На правах рукописи

Смирнов Павел Владимирович

Протокольное обеспечение доказательной регистрации событий в системах защиты информации

Специальность 05.13.19 – методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание учёной степени

кандидата технических наук

Автор

Москва – 2007

Работа выполнена в Московском инженерно-физическом институте
(государственном университете)

Научный руководитель: кандидат технических наук, доцент
Петрова Тамара Васильевна

Официальные оппоненты: доктор технических наук, профессор
Щербаков Андрей Юрьевич

кандидат технических наук, доцент
Запечников Сергей Владимирович

Ведущая организация: Московский государственный технический университет им. Н.Э. Баумана

Защита состоится 21 мая 2007 г. в 15 часов
на заседании диссертационного совета ДМ 212.130.08 в МИФИ по адресу:
115409, Москва, Каширское шоссе, д.31.

С диссертацией можно ознакомиться в библиотеке МИФИ.
Автореферат разослан _____ 2007 года.

Просим принять участие в работе совета или прислать отзыв в одном экземпляре, заверенный печатью организации.

Учёный секретарь
диссертационного совета к.т.н., доцент Горбатов В.С.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. В последние годы в большинстве исследований, посвященных информационной безопасности, среди множества угроз отдельным пунктом выделяется проблема утечек конфиденциальной информации, происходящих по вине внутренних нарушителей. Так, по данным отчётов CERT, CSI и ФБР за 2005 и 2006 годы более половины опрошенных коммерческих и правительственных организаций хотя бы раз в течение года пострадали от утечки данных. Почти для 40% респондентов ущерб от внутренних нарушителей составил более одной пятой убытков от всех нарушений информационной безопасности.

Приведённая статистика обосновывает важность борьбы с утечками конфиденциальной информации, вызванными внутренними нарушителями. Технические и организационные меры борьбы с утечкой конфиденциальной информации не всегда эффективны, поэтому в дополнение к ним целесообразно использовать правовые методы. В политике безопасности организации должен быть закреплён принцип регистрации всех действий с конфиденциальной информацией, в том числе и в электронной форме. Именно записи в журналах регистрации позволяют определить круг лиц, через которых могла произойти утечка, и при успешном расследовании инцидента привлечь к ответственности нарушителя. Электронной регистрационной записи можно придать доказательную силу, включив в неё дополнительные данные, обеспечивающие невозможность отказа субъекта от осуществления операции над документом.

Функция регистрации событий является неотъемлемой функцией подсистемы управления доступом, которая присутствует в любой системе, где требуется обеспечение безопасности информации. Предположим, что субъект желает получить доступ к некоторому объекту. При этом монитор обращений аутентифицирует субъекта, проверяет его права доступа к объекту и разрешает или отклоняет запрашиваемый доступ. Регистрационная запись, которую сохраняет монитор обращений, содержит идентификаторы субъекта и объекта, тип запрашиваемого доступа и принятое решение: разрешить или отклонить. Для обеспечения доказательной силы регистрационной записи необходимо добавить к этой записи доказательства того, что субъект действительно запрашивал доступ к объекту, и если доступ был разрешён, то и доказательство, что субъект получил доступ.

Для достижения поставленных целей может использоваться протокол неотказуемого равноправного обмена. Задача протокола равноправного обмена заключается в доставке обмениваемых документов участникам протокола таким образом, что либо оба получают требуемый документ, либо ни один из участников не получает ничего. Если кроме равноправности обмена требуется обеспечить доказательство участия в обмене, то используется протокол неотказуемого равноправного обмена. Таким образом, использование протокола неотказуемого равноправного обмена запроса на осуществление операции над объектом на результат этого запроса позволяет решить задачу доказательной регистрации событий в системе управления доступом, не оставляя возможности субъекту или монитору обращений создать регистрационную запись обманным путём.

Протоколы равноправного обмена применимы и для решения множества других задач. Актуальной проблемой в исследовании этих протоколов является создание обобщённых протоколов, т.е. таких протоколов, которые могут быть использованы как для обмена простых электронных документов, так и для обмена электронного документа на документ с электронной цифровой подписью (ЭЦП). Обобщённые протоколы позволяют обмениваться любыми объектами, представимыми в электронной форме. В диссертационной работе такие объекты называются бизнес-документами.

Целью диссертационной работы является синтез обобщённых протоколов неотказуемого равноправного обмена, доказательство их корректности и реализация системы доказательной регистрации событий на базе таких протоколов.

В соответствии с поставленной целью в диссертационной работе **решаются следующие задачи**:

- Разработка модели обобщённого протокола неотказуемого равноправного обмена.
- Разработка эффективных способов модификации протоколов передачи бизнес-документов для придания им свойств, необходимых для объединения в обобщённом протоколе равноправного обмена.
- Разработка обобщённых протоколов неотказуемого равноправного обмена.
- Реализация системы доказательной регистрации событий на основе протокола неотказуемого равноправного обмена.

Методы исследования: теоретическая криптография, теория множеств, теория алгоритмов, теория распределённых алгоритмов.

Научная новизна работы заключается в следующем:

- Впервые предложена модель обобщённого протокола неотказуемого равноправного обмена для асинхронных сетей.
- Предложен способ изменения произвольного протокола передачи бизнес-документа для придания ему свойств доказуемости доставки или генерируемости, необходимых для обмена этого бизнес-документа с помощью обобщённого протокола.
- Разработан ряд новых обобщённых протоколов неотказуемого равноправного обмена с различными свойствами.
- Впервые предложен обобщённый протокол неотказуемого равноправного обмена зависимых бизнес-документов.
- Предложена концепция и реализована система доказательной регистрации событий.

На защиту выносятся следующие основные результаты работы:

- Расширенная модель распределённых алгоритмов на основе модели Шунтера для описания обобщённых протоколов неотказуемого равноправного обмена в асинхронных сетях, где центр доверия (ЦД) участвует только при возникновении ошибки.
- Предложенный автором способ модификации произвольных протоколов передачи бизнес-документов для придания им свойств доказуемости доставки или генерируемости, необходимых для их обмена с помощью

обобщённого протокола. Способ является оптимальным с точки зрения количества дополнительных сообщений и времени выполнения протокола.

- Протокол неотказуемого равноправного обмена генерируемого документа на документ, обеспечивающий доказуемость отправки, без дополнительной сложности.
- Протокол неотказуемого равноправного обмена двух генерируемых бизнес-документов без дополнительной сложности. При восстановлении прерванного обмена с помощью ЦД, право обладания бизнес-документом передаётся через него.
- Протокол неотказуемого равноправного обмена двух генерируемых бизнес-документов. При любом стечении обстоятельств ЦД не обладает бизнес-документом.
- Способ использования произвольного обобщённого протокола неотказуемого равноправного обмена для обмена зависимых бизнес-документов.
- Реализация системы доказательной регистрации событий.

