ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF EDUCATION AND SCIENCE
OF THE REPUBLIC OF KAZAKHSTAN

Л.Н. ГУМИЛЕВ АТЫНДАҒЫ
ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ
ЕВРАЗИЙСКИЙ НАЦИОНАЛЬНЫЙ
УНИВЕРСИТЕТ ИМ. Л.Н. ГУМИЛЕВА
GUMILYOV EURASIAN
NATIONAL UNIVERSITY

ЖАС ҒАЛЫМДАР КЕҢЕСІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2015» атты X Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ X Международной научной конференции студентов и молодых ученых «Наука и образование - 2015»

PROCEEDINGS of the X International Scientific Conference for students and young scholars «Science and education - 2015»

УДК 001:37.0
ББК72+74.04
Ғ 96

Ғ96
«Ғылым және білім – 2015» атты студенттер мен жас ғалымдардың X Халық. ғыл. конф. = X Межд. науч. конф. студентов и молодых ученых «Наука и образование - 2015» = The X International Scientific Conference for students and young scholars «Science and education - 2015». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie-2015/, 2015. – 7419 стр. қазақша, орысша, ағылшынша.

ISBN 978-9965-31-695-1

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001:37.0
ББК 72+74.04

ISBN 978-9965-31-695-1

жүйе уақыт ағымымен тексеріле отырып, сол уақыт аралығында жұмысқа керекті жаңа талаптар айқындалады. Табылған нағыз үйлесімді шешімдер бағдарламаның өмірлік цикліне әсер етеді, оның дұрыс жұмыс жасауын жақсартады. Қарастырылған жұмыс нәтижесінде, алға қойған міндеттің шешімім табу мақсатында, белгілі бір сала бойынша жұмыс жасалынды. Программаны жасау барысында объектілер арасындағы байланыстар қатаң сақталынып жасалды. Сонымен қатар, программалық жабдықтаманың интерфейсі қолданушыға өте түсінікті етіп істелінді. Жаңа технологиялар негізінде айтылған жобаның веб және мобильді қосымшасы жасалды. Бағдарламаны мектеп оқушылары, студенттер, қазақ тілін үйренем деушілер, қазақ тілін зерттеушілер және т.б адамдар қолдана алады.

Қолданылған әдебиет

1. TextAnalyst 2.0 – персональная система автоматического анализа текста //http://www.analyst.ru.
2. Сулейманов Д.Ш., Аюпов М. Семантический анализ естественно-языковых текстов в вопросно-ответном режиме, 2003.
3. Автоматическая Обработка Текста //http://www.aot.ru.
4. Википедия: Cyc – проект по созданию объёмной онтологической базы знаний //http://ru.wikipedia.org/wiki/Cyc.
5. Тематический анализ для естественно-языковых текстов //http://www.dialog-21.ru/dialog2006/materials/html/Gladun.htm.

УДК 004.75

ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ В СИСТЕМЕ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ

Молдашова Жибек Кудабаевна
zhiba_best@mail.ru
Магистрант Евразийского национального университета им. Л.Н.Гумилева, Механико-математический факультет, Астана, Казахстан
Научный руководитель – Д.Қозыбаев

Системы электронных платежей получает все большее распространение в современной банковской индустрии. Являясь аналогами традиционных банковских платежных систем наличных и безналичных расчетов, они вместе с тем имеют целый ряд специфических особенностей, порождающих совершенно новые требования к их безопасности: предотвращение повторной траты монеты, обеспечение невозможности подделки «электронных денег» и др.

Проектирование и эксплуатация любых сложных информационных систем, к которым, безусловно, относятся и системы электронных платежей, требует определенной научно-методической основы[1]. Как правило, в целях удобства рассмотрения системы специалистами различных предметных областей и потребителями приходится выделять несколько уровней структурирования системы, отличающихся степенью детализации элементов. Для любой крупной информационной системы можно отметить как минимум три таких уровня: операционный (в иностранной литературе часто называемый также «бизнес-взгляд»), системный и технический. Разноуровневые взгляды отражают различные способы модельного представления системы электронных платежей. Рассмотрим различные уровни модельного представления системы электронных платежей.

