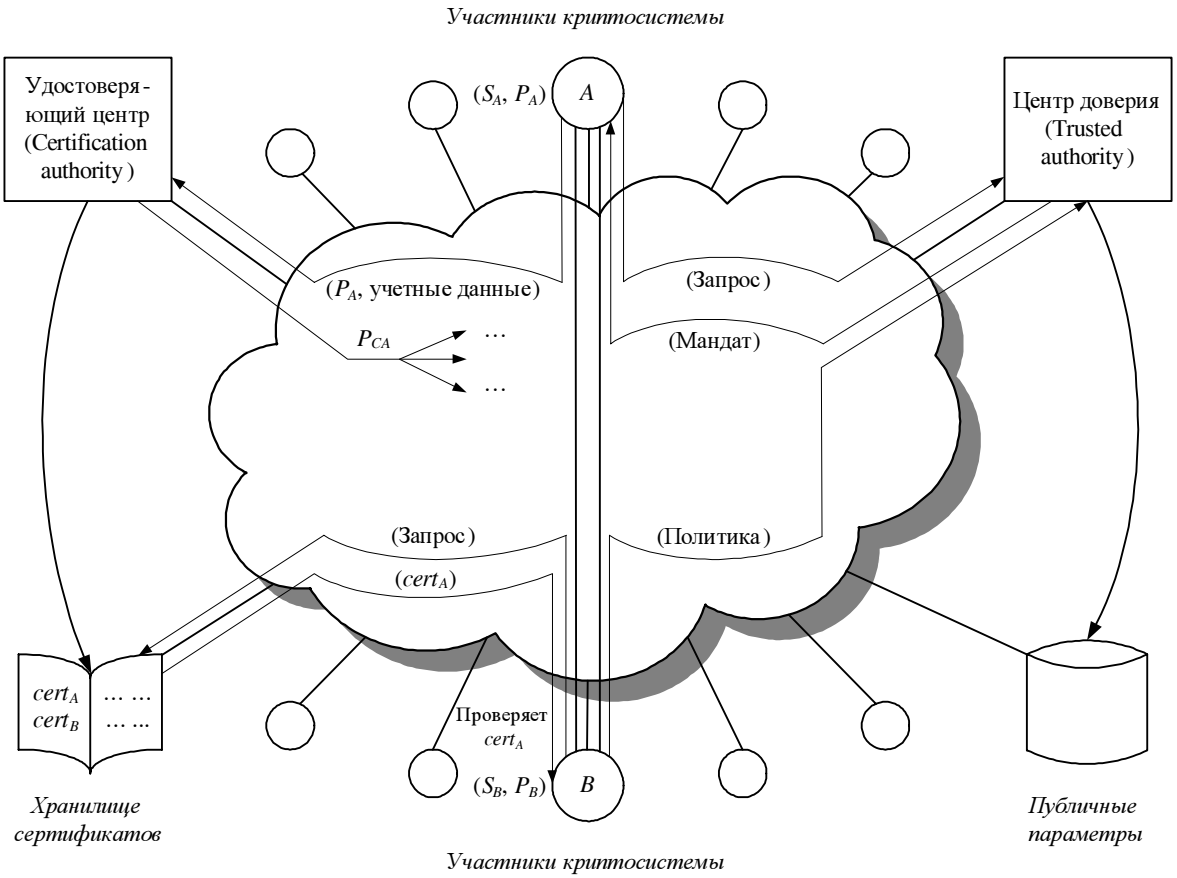

Рис. 1. Схема функционирования криптосистемы на основе планирования потоков заданий

Отправитель имеет возможность выполнить зашифрование без знания того, какие мандаты получатель имеет в настоящее время. После получения шифрованного сообщения пользователь обращается в ЦД для доказательства удовлетворения требованиям политики. При положительном результате проверки ЦД выпускают мандаты, которые могут гарантировать, что некоторое действие было выполнено или что некоторое событие произошло до того, как мандаты были предоставлены пользователям.

Определена совокупность требований к проектируемой системе:

· Система должна соответствовать общепринятым концепциям организации открытых информационных систем (переносимость, способность к взаимодействию, масштабируемость, управляемость и др.), международным стандартам по распределённой обработке данных и моделям защиты информации.