Практическую значимость представляют разработанные обобщённые протоколы неотказуемого равноправного обмена, а также система доказательной регистрации событий. Результаты могут быть использованы для обеспечения доказательной регистрации событий в подсистеме управления доступом систем защиты информации, а также для построения сервисов электронной коммерции.

Внедрение результатов исследований. Протокол доказательной регистрации событий используется для регистрации криптографических операций в программно-аппаратном криптографическом модуле «КриптоПро HSM», разработанном ООО «КРИПТО-ПРО». Реализация системы доказательной регистрации событий используется в подсистеме «Электронный нотариат» ФИЦ в НИИ «Восход». Результаты диссертационной работы внедрены в учебный процесс на факультете «Информационная безопасность» Московского инженерно-физического института (государственного университета).

Публикации и апробация работы. По теме диссертации опубликовано 9 печатных работ, в т.ч. 4 научных статьи и 5 тезисов докладов. Результаты работы докладывались на конференциях и семинарах различного уровня, в том числе:

- в трудах Международной научно-практической конференции «Информационная безопасность», Таганрог, 2005 г;
- в сборнике тезисов Общероссийской научно-технической конференции «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, 2005-2006 гг.;
- на Всероссийской научно-практической конференции «Проблемы информационной безопасности в системе высшей школы», Москва, 2005-2006 гг.;
- на международной конференции EUROCRYPT’2006 (rump session);
- на международной конференции «РусКрипто 2007».

Структура и объём работы.

Диссертация состоит из введения, пяти глав, заключения, списка использованных источников из 144 наименований и пяти приложений. Работа изложена на 195 страницах с 33 рисунками и 7 таблицами, не включая приложения.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы диссертации, определяются цели, формулируются задачи исследования, описывается структура и логика работы.

В первой главе приводится систематизированный обзор и даётся классификация описанных в литературе протоколов равноправного обмена, уточняются методы и пути решения поставленной научной задачи.

Большинство существующих работ в области протоколов равноправного обмена связано с обменом определёнными типами бизнес-документов, тогда как лишь в нескольких исследованиях рассматривается понятие обобщённого равноправного обмена. Обобщённый протокол равноправного обмена предназначен для любых бизнес-документов с некоторыми ограничениями. Такие протоколы строятся, например, исходя из предположения, что бизнес-документ может быть передан за одно сообщение, или передан адресату через третью сторону с сохранением всех свойств.

В литературе описываются протоколы для обмена следующих типов бизнес-документов:

- *Закрытых данных*. Протокол передачи открывает данные, которые до этого были неизвестны получателю.
- *Документов с ЭЦП*. Отправитель создаёт подпись под определённым документом и передаёт подписанный документ получателю.
- *Платежей*. В результате выполнения протокола платежа отправитель переводит некоторую денежную сумму получателю.

В общем случае любой набор бизнес-документов может быть обменян на любой другой набор. Для частных случаев обмена единичных бизнес-документов, перечисленных выше, потребуется, по крайней мере, девять различных протоколов равноправного обмена. Учитывая, что может существовать множество различных реализаций бизнес-документов, разных протоколов требуется гораздо больше. В большинстве опубликованных исследований уделяется внимание лишь нескольким частным случаям обмена.

- *Подписание контрактов*. Протокол подписания контрактов служит для создания неотказуемого двустороннего соглашения. Он может быть реализован путём равноправного обмена подписями под текстом контракта.
- *Заказная электронная почта*. Протокол заказной электронной почты служит для обмена сообщения на подтверждение его получения. Такие протоколы часто называют протоколами неотказуемой передачи (non-repudiation protocol). Он может быть реализован путём равноправного обмена закрытых данных (сообщения) на подпись под описанием сообщения.
- *Покупка*. Протокол совершения покупки служит для обмена закрытых данных на платёж. Особым случаем данного протокола служит обмен

платежа на подтверждение его получения, т.е. на подпись под определённым документом.

Протоколы равноправного обмена также классифицируются по степени участия ЦД в протоколе.

- *Протоколы с активным ЦД*. Активный ЦД участвует в каждом обмене и гарантирует честность.
- *Оптимистичные протоколы*. В оптимистичном протоколе обмена ЦД присутствует, но не принимает участие, если участники обмена действуют согласованно и не отступают от протокола. ЦД привлекается для восстановления равноправности в случае несогласия участников, отступления от протокола или ошибки.
- *Протоколы постепенного обмена*. Протоколы постепенного обмена дают лишь вероятностную гарантию равноправности и не требуют участия ЦД.

Очевидно, протоколы равноправного обмена без ЦД были бы наилучшими с практической точки зрения, однако такие протоколы основываются на постепенном обмене, т.е. небольшие части бизнес-документа обмениваются по очереди за большое число раундов. Известно, что равноправный обмен без ЦД и постепенного обмена невозможен.

После сравнения свойств протоколов с различным участием ЦД делается вывод, что оптимистичные протоколы равноправного обмена являются лучшими в большинстве случаев с практической точки зрения.

Особое внимание в обзоре уделяется существующим обобщённым протоколам обмена. Делается вывод, что они не позволяют осуществить обмен произвольными бизнес-документами по следующим причинам: 1) протоколы Асокана (Asokan N. “Fairness in Electronic Commerce”) имеют существенные ограничения на допустимые типы бизнес-документов; 2) протоколы Шунтера (Schunter M. “Optimistic Fair Exchange”) используют абстрактные свойства протоколов передачи бизнес-документов, но не предложен способ придания этих свойств произвольному протоколу.

Во второй главе вводится модель протокола равноправного обмена как распределённой системы взаимодействующих процессов в асинхронной сети, рассматривается протокол передачи бизнес-документа как составная часть протокола равноправного обмена.

Процесс – участник протокола представляется как алгоритм со следующими свойствами:

1. Работа алгоритма начинается с получения входных данных, выбранных из множества допустимых входов I, и заканчивается выдачей результата выполнения из множества допустимых выходов O. Алгоритм может не завершить работу вообще.
2. Работающие алгоритмы могут обмениваться сообщениями друг с другом по асинхронной сети. Каждое отправляемое сообщение, помимо алгоритма-источника сообщения, становится известным лишь алгоритму-получателю.
3. Множества допустимых входов алгоритма может содержать специальный элемент $wakeup \in I$. Такой алгоритм, находящийся в состоянии ожидания

сообщения, в любой момент может получить на вход $wakeup$, после чего он прекращает ожидание и продолжает выполнение по другой ветке.