Операционный взгляд («бизнес-взгляд») - это рассмотрение системы в аспекте эффективной поддержки деловой деятельности человека в той предметной области, для которой она предназначена.

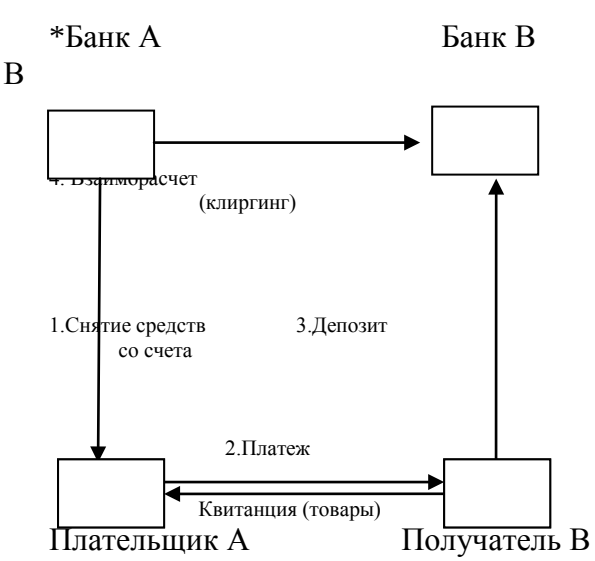
Системный взгляд - это рассмотрение информационной системы в аспекте ее системной

организации (т. е. как организованной совокупности взаимосвязанных элементов), определяемой требованиями операционного взгляда. На этом уровне выделяют такие структурные элементы, как отдельные вычислительные системы, каналы связи, маршрутизаторы и т.п., говорят о способах организации вычислений, распределении функциональности между структурными элементами системы, выборе и разработке системного и прикладного программного обеспечения, выдвигают требования к интеграции в системе различных функций.

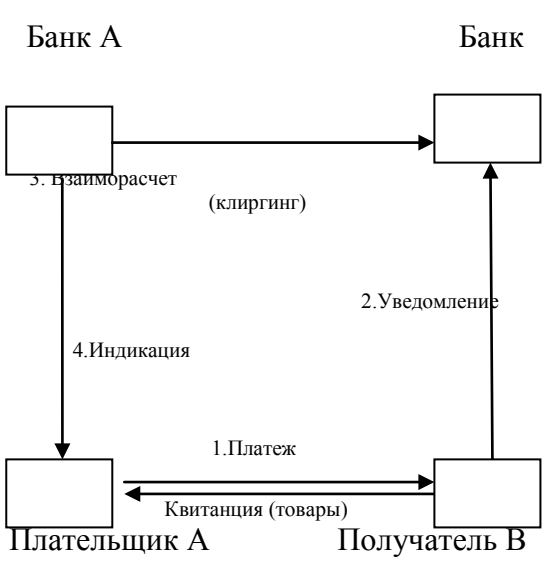
Технический взгляд - это рассмотрение информационной системы в аспекте ее технического построения, практической реализации, конкретных способов организации ее работы. При рассмотрении технических деталей реализации систем оперируют спецификациями, стандартами и иными нормативно-техническими документами. На первый план выходят понятия переносимости и способности к взаимодействию между отдельными элементами системы.

В любой системе электронных платежей всегда можно выделить четыре главных участника: *плательщика **А,** получателя* платежа **В**, *банк плательщика* и *банк получателя***.** Иногда для упрощения схем движения денежных средств считают, что плательщика и получателя обслуживает один и тот же банк.