· СКЗИППЗ должна функционировать в среде корпоративной компьютерной сети, должна обеспечивать достаточные возможности управления защитой, контроля и учёта использования ресурсов, требовать минимального количества «ручных» операций по обслуживанию и настройке. Вместе с тем функционирование системы в среде корпоративной компьютерной сети подразумевает ряд условий, более благоприятных по сравнению с глобальными сетями: наличие единого центра административного управления; достаточно высокая пропускная способность каналов связи и достаточно высокие вычислительные возможности серверов, обслуживающих пользователей; постоянная возможность передачи данных между узлами в режиме реального времени; наличие персонала, ответственного за

оперативно-диспетчерское управление информационной системой предприятия; синхронизация системных часов узлов (что обеспечивается сервисом времени); единые правила именования ресурсов, наличие директориального сервиса; единая политика безопасности и др.

· Алгоритмы, реализующие сервисы защиты, должны быть достаточно эффективны, чтобы заметно не отражаться на производительности компьютерной сети при выполнении ею своих основных функций по обслуживанию пользователей и прикладных программ (ПП).

· Система должна использовать криптоалгоритмы, основанные на идентификационной информации, симметричные и асимметричные криптоалгоритмы.

При разработке логической модели СКЗИППЗ были приняты следующие предположения. СКЗИППЗ функционирует в рамках корпоративной компьютерной сети (Рис. 2). В состав СКЗИППЗ входят пользовательские рабочие станции, удостоверяющий центр, центры доверия.