Элемент $wakeup \in I$ в свойстве 3 вводится для обработки таймаутов доставки сообщений в асинхронной сети. После получения на вход $wakeup$ алгоритм прекращает ожидание сообщения и должен завершиться без обмена сообщениями с другой стороной обмена, т.е. дальнейший обмен сообщениями возможен с третьими сторонами – ЦД, банком, процессинговым центром платёжной системы и т.п.

Во многих протоколах для обеспечения невозможности отказа участникоа от тех или иных действий используется ЭЦП. В работе полагается, что все алгоритмы, участвующие в протоколе, являются субъектами инфраструктуры открытых ключей и обладают сертификатами открытых ключей. Сертификаты могут быть выданы одним или несколькими Удостоверяющими центрами. Для успешного выполнения протокола необходимо, чтобы все участники принимали сертификаты всех других участников, т.е. доверяли этим Удостоверяющим центрам.

Для того чтобы формализовать свойства протоколов равноправного обмена бизнес-документами, необходимо определить, что означает «приобретение» или «потеря» бизнес-документа или его части. В работе обладание бизнес-документом моделируется путём определения семейства протоколов использования. Успешное выполнение протокола использования каким-либо алгоритмом возможно тогда и только тогда, когда данный алгоритм обладает знанием о бизнес-документе. Успешно выполнить все протоколы использования может только алгоритм, обладающий бизнес-документом. Считается, что при неудачном обмене бизнес-документ остаётся недоступным получателю, если он не может успешно выполнить ни один протокол использования бизнес-документа из семейства.

Класс бизнес-документов – это набор $B = (U, D, ID)$, состоящий из алгоритма использования U, множества D описаний бизнес-документов, и множества ID идентификаторов итераций протокола использования. Алгоритм U может выполнять семейство протоколов использования $\{use_i \mid i \in U_{id}\}$.

Примерами классов бизнес-документов и возможных описаний могут служить следующие:

1. *Платёж* может описываться валютой, суммой, и идентификатором плательщика.
2. *Подпись* может быть описана идентификатором подписывающего и содержимым сообщения.
3. *Данные* могут быть описаны в простой словесной форме или хеш-значением.

Равноправный обмен в рассматриваемой модели происходит между двумя алгоритмами – сторонами обмена (далее – алгоритм-сторона). Каждый алгоритм получает на вход описание бизнес-документа, которым он обладает, и описание бизнес-документа, который он должен получить в обмен на этот. Протокол обмена будет безопасным, если стороны обмена станут обладателями бизнес-документов только при условии совпадения ожидаемых документов с тем, что предлагают участники. Если это не так, ничего не должно измениться, т.е. ни один из участников не должен получить информацию о содержимом бизнес-документа.

Опр. 1. *Протокол обмена бизнес-документов* – это набор $(P, Q, B_P, B_Q, T, AM, ID)$, состоящий из алгоритмов-сторон P и Q, классов бизнес-документов $B_P = (U_P, D_P, ID)$ и $B_Q = (U_Q, D_Q, ID)$, алгоритма ЦД T, множества AM вспомогательных алгоритмов без входа и выхода и множества ID идентификаторов итераций. Алгоритмы множества AM называются третьими сторонами протокола.

Алгоритмы P и Q могут выполнять протокол обмена друг с другом. Если при обмене бизнес-документами корректными алгоритмами и отсутствии входов $wakeup$ ЦД T не принимает участия в протоколе, то такой протокол обмена называется *оптимистичным*. Протокол обмена называется *равноправным* при выполнении следующих свойств: 1) в результате успешного обмена стороны становятся обладателями желаемых бизнес-документов; 2) при неудачном обмене стороны по-прежнему обладают своими бизнес-документами и не получили знания о документах друг друга. ■

Теперь определим свойство невозможности отказа от обмена. После успешного обмена каждая сторона должна иметь возможность доказать, что обмен действительно состоялся, и какие именно документы были обменяны, причём подделка такого доказательства должна быть невозможна.

Опр. 2. Пусть задан протокол равноправного обмена бизнес-документов (P, Q, B_P, B_Q, AM, ID). Добавим в этот набор алгоритм-проверяющий V и доопределим алгоритмы-стороны P и Q таким образом, чтобы каждый из них мог выполнить протокол проверки доказательства с V, в конце выполнения которого V получает на выходе $(exchanged, P, Q, d_P, d_Q, id)$, где $d_P \in D_P$, $d_Q \in D_Q$, $xref \in XREF$ и $id \in ID$ или $(failed, id)$. Первый выход означает, что стороны P и Q обменяли бизнес-документы с описаниями d_P и d_Q в обмена, обозначенном идентификатором id. Второй выход означает, что проверка не удалась.

Протокол неотказуемого равноправного обмена бизнес-документов – это определённый выше набор $(P, Q, B_P, B_Q, AM, V, ID)$, который удовлетворяет следующим свойствам: 1) при успешном обмене обе стороны могут успешно выполнить протокол проверки доказательства; 2) при неудачном обмене ни одна из сторон не может успешно выполнить этот протокол. ■

Протокол равноправного обмена должен включать в себя передачу одного бизнес-документа от стороны P к Q, и другого от стороны Q к P. Обмениваемые документы могут принадлежать к разным классам, а следовательно, протоколы их передачи в общем случае различны. Каким бы ни был каждый протокол передачи бизнес-документа – одношаговым или многошаговым с участием третьих сторон – простое объединение двух протоколов передачи не даст в результате протокол равноправного обмена.

В диссертационной работе определяются два свойства протоколов передачи бизнес-документов – генерируемость и доказуемость отправки. Использование этих свойств позволяет построить протоколы равноправного обмена. Генерируемость в протоколе передачи бизнес-документа означает, что отправитель может уполномочить ЦД завершить или повторить доставку бизнес-документа получателю. В этом случае, если получатель докажет ЦД, что он выполнил свои обязательства в настоящем обмене, то ЦД может сгенерировать бизнес-документ

для него, не нарушая равноправность протокола. Протокол передачи бизнес-документа с доказуемостью отправки гарантирует, что корректный отправитель сможет доказать ЦД, что получатель стал обладателем бизнес-документа или может стать им без участия отправителя. Если в свою очередь получатель такого документа предварительно подготовил свой документ к генерации, то этого доказательства для ЦД достаточно, чтобы сгенерировать отправителю требуемый документ и тем самым обеспечить равноправный обмен.

Для того чтобы разрабатываемые протоколы равноправного обмена бизнес-документов, обладающих генерируемостью или доказуемостью отправки, оставались обобщёнными, в диссертационной работе приводятся методики модификации произвольного протокола передачи бизнес-документов с целью придания ему необходимых свойств.