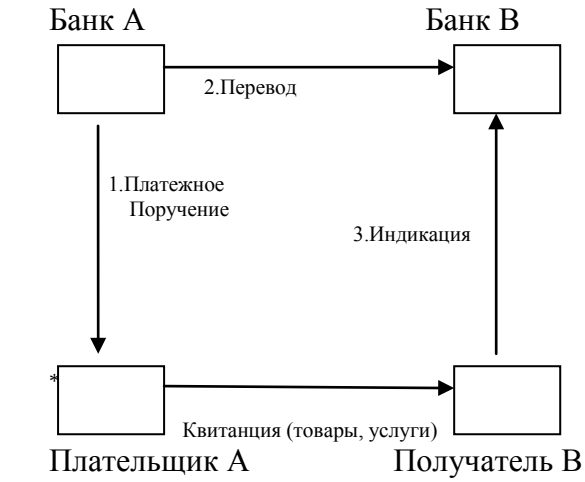
Системы наличных платежей



Система платежей по чекам или кредитным картам



Системы денежных переводов



Системы с дебетными поручениями

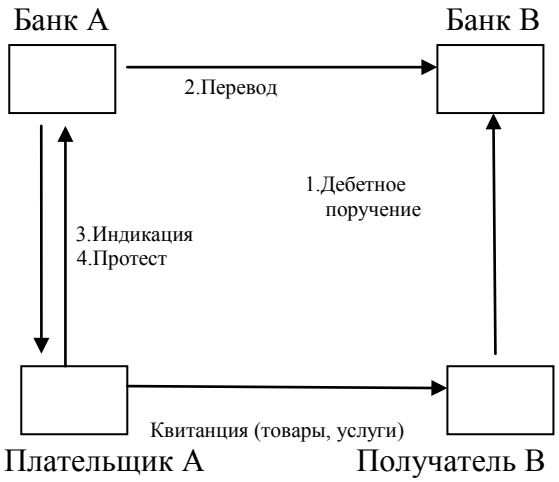


Рисунок 1- Типы платежных банковских систем

Системы наличных платежей похожи на традиционную систему эмиссии и обращения реальных наличных денег: монет и банкнот. Основные операции в системах наличных платежей таковы:

1. Плательщик ***A*** выполняет операцию *снятия средств со счета*, в ходе которой он получает наличные деньги от банка, а банк вычитает соответствующую величину со счета плательщика.

2. Плательщик ***A*** при покупке товаров или при оплате услуг вручает наличные деньги непосредственно получателю ***B*** - так выполняется операция *платежа***.**

3. Получатель ***B*** депонирует деньги на свой банковский счет - это операция *депозита.*

4.В системе электронных платежей (в отличие от традиционного устройства наличных расчетов) необходимо провести *взаиморасчет*(или *клиринг**)*** между банками плательщика и получателя, т. е. необходимо некоторое взаимодействие между двумя банками, в ходе которого приводятся в соответствие количества реальных и «электронных» денег в каждом из банков и на каждом из счетов плательщика и получателя[2].

Системы платежей по чекам или кредитным картам функционируют по иной схеме, а имен*но:

1. Плательщик ***A*** при выполнении *платежа* передает ***B*** свидетельство его согласия заплатить получателю некоторую сумму денег.

2. Получатель вручает это свидетельство своему банку (в системах с кредитными картами эта операция выполняется через специально вводимого в систему участника, называемого *эквайрером***).**

3. Банк получателя обращается к банку плательщика и запрашивает от него реальные деньги - это операция *клиринга***.**

4. Банк плательщика оповещает плательщика о том, что деньги действительно были выведены с его счета в соответствии с изъявленным им желанием.