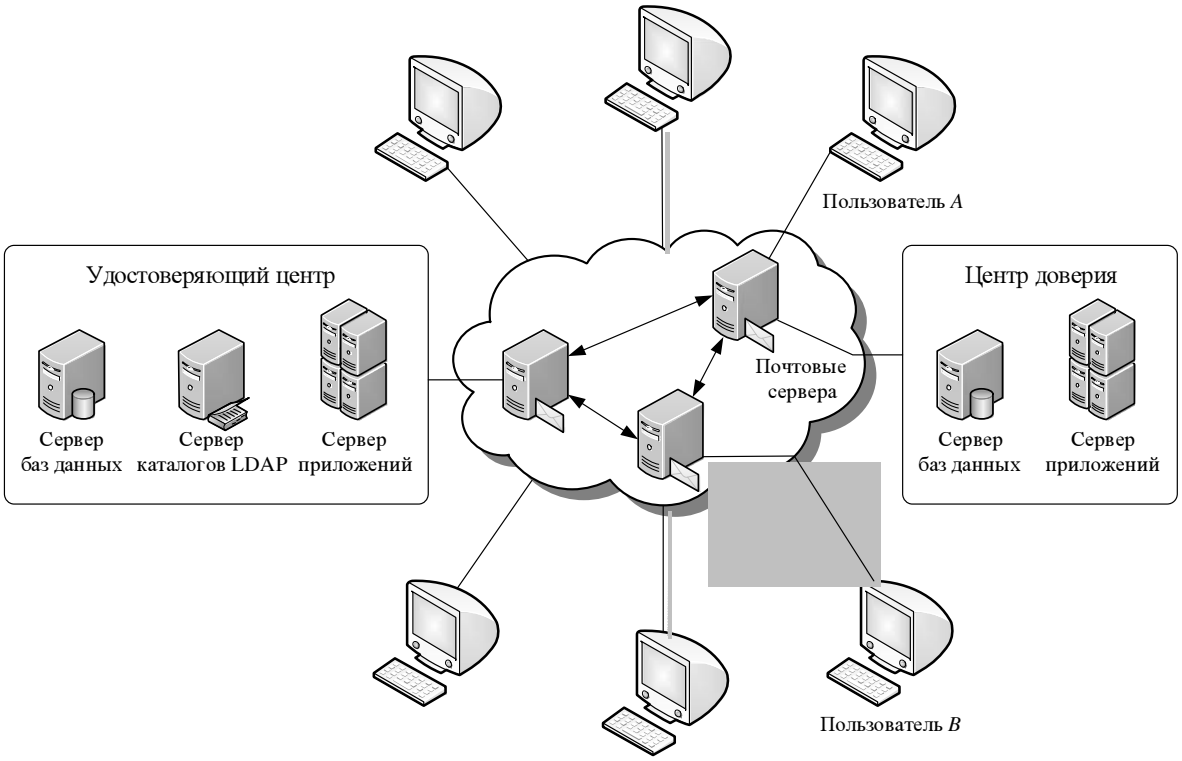

Рис. 2. Обобщённая топологическая схема клиент-серверных компонентов системы

Концептуально СКЗИППЗ представляется как комплекс программ, расширяющих функции ОС и формирующий для ПП среду криптографической защиты информации на основе планирования потоков заданий посредством предоставления определённых услуг (сервисов), доступных через интерфейсы прикладного программирования (ИПП).

Исходя из перечисленных требований, синтезирована архитектурная модель СКЗИППЗ. На рис. 3 показаны основные архитектурные компоненты СКЗИППЗ в их взаимосвязи, а также взаимодействия с другим системным и прикладным ПО.

Каждый архитектурный компонент имеет функциональную спецификацию, декларированную в виде системного интерфейса. Часть интерфейсов объявляются ИПП, т. е. соответствующие функции объявляются доступными для вызова ПП, и могут использоваться ими в качестве системных сервисов (услуг) информационной системы.

На каждом физическом элементе системы: пользовательских рабочих станциях, удостоверяющем центре, центрах доверия — реализуется некоторое подмножество функций, объявленных в функциональной спецификации. Способ их реализации при описании архитектуры системы не

оговаривается. Таким образом, различные архитектурные компоненты СКЗИППЗ будут присутствовать на различных узлах компьютерной сети.