Для получения свойства генерируемости протокол передачи разбивается на два подпротокола – подготовки генерируемости и передачи генерируемого документа. Первый протокол не должен дать знание о бизнес-документе другой стороне, но довести передачу до такого состояния, в котором эта сторона может получить подготовленный к генерации документ, обращаясь только к ЦД. Для достижения этих целей каждое сообщение, несущее знание о бизнес-документе, зашифровывается для ЦД. Тогда генерация будет выполняться путём отправки этих сообщений для расшифрования к ЦД. Во многих случаях, успешное выполнение протокола использования зависит от третьих сторон, участвующих в передаче бизнес-документа, таких как банк или процессинговый центр. Отправлять этим сторонам зашифрованное сообщение не представляется возможным, поскольку их действия зависят от содержимого этого сообщения. В таком случае необходимо модифицировать алгоритм действий третьей стороны, которая после получения такого сообщения не будет помогать выполнять протокол использования стороне-получателю до предъявления им свидетельства о том, что была выполнена генерация или передача генерируемого документа в его адрес.

Для получения свойства доказуемости отправки в произвольном протоколе передачи бизнес-документа предусматривается возможность повторной отправки данного документа через ЦД.

В третьей главе с использованием модели, описанной в предыдущей главе, строятся новые протоколы равноправного обмена и протоколы неотказуемого равноправного обмена бизнес-документами, протоколы передачи которых обеспечивают свойства генерируемости или доказуемости отправки.

Первый протокол предназначен для обмена генерируемого бизнес-документа на документ, обеспечивающий доказуемость отправки. В этом протоколе сначала обладатель генерируемого документа выполняет подготовку его генерируемости, после чего другой участник передаёт свой документ, обладающий доказуемостью отправки, и в конце первый участник передаёт генерируемый документ. Если в протоколе возникает ошибка, то второй участник обращается к ЦД для генерации документа, доказывая, что он выполнил свои обязательства по обмену. Простого объединения соответствующих протоколов в указанном порядке недостаточно для достижения равноправности обмена, поскольку ЦД не знает, какой именно документ хотел получить первый участник в обмен на свой, поэтому в протокол добавлено сообщение, обеспечивающее невозможность отказа от согласия на обмен

первого участника. Новое сообщение передаётся им второму участнику в ходе подготовки генерируемости.

Иллюстрация протокола обмена представлена на рис. 1. Здесь сплошные стрелки означают входы и выходы алгоритмов, пунктирные – дополнительное сообщение протокола и альтернативные выходы алгоритмов, сигнализирующие об ошибке, S_P и R_P – алгоритмы передачи и приёма документа с обеспечением генерируемости соответственно, S_Q и R_Q – алгоритмы передачи и приёма документа с доказуемостью отправки. Алгоритм-сторона P, обладающая генерируемым документом, является композицией алгоритмов P', S_P и R_Q. Алгоритм-сторона Q, обладающая документом с доказуемостью отправки, является композицией алгоритмов Q', S_Q и R_P. Алгоритмы P' и Q' являются управляющими в композициях, т.е. они получают команды на вход и выдают результат и при этом в процессе своей работы могут отдавать команды на вход другим алгоритмам и получать от них выходы. Взаимодействие сторон с ЦД при возникновении ошибок, а также все другие протоколы аналогичным образом проиллюстрированы в работе.

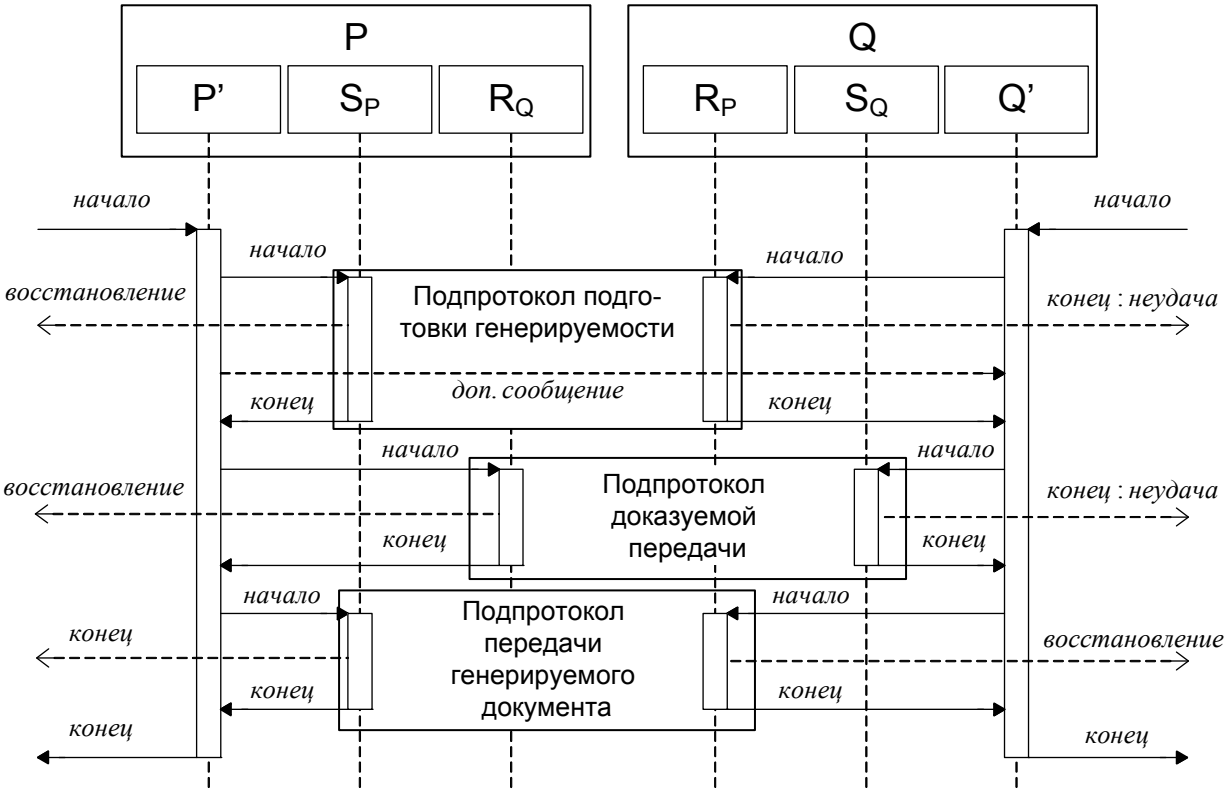

Рис. 1. Протокол равноправного обмена генерируемого документа на документ с доказуемостью отправки

Второй протокол предназначен для равноправного обмена двух генерируемого бизнес-документов, возможно, различных классов. Здесь сначала обладатель генерируемого документа выполняет его подготовку к генерации, после чего другой участник подготавливает генерацию своего документа, затем первый участник осуществляет передачу, и в конце второй участник передаёт свой документ. Если в протоколе возникает ошибка, то первый участник обращается к ЦД с целью предотвращения генерации документа, если же до этого второй участник уже обращался к ЦД и сгенерировал свой документ, то первый получит при этом

необходимый ему документ. Для информирования ЦД о намерении обмена бизнес-документами в протокол добавлено сообщение, обеспечивающее невозможность отказа от согласия на обмен одной из сторон. При этом для того чтобы ЦД мог передать первому участнику документ второго, ему понадобится сохранить его у себя при восстановлении второго участника.