Системы денежных переводов работают по следующей схеме: плательщик посылает платежное поручение в свой банк, который осуществляет взаиморасчет с банком получателя, а затем уже последний извещает получателя, что деньги достигли его.*Системы с дебетными поручениями* функционируют таким образом. Получатель извещает свой банк, что он должен получить деньги от некоторого плательщика, после чего банк получает их от банка предполагаемого плательщика. Банк плательщика извещает предполагаемого плательщика о снятии средств с его лицевого счета. В такой системе, очевидно, плательщику должно быть разрешено опротестовывать уже совершенные платежные операции. Обычно, чтобы ограничить злоупотребления, существует также предварительная фаза, где плательщик позволяет определенному получателю инициировать такие дебетные поручения (например, для оплаты телефонных счетов).

В самом общем виде цель обеспечения безопасности системы электронных платежей можно сформулировать как достижение *многосторонней безопасности (multi-partysecurity)**,*** т. е. учет всего множества требований по безопасности каждого участника и невозможность требовать никаких дополнительных гарантий доверия, кроме заранее установленных.Говоря более конкретно, в информационной безопасности системы электронных платежей можно выделить три традиционные составляющие: доступность, целостность, конфиденциальность. Существенно, что приоритетность решения этих задач в системы электронных платежей именно такова: на первом месте стоит *доступность*, затем целостность и только потом конфиденциальность. В самом деле, первостепенное значение для банковских систем имеет именно возможность пользоваться их услугами в любой момент времени, и только если такая возможность обеспечена, можно требовать обеспечения различных аспектов качества информации, циркулирующей в ней. Доля конфиденциальной информации в системе электронных платежей весьма мала (это, вероятно, будут только персональные данные клиентов и сведения, составляющие тайну вкладов), а вот нарушение целостности

финансовой информации может привести к весьма существенным экономическим потерям.

Некоторые электронные платежные системы не используют никакой криптографической защиты вообще[3]. Плательщик при выполнении платежа просто посылает получателю в открытом виде номер своей кредитной карты. Это безопасно для плательщика (пока кто-то другой не умеет подделывать его собственноручную подпись), хотя полностью небезопасно с точки зрения криптографии. Такого рода система платежей является «электронным» аналогом так называемых MOTO-транзакций (mailorder/transferorder), где покупатель заранее уведомляет продавца о желании приобрести тот или иной товар (услугу), но предполагаемый получатель платежа не имеет подписи плательщика, т. е. клиент может отказаться от предъявляемого ему при поставке товара счета. Это условие вполне логично, так как получатель не имеет никаких реальных свидетельств того, что плательщик действительно желает заплатить ему деньги.

В некоторых, не очень ответственных случаях использование таких платежных систем вполне допустимо, например для магазинов, продающих книги в малых количествах физическим лицам с доставкой на дом. Издержки, связанные с вероятными отказами заказчиков от поставляемого им товара, в таких случаях компенсируются продавцом за счет повышения цен на свои товары.Примером такой системы является система платежей в сети Интернет FirstVirtual.

Другой возможный вариант построения простой системы электронных платежей - проведение платежей по кредитным картам через защищенный канал, образуемый протоколом SSL, который предоставляет веб-браузер[4]. Того же можно достичь и используя обычную схему аутентификации с фиксированными либо одноразовыми паролями, общими для системы и клиентов. По защищенному каналу передается номер кредитной карты покупателя или другой пароль, но не подпись плательщика.Для плательщика такая система по-прежнему является безопасной, но для получателя платежа риск снижается, так как для атакующего собирать номера кредитных карт становится намного сложнее из-за необходимости решать задачи криптоанализа либо иным путем узнавать ключи (пароли), используемые клиентами системы.По этому принципу работает большинство локальных платежных систем и «электронных магазинов», действующих в сети Интернет.

