МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Протоколы электронных денег

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Яшина Ивана Алексеевича

Научный руководитель
к. ф.-м. н., доцент _____ В. Е. Новиков
22.01.2022 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
22.01.2022 г.

Саратов 2022

ВВЕДЕНИЕ

В прошлом наличные деньги стали настоящим прорывом, которое позволило человечеству шагнуть на следующую ступень развития. Но со временем стали проявляться их недостатки. Они неудобны при носке и при оплате товаров и услуг. В случае утери их практически невозможно будет вернуть или как-то запретить их использование. Они легко повреждаемы и способствуют распространению микробов и вирусов.

Дебетовые карточки стали современным решением, которое было лишено всех недостатков наличных денег. Но при этом появилась новая проблема. При каждом платеже дебетовая карточка полностью идентифицирует своего владельца, что может привести к неприятным для него последствиям. Например, если оплачивать карточкой билеты на самолёт или поезд, а также поездки на такси и общественном транспорте, то у банка и организаций, предоставляющих услуги по перевозке, появляется возможность отслеживать перемещения владельца этой карточки, что является нарушением прав и свобод человека[1].

Если взглянуть на эту проблему более обобщённо, то задача состоит в создании системы контроля за доступом к ресурсам, которая удовлетворяет двум, казалось бы, взаимно исключающим требованиям:

- клиент должен иметь возможность обратиться к системе анонимно;
- клиент должен иметь возможность доказать право на доступ к ресурсу.

Наличные деньги удовлетворяют этим двум требованиям. С одной стороны, для того чтобы получить доступ к товару или услуге достаточно предоставить определённое количество денег. С другой, хотя на купюрах присутствует уникальный номер, отследить по нему кто и когда расплачивался не представляется возможным.

[1] Шнайер, Б. Прикладная криптография [Электронный ресурс] / Б. Шнайер. – М. : Триумф, 2002. - 1040 с. - Загл. с экрана. - Яз. рус.

Полноценной заменой наличных денег и дебетовых карточек, а также решением проблемы, описанной выше, являются протоколы неотслеживаемых электронных денег (далее просто электронные деньги). Первый кто занимался их разработкой является американский криптограф Дэвид Чаум[2].

На сегодняшний момент работа по этой теме разделилась на два направления. Одни занимаются созданием новых протоколов с необходимыми опциями для платёжных систем, а другие, в том числе и Дэвид Чаум, создают инструкции как внедрить в современную банковскую систему электронные деньги[3, 4, 5].

Целями данной работы являются систематизация протоколов электронных денег, рассмотрение существующих схем и программная реализация одной из них. Для этого требуется решить следующие задачи:

1) рассмотреть устройство платёжных систем;

2) систематизировать разновидности протоколов электронных денег;

3) изучить и подробно расписать в виде протоколов конкретные разработанные схемы электронных денег;

4) создать сервис, демонстрирующий возможную реализацию одного из протоколов электронных денег на практике.

Дипломная работа состоит из введения, 6 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 65 страниц, из них 47 страниц – основное содержание, включая 17 рисунков и 2 таблицы, список использованных источников из 16 наименований.

---

[2] Ященко, В. В. Введение в криптографию [Электронный ресурс] / В. В. Ященко, Ю. В. Нестеренко, А. В. Черемушкин, А. Ю. Зубов. – М. : МЦНМО, 2012. - 348 с. - Загл. с экрана. - Яз. рус.

[3] User efficient recoverable off-line e-cash scheme with fast anonymity revoking [Электронный ресурс]. - URL: https://www.sciencedirect.com/science/article/pii/S0895717712001811#! (дата обращения: 15.11.2021). - Загл. с экрана. - Яз. англ.

[4] Date Attachable Offline Electronic Cash Scheme [Электронный ресурс]. - URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4052482/ (дата обращения: 25.11.2021). - Загл. с экрана. - Яз. англ.

[5] How to issue a central bank digital currency [Электронный ресурс]. - URL: https://www.snb.ch/en/mmr/papers/id/working_paper_2021_03 (дата обращения: 5.12.2021). - Загл. с экрана. - Яз. англ.

КРАТКОЕ СОДЕРЖАНИЕ

В дипломной работе в разделе 1 «Необходимые алгебраические основы» приведены математические конструкции, на которых основываются рассматриваемые здесь протоколы электронных денег.

Группой $(G, *)$ называется некоторое множество G с бинарной операцией $*$ на нём, для которого выполняются следующие три условия:

1) операция $*$ *ассоциативна*, то есть для любых $a, b, c \in G$ будет справедливо равенство

$$a * (b * c) = (a * b) * c;$$

2) в G существует *единичный элемент* или просто *единица*, обозначаемый как e, такой, что для любого $a \in G$ будет справедливо равенство

$$a * e = e * a = a;$$

3) для каждого $a \in G$ существует *обратный элемент* $a^{-1} \in G$, такой, что будет справедливо равенство

$$a * a^{-1} = a^{-1} * a = e.