Схема третьего разработанного автором протокола похожа на предыдущую схему обмена двумя генерируемыми документами, но здесь для устранения передачи владения бизнес-документом ЦД, в последовательность шагов протокола вводится обмен неотказуемыми свидетельствами о том, что сторона обмена получила всё необходимое для генерации нужного ей бизнес-документа. Тогда ЦД будет осуществлять генерацию для одной стороны только при предъявлении ей такого свидетельства от другой стороны обмена.

В диссертационной работе приведены формализованные схемы разработанных протоколов и доказано их соответствие требованиям опр. 1. Для каждого из трёх новых протоколов описаны модифицированные схемы, позволяющие достичь невозможности отказа от обмена, доказано их соответствие требованиям опр. 2.

Описанные выше обобщённые протоколы равноправного обмена не охватывают случай зависимых бизнес-документов. Они подходят для всех пар обмениваемых бизнес-документов, кроме тех, в которых один документ зависит от другого. Зависимость между обмениваемыми бизнес-документами возникает в случае, если один из бизнес-документов неизвестен (не существует), или известен, но не может быть передан до момента получения первого бизнес-документа, т.е. создание второго бизнес-документа требует знания о первом.

В диссертационной работе описана схема реализации обобщённого протокола неотказуемого равноправного обмена зависимых бизнес-документов, в основе которого может лежать любой протокол неотказуемого равноправного обмена независимых бизнес-документов, доказаны свойства этой схемы.

Разработанные автором протоколы, которые приведены в третьей главе, в совокупности с результатами второй главы решают общую задачу неотказуемого равноправного обмена произвольными бизнес-документами. В разнообразных системах с различными типами бизнес-документов могут использоваться разные протоколы. Выбор протокола обусловлен особенностями системы и бизнес-документов.

В четвёртой главе ставится задача доказательной регистрации событий, схемы, представленные в предыдущих главах, применяются для построения протокола доказательной регистрации событий, описывается архитектура реализованной системы доказательной регистрации событий.

Рассмотрим взаимодействие субъекта с монитором обращений в системе управления доступом, когда субъект желает сохранить содержимое запроса в тайне до фактического осуществления операции. В этом случае ответ на запрос не известен заранее, и поэтому должен применяться протокол обмена зависимых бизнес-документов. В работе приводится построение этого протокола.

Реализованная система доказательной регистрации событий предназначена для защиты вызова удалённых процедур, выполняемого с помощью протокола SOAP RPC на платформе .NET. Архитектура системы представлена на рис. 2.

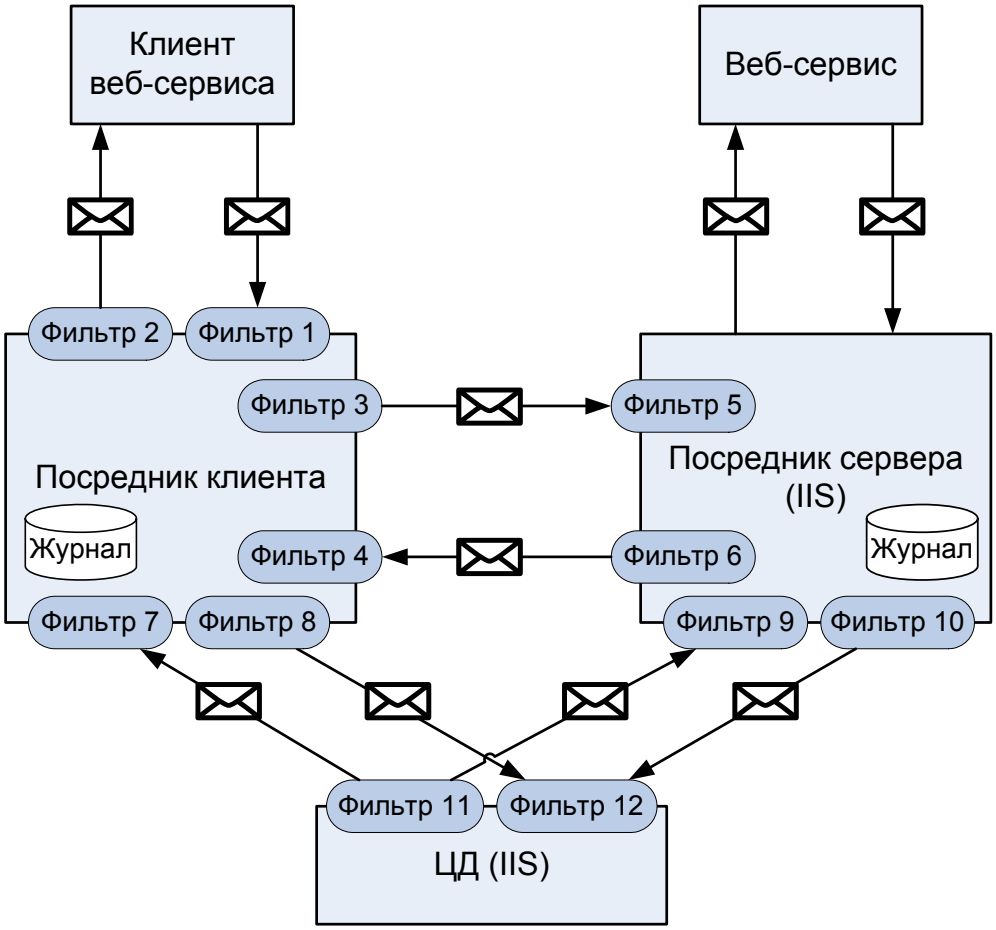

Рис. 2. Архитектура системы доказательной регистрации событий

Основная логика работы системы по созданию и проверке сообщений реализована в фильтрах, встраиваемых в объекты-посредники клиента и сервера и в ЦД, которые реализованы в виде веб-сервисов с использованием пакета Microsoft WSE. Фильтры также являются фильтрами WSE. Использование маршрутизаторов SOAP-сообщений, которые также могут быть разработаны с помощью WSE, позволяет обеспечить доказательную регистрацию событий обмена по протоколу SOAP RPC для клиентов и серверов, работающих на любой платформе.