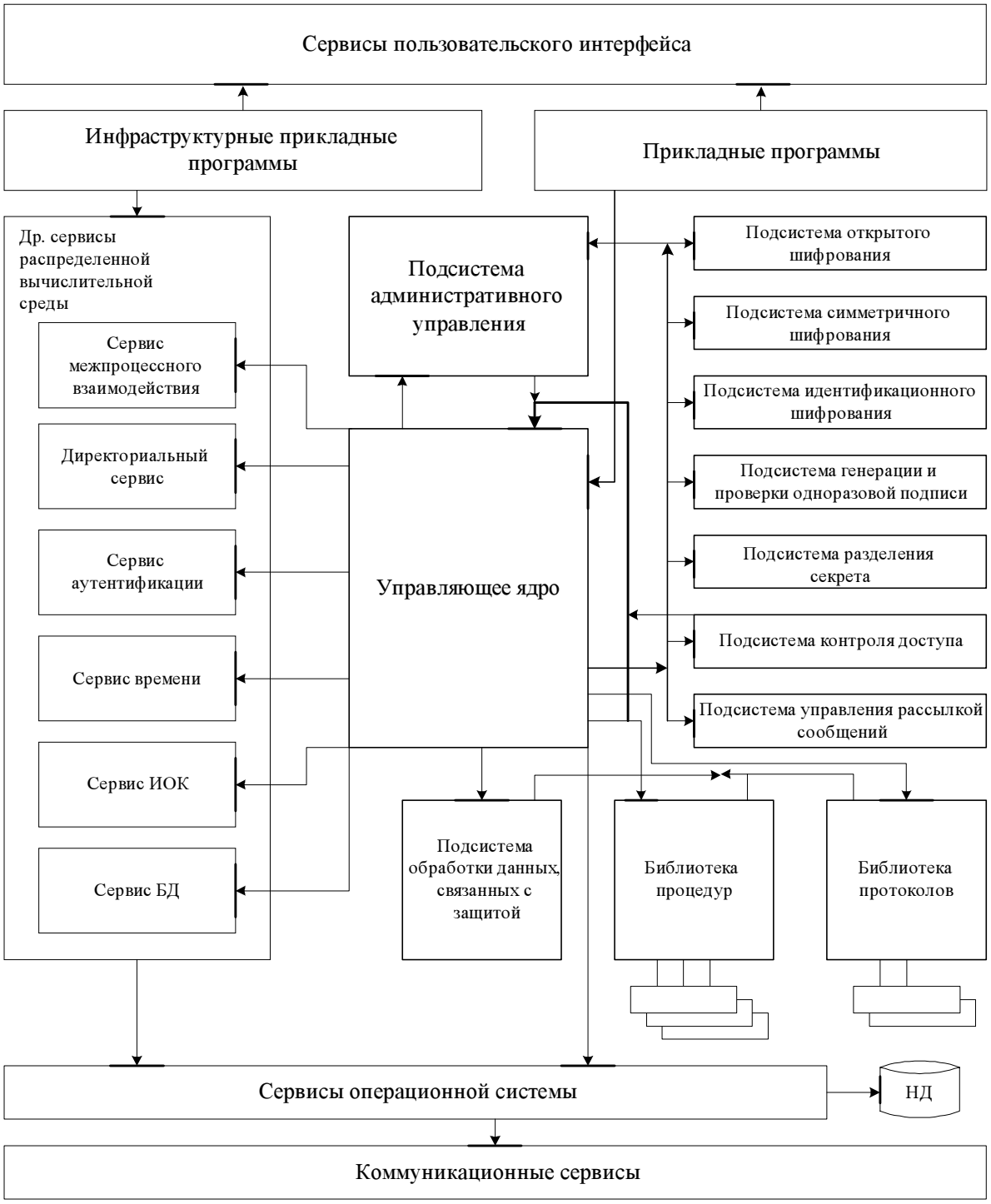

Рис. 3. Архитектурная модель системы (НД — носитель данных)

При разработке архитектурной модели СКЗИППЗ был определён необходимый состав функций, вызываемых взаимодействующими модулями системы, а также перечень услуг, предоставляемых системой ПП. Классификация функций интерфейсов СКЗИППЗ показана на рис. 4.

Центральным элементом архитектуры является управляющее ядро СКЗИППЗ. Ядро взаимодействует с другими архитектурными компонентами СКЗИППЗ.

Рис. 4. Классификация функций интерфейсов системы (— функции, включаемые в ИПП)*

Архитектурные компоненты СКЗИППЗ включают в себя восемь подсистем: административного управления; открытого шифрования; симметричного шифрования; идентификационного шифрования; генерации и проверки одноразовой подписи; разделения секрета; управления рассылкой сообщений; контроля доступа. Обмен данными между отдельными модулями, подсистемами одного и того же комплекса программ, а также с ПП организуется ядром комплекса программ посредством очередей сообщений для каждого модуля.

Части интерфейсов каждой из перечисленных подсистем объявляются ИПП. Вызовы функций ИПП могут осуществляться другими архитектурными компонентами СКЗИППЗ, другим системным ПО сети и (преимущественно) ПП.

Задача честного обмена цифровыми подписями между двумя или более участниками криптосистемы — одна из важнейших задач электронной коммерции. Она является ключевой для успешного решения множества других задач: честного обмена цифровыми потоками данных (digital content fair exchange), сертифицированной электронной почты (certified e-mail), обмена «электронной монетой», одновременного подписания контракта (simultaneous contract signing) [3]. Рассмотрим эту задачу для двустороннего случая.

Предположим, необходимо осуществить обмен электронными документами или «электронными деньгами». Документы или деньги представлены в виде информации, заверенной цифровой подписью. Предположим, у нас есть два участника криптосистемы: A и B. Каждый из них имеет пару секретного и открытого ключей цифровой подписи: $(sk_A, \rho k_A)$ и $(sk_B, \rho k_B)$ соответственно. Они предварительно согласовали тексты документов, которыми собираются обмениваться и сгенерировали под ними свои цифровые подписи: $\sigma_A = Sign_{sk_A}(M_A)$ и $\sigma_B = Sign_{sk_B}(M_B)$ соответственно. Требуется, чтобы в результате выполнения протокола каждый из них либо обладал обеими цифровыми подписями $[\sigma_A, \sigma_B]$ сразу, либо

отклонил обмен как неудавшийся. Главное не должно быть ситуации, при которой одна сторона протокола могла бы получить цифровую подпись противоположной стороны, но при этом не передать ей свою собственную. Описанная криптосхема носит название схемы честного обмена цифровыми подписями (fair exchange). Приведем схему обмена цифровыми подписями (Рис. 5).