В системах с симметричной аутентификациейэлектронных платежей имеет место аутентификация сообщений, передаваемых участниками системы, причем для этого используются симметричные методы аутентификации - генерация хеш-кодов при помощи хеш-функции с ключом. По сути дела, в этих системах электронных платежей имитируется классическая система бумажного банковского документооборота, только ручные подписи на документах заменяются хеш-кодами сообщений, для генерации которых используются общие секретные ключи, которые имеет каждая пара участников системы.Например, перевод денег со счета на счет между банками может быть выполнен путем простого обмена двумя сообщениями. В чековых системах это имеет смысл только для системы электронных платежей с неотложным выполнением платежей, так как получатель не может даже проверить аутентичность платежного сообщения - хеш-код может проверить только банк. Таким образом, получатель даже не знает, имеет ли плательщик сумму, необходимую для выполнения платежа, до тех пор, пока не получит сообщение от банка с хеш-кодом, который он сможет проверить.Примером такой системы электронных платежей являлась первоначальная версия системы электронных платежей NetBill, но новые версии этой системы электронных платежей стали использовать для аутентификации сообщений цифровую подпись.

Системы электронных платежей с аутентификацией сообщений посредством цифровой подписи открывают широкие возможности для построения аналогов традиционных банковских систем: чековых, систем денежных переводов, систем с кредитными картами. Ручные подписи на банковских документах заменяются цифровыми подписями, секретные ключи подписывающего хранятся на защищенных устройствах, а сама структура документооборота и формы документов остаются точно такими же, как в

традиционных платежных системах.

Список использованных источников

1. Запечников С.В. , Криптографические протоколы и их применение в финансовой и коммерческой деятельности: Учебное пособие для вузов.- М.: Горячая линия – Телеком, 2007.-320с.
2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. Учеб. пособие. - М.: Гелиос АРВ, 2001.-480 с.
3. Анохин М. И., Варновский Н. П., Сидельников В. М., Ященко В. В. Криптография в банковском деле: Метод, материалы. - М.: МИФИ, 1997.
4. Брассар Ж. Современная криптология. - М.: Полимед, 1999.

УДК 512, 519.688

СВОБОДНЫЕ И ВНЕШНИЕ МОДУЛИ СИСТЕМЫ КОМПЬЮТЕРНОЙ АЛГЕБРЫ GAP

Никитин Илья Александрович

vio.nik@mail.ru

Студент Павлодарского государственного университета им. С. Торайгырова

г. Павлодар, Казахстан

Научный руководитель – Ин. И. Павлюк

Областью исследования является система компьютерной алгебры GAP(Groups, Algorithms, Programming). Основным плюсом GAP являются открытые для редактирования свободные модули и создание собственных подмодулей [1].

Модуль – функционально завершенная часть программы, которая выполняет второстепенные задачи [2].

Система компьютерной алгебры GAP на данный момент имеет два типа модулей:

-частные – для матричных представлений элементов и групп;

-свободные модули и их подмодули для конечно определенных групп.

В GAP элементы свободных модулей хранятся в виде списков элементов. Для свободных модулей некоторые функции недоступны, такие как векторные пространственные функции и наборы теоретических функций [3].

В большинстве случаев для описания базовой концепции работы с теорией групп используют симметричную группу S^3. Напомним, математический вид группы S^3 представляется шестью элементами:

$$S^3 = \{e, a, a^2, b, ab, a^2b\}$$

Генетический код группы:

Подгруппы группы S^3 имеют вид:

$H_0 = \{e\}$ – тривиальная подгруппа;

$H_1 = \{e, a, a^2\} = C(a)$ – циклическая подгруппа порядка 3;

$H_2 = \{e, b\} = C(b)$ – циклическая подгруппа порядка 2;

$H_3 = \{e, ab\} = C(ab)$ – циклическая подгруппа порядка 2;

$H_4 = \{e, a^2b\} = C(a^2b)$ – циклическая подгруппа порядка 2;

.

Общая формула бинарного отношения сопряжения двух элементов имеет вид:

$$(a_c \equiv b) \overset{def}{\Leftrightarrow} ((\exists x \in G)(a^x = x^{-1}ax = b)).$$

Сопряженность – это классическое отношение эквивалентности на элементах группы [4].