Все сообщение, пересылаемые между посредниками клиента, сервера и ЦД туннелируется в протокол TLS с двусторонней аутентификацией. Поддержка клиентской части протокола предоставляется ОС Windows, серверная часть реализована в веб-сервере Microsoft IIS (Internet Information Services). Для аутентификации сторон используются те же сертификаты открытых ключей, которыми подписываются сообщения протокола.

Дополнительный объём трафика, порождаемый выполнением протокола доказательной регистрации событий, по сравнению с простым обменом запроса на ответ по протоколу SOAP RPC, не зависит от объёма запроса и ответа и составляет примерно 41 Кб.

Было произведено измерение временных затрат на выполнение протокола доказательной регистрации событий. Для этого использовались компьютеры следующей конфигурации: клиент – процессор Intel Pentium 4 3,0 ГГц, сервер – процессор Intel Pentium 4 XEON 2,8 ГГц. Клиент и сервер связаны между собой по локальной сети пропускной способностью 1 Гбит/с.

По результатам измерений построены два графика. Первый график иллюстрирует зависимость среднего времени обработки запроса от размера входной строки (рис. 3) при постоянном размере ответа 200 байт. На втором графике представлена зависимость среднего времени обработки запроса от размера ответа (рис. 4) при постоянном размере входной строки 200 байт. Для сравнения на обоих графиках присутствует кривая зависимости среднего времени обработки запроса этим же веб-сервисом без доказательной регистрации событий.

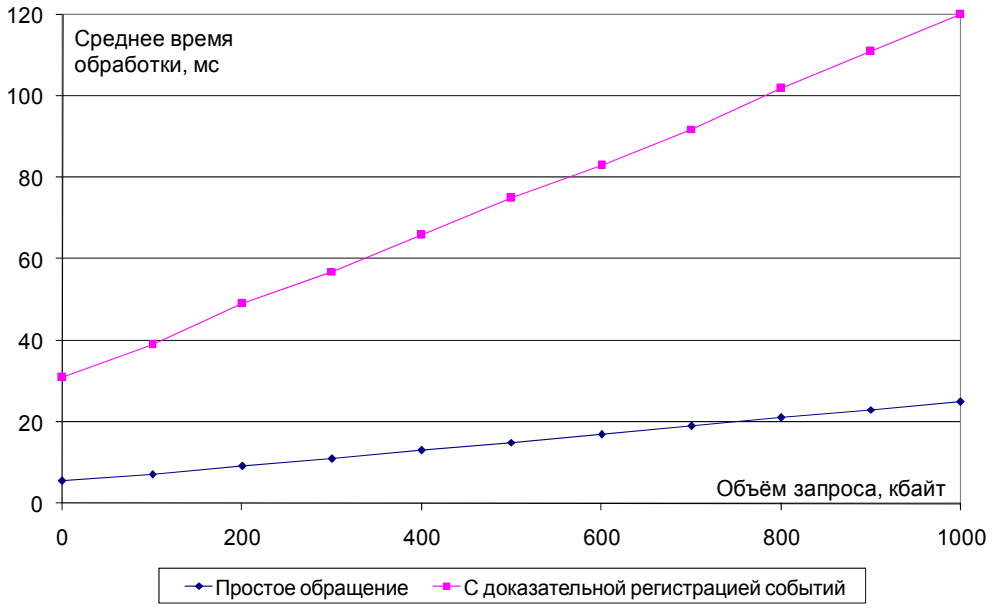

Рис. 3. График зависимости среднего времени обработки от объёма запроса

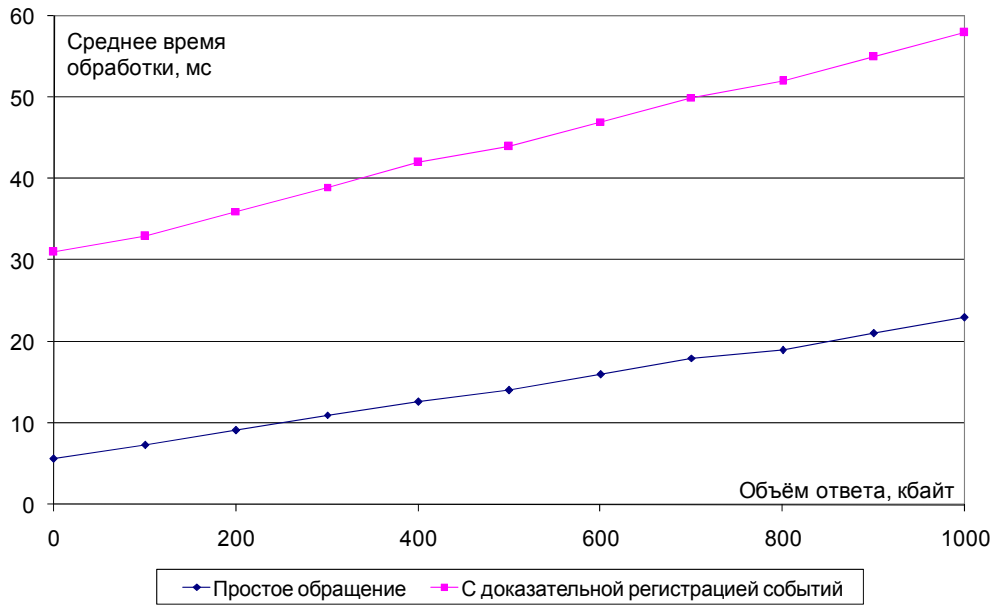

Рис. 4. График зависимости среднего времени обработки от объёма ответа

<u>В пятой главе</u> приводятся примеры использования разработанных протоколов для решения прикладных задач в двух проектах.

Первый проект представляет собой программно-аппаратный криптографический модуль «КриптоПро HSM» (далее – ПАКМ «КриптоПро HSM»).

ПАКМ «КриптоПро HSM» представляет собой сетевое устройство, подключаемое либо непосредственно к серверу (хосту), использующему криптографические сервисы ПАКМ, либо в сегмент локальной сети через стандартные сетевые устройства (коммутаторы, маршрутизаторы, концентраторы) для обслуживания групп серверов и компьютеров пользователей сети.

Все криптографические запросы должны отражаться в журнале событий ПАКМ с идентификацией пользователей и их ключевых контейнеров, с указанием времени совершения криптографической операции, значений формируемых ЭЦП и объемов зашифрованной/расшифрованной информации. Для обеспечения доказательной силы регистрационных записей обращения с такими операциями пользователя СКЗИ к ПАКМ осуществляются с применением протокола доказательной регистрации событий, приведённого в четвёртой главе. Архитектура подсистемы доказательной регистрации событий ПАКМ представлена на рис. 5.

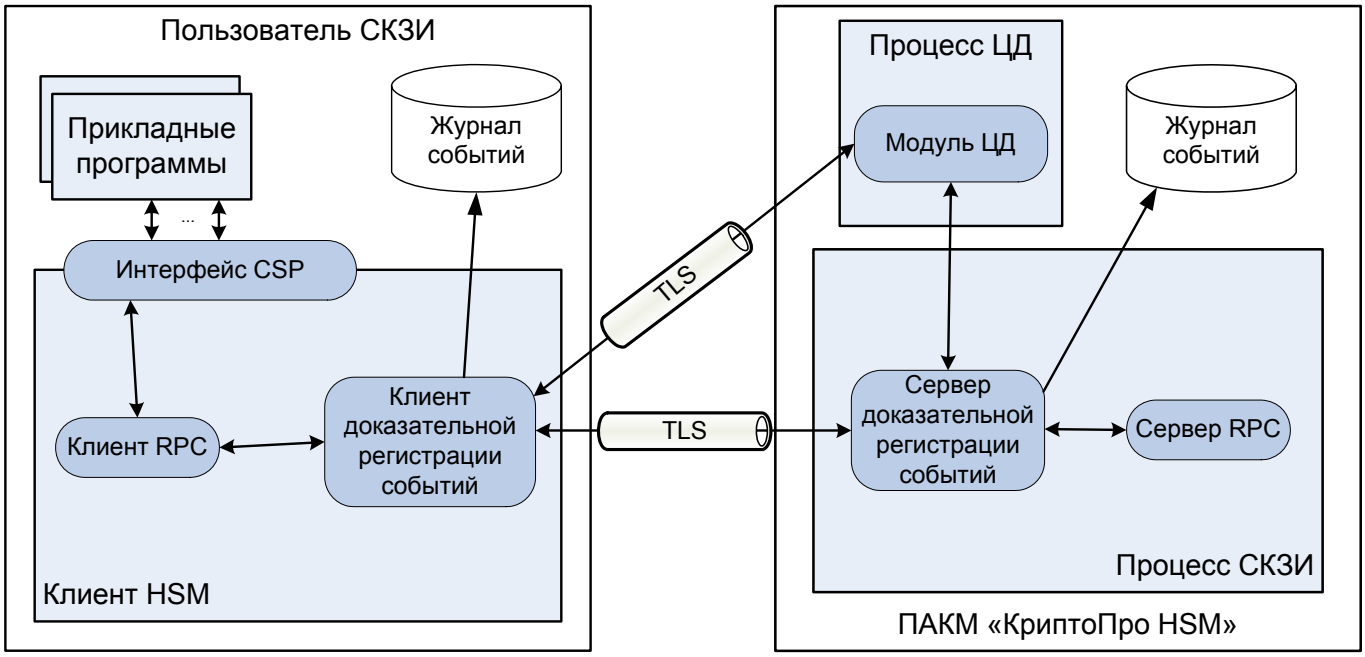

Рис. 5. Архитектура подсистемы доказательной регистрации событий ПАКМ «КриптоПро HSM»

В задачу второго проекта входила разработка подсистемы «Электронный нотариат» федерального центра поддержки межведомственного автоматизированного электронного взаимодействия и обмена, обеспечения доступа органов государственной власти, населения и организаций к ключевым государственным информационным ресурсам (федеральный информационный центр – ФИЦ).

Основной целевой функцией подсистемы «Электронный нотариат» ФИЦ является подтверждение подлинности ЭЦП. Эта функция осуществляется в следующем порядке:

1. В подсистему «Электронный нотариат» ФИЦ от пользователя поступает документ с подтверждаемыми (исходными) ЭЦП для проверки. Документ принимается, если он соответствует формату, установленному в Правилах проверки исходной электронной цифровой подписи.

2. Подсистема «Электронный нотариат» ФИЦ осуществляет проверку подтверждаемых (исходных) подписей документа в соответствии с Правилами проверки исходной ЭЦП.
3. Если проверка подтверждаемых (исходных) подписей в соответствии с Правилами проверки исходной ЭЦП прошла успешно, то подсистема «Электронный нотариат» ФИЦ подтверждает подлинность исходных подписей путём формирования подтверждающей ЭЦП под электронным документом.

Одним из возможных вариантов использования услуг подсистемы «Электронный нотариат» ФИЦ является автоматизированная подача документа с подтверждаемыми ЭЦП в ФИЦ с его последующей обработкой и выдачей ответа также в автоматическом режиме. Данный вариант применения актуален для электронных торговых площадок, которым требуется взаимодействие с зарубежными контрагентами. Для признания юридической значимости ЭЦП при трансграничном взаимодействии ФИЦ выступает в роли ЦД, который проверяет подлинность исходной ЭЦП, созданной с использованием несертифицированных в России средств ЭЦП по зарубежным алгоритмам. Подтверждающая подпись создаётся на российских алгоритмах с помощью сертифицированных средств ЭЦП, что обеспечивает признание подписей, созданных с использованием зарубежных алгоритмов, пользователями электронной торговой площадки. Разрешение споров во всех случаях происходит в российском суде по российским законам.

Для обеспечения доказательной силы регистрационных записей автоматические обращения для подтверждения подлинности ЭЦП осуществляются с применением протокола доказательной регистрации событий, описанного в четвёртой главе. Архитектура части подсистемы «Электронный нотариат» ФИЦ, реализующей протокол доказательного аудита, представлена на рис. 6.

В заключении приведены основные результаты диссертационной работы.