Данная схема наглядно демонстрируют, что решение задачи характеризуется определенной, строго упорядоченной последовательностью действий участников системы. СКЗИППЗ позволит управлять последовательностью выполнения индивидуальной работы каждым из участников системы за счет распределения в нужные моменты времени прав доступа к секретным ключам (или, наоборот, ограничения таких прав).

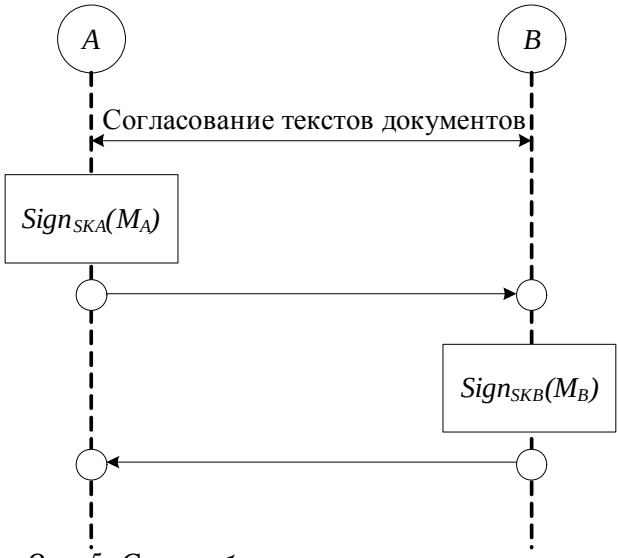

Рис. 5. Схема обмена цифровыми подписями

Автором разработан алгоритм решения задачи честного обмена цифровыми подписями с помощью СКЗИППЗ (Рис. 6).

Каждый пользователь, который хочет стать участником СКЗИППЗ, должен выполнить протокол регистрации нового участника системы, в результате чего УЦ предоставит ему сертификат открытого ключа шифрования для схемы открытого шифрования.

Предположим, два участника системы A и B хотят осуществить обмен цифровыми подписями. Они предварительно согласовали тексты документов, которыми собираются обмениваться, и сгенерировали под ними свои цифровые подписи. A определяет в политике следующие элементы: проверка существования политики B; шифрованное сообщение A; текст документа, зашифрованный на открытом ключе A; текст документа, зашифрованный на открытом ключе B. B определяет в политике следующие элементы: проверка существования политики A; шифрованное сообщение B; текст документа, зашифрованный на открытом ключе B; текст документа, зашифрованный на открытом ключе A.

После этого каждый участник системы зашифровывает цифровую подпись и посылает шифрованное сообщение другому участнику. Далее A доказывает ЦД, что он удовлетворяет всем требованиям политики B: проверяется существование политики A; сравнение полученного сообщения с шифрованным сообщением B; сравнение обоих зашифрованных текстов документов. ЦД обозначен символом T (англ. trusted authority). ЦД при положительном результате проверки удовлетворения требованиям политики выпускает мандат для A. С помощью мандата A расшифровывает цифровую подпись. Аналогично B доказывает ЦД, что он удовлетворяет всем требованиям политики A: проверяется существование политики B; сравнение полученного сообщения с шифрованным сообщением A; сравнение обоих зашифрованных текстов документов. ЦД при положительном результате проверки удовлетворения требованиям политики выпускает мандат для B. С помощью мандата B расшифровывает цифровую подпись.

При возникновении конфликтной ситуации, т. е. если в сообщении была зашифрована другая информация, оба участника обладают достаточными доказательствами для ее разрешения в судебном порядке.

Схема честного обмена цифровыми подписями является базовой для многих других, среди которых в первую очередь следовало бы отметить схемы взаимного честного обмена цифровыми данными, схемы, реализующие сертифицированную электронную почту, и схемы, решающие задачу одновременного подписания контракта.