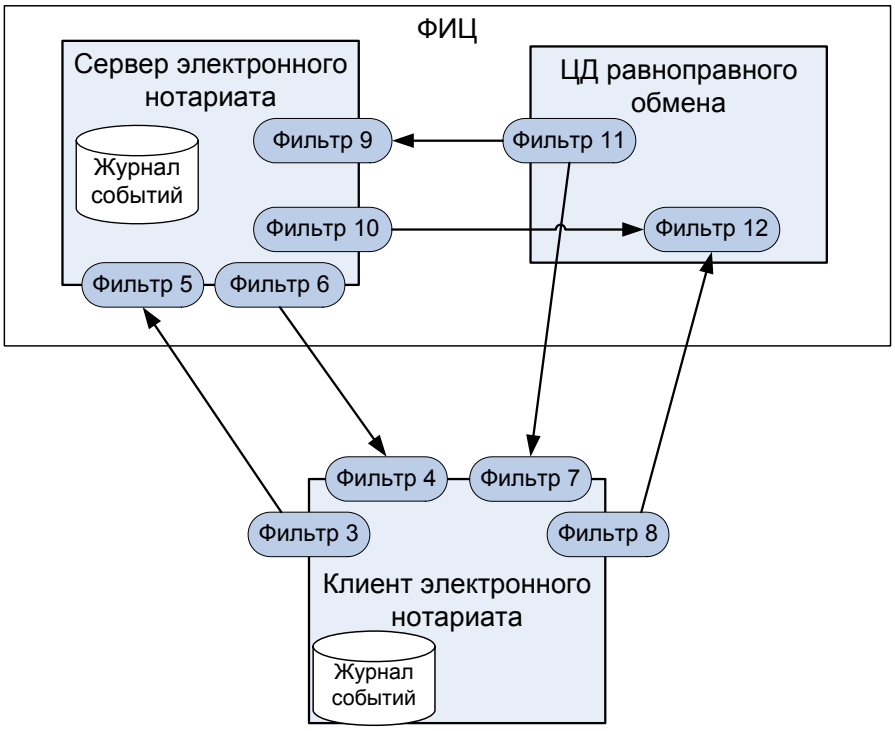

Рис. 6. Архитектура подсистемы «Электронный нотариат» ФИЦ

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

Основным научным результатом исследования является разработка методик и обобщённых протоколов, позволяющих осуществить доказательную регистрацию событий в любой системе.

В процессе выполнения данной работы были получены следующие теоретические и практические результаты:

1. На основе анализа предложенных в литературе протоколов равноправного обмена различных типов бизнес-документов с различной степенью участия ЦД, а также обобщённых протоколов равноправного обмена, применимых к любым типам бизнес-документов, сделан вывод о недостаточной проработке этих протоколов. Свойство невозможности отказа не является неотъемлемой частью ни одного из известных протоколов равноправного обмена. С использованием существующих протоколов нельзя решить общую задачу равноправного обмена произвольными типами бизнес-документов с обеспечением невозможности отказа от обмена.

2. В терминах теории распределённых алгоритмов предложена модель протокола равноправного обмена в виде набора взаимодействующих процессов, отправляющих друг другу сообщения по асинхронной сети. Приведены формальные определения бизнес-документа, протокола оптимистичного неотказуемого равноправного обмена в рамках данной модели. Предложены методики преобразования произвольного протокола передачи бизнес-документа для получения свойств генерируемости или доказуемости отправки, которые могут быть применены для адаптации произвольных бизнес-документов к существующим и новым протоколам равноправного обмена, использующим эти свойства.

3. Построены три новых обобщённых протокола неотказуемого равноправного обмена для бизнес-документов, протоколы передачи которых обладают свойствами доказуемости отправки или генерируемости. Протоколы обладают различными свойствами и предъявляют разные требования к инфраструктуре, что обуславливает их применимость в различных системах. Для двух из построенных протоколов достигнута граница минимальной дополнительной сложности в смысле числа сообщений и единиц времени выполнения. Предложен протокол неотказуемого равноправного обмена зависимых бизнес-документов. Корректность всех построенных протоколов доказана в рамках введённой модели протокола равноправного обмена. Разработанные протоколы в совокупности с результатами предыдущей главы решают общую задачу неотказуемого равноправного обмена произвольными бизнес-документами.

4. Сформулирована задача доказательной регистрации событий. Обобщённые схемы неотказуемого равноправного обмена применены для построения конкретного протокола доказательной регистрации событий. Специфицированы представления сообщений протокола доказательной регистрации событий вызова удалённых процедур по протоколу SOAP RPC на языке XML с учётом международных рекомендаций и стандартов. Реализована система доказательной регистрации событий обращений к веб-сервисам, использующая разработанный протокол.

5. Разработанный протокол доказательной регистрации событий применён для обеспечения доказательной силы регистрации криптографических операций, осуществляемых пользователями средства криптографической защиты информации

на программно-аппаратном криптографическом модуле «КриптоПро HSM». Опытный образец системы доказательной регистрации событий обращений по протоколу SOAP RPC применён для обеспечения доказательной регистрации событий автоматизированной подачи электронных документов на подтверждение подлинности ЭЦП в подсистеме «Электронный нотариат» ФИЦ.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Смирнов П.В., Челпанов А.В. О несоответствии стандартам процедуры построения цепочек сертификатов в ОС семейства Microsoft Windows // Безопасность Информационных Технологий. – 2004. – №4. – с. 93-95.
2. Смирнов П.В. Балансировка нагрузки и отказоустойчивость при проверке статусов сертификатов в ИОК // PC Week Russian Edition. – 2004. – №44. – с. 24-26.
3. Смирнов П.В. Метод обеспечения балансировки нагрузки и отказоустойчивости при проверке статусов сертификатов в ИОК // Безопасность Информационных Технологий. – 2005. – №4. – с. 50-56.
4. Смирнов П.В. Получение необходимых для протоколов равноправного обмена свойств при передаче документов // Вестник МГУ леса. Лесной вестник. - М.: МГУ леса. – 2006. – Препринт №179. – 17 с.
5. Смирнов П.В. Обеспечение отказоустойчивости при проверке статуса сертификата открытого ключа // В сб. научных трудов XII Всероссийской конференции «Проблемы информационной безопасности в системе высшей школы». – Москва, 2005. – с. 61-62.
6. Смирнов П.В. Управление размером списка отзыва сертификатов как метод повышения отказоустойчивости // В сб. тезисов Международной научно-практической конференции «Информационная безопасность». – Таганрог, 2005. – с. 194-195.
7. Смирнов П.В. Способ задания времени отзыва сертификата для решения проблемы с кэшированием CRL // В сб. материалов XIV Общероссийской научно-технической конференции «Методы и технические средства обеспечения безопасности информации». – Санкт-Петербург, 2005. – с. 70.
8. Смирнов П.В. Учёт выходных дней в расписании публикации CRL для Центра Сертификации Microsoft // В сб. научных трудов XIII Всероссийской конференции «Проблемы информационной безопасности в системе высшей школы». – Москва, 2006. – с. 102-103.
9. Смирнов П.В. Доказательный аудит на основе протокола неотказуемого равноправного обмена // В сб. материалов XV Общероссийской научно-технической конференции «Методы и технические средства обеспечения безопасности информации». – Санкт-Петербург, 2006. – с. 120.

Подписано в печать 10.04.2007 г.
Формат 60x90 $^{1}/_{16}$. Объем 1,5 печ.л. Тираж 100 экз.

Государственное образовательное учреждение
высшего профессионального образования
Московский инженерно-физический институт
(государственный университет)
115409, г. Москва, Каширское шоссе, д.31