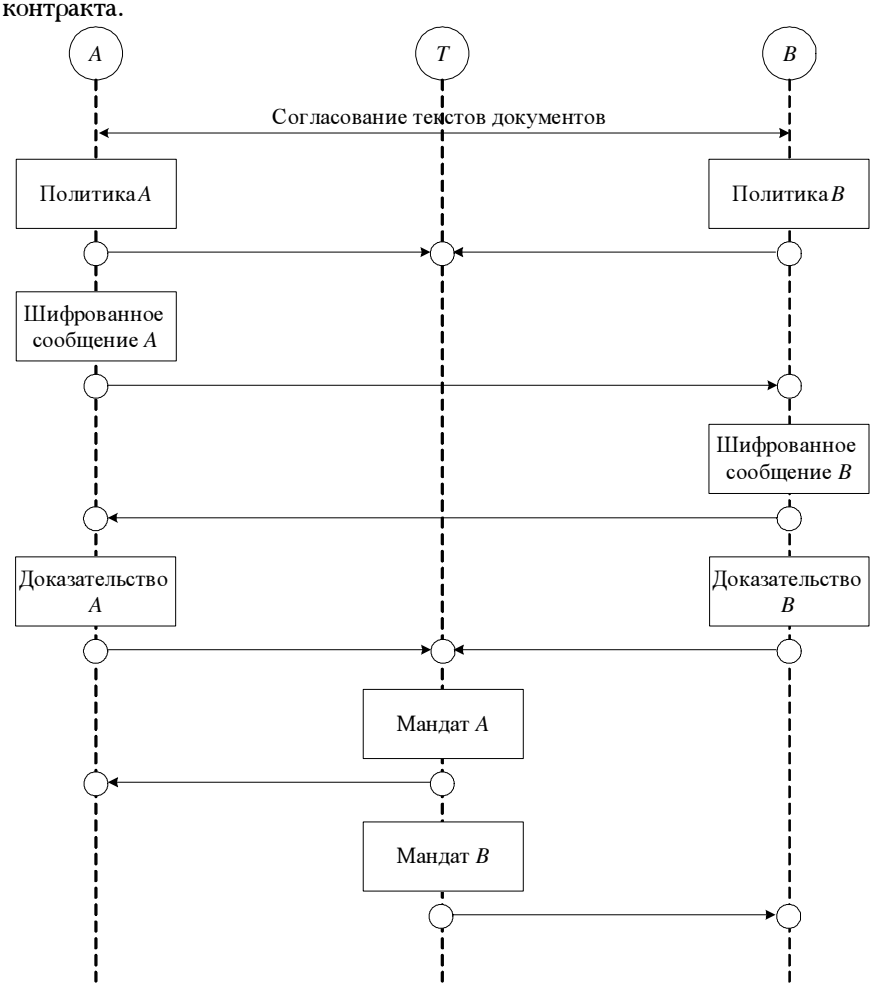

Рис. 6. Схема честного обмена цифровыми подписями с помощью планирования потоков заданий

Система криптографической защиты информации на основе планирования потоков заданий обеспечивает возможность решения типовых задач в сфере электронной коммерции с помощью унифицированной системы криптографической защиты информации, управляющей выполнением операций, требующих применения секретных ключей.

Архитектурная модель системы, состав и структура ее подсистем, общая топология размещения элементов системы и ее функциональное описание могут быть использованы при дальнейшей разработке системы криптографической защиты информации на основе планирования потоков заданий вплоть до её практической реализации.

СПИСОК ЛИТЕРАТУРЫ:

1. *Al-Riyami S. S., Malone-Lee J. and Smart N. P.* Escrow-Free Encryption Supporting Cryptographic Workflow. http://eprint.iacr.org/2004/258.

2. *Barbosa M., Farshim P.* Secure Cryptographic Workflow in the Standard Model. http://eprint.iacr.org/2006/450.

3. *Запечников С. В.* Криптографические протоколы и их применение в финансовой и коммерческой деятельности: Учебное пособие для вузов. М., 2007. – 320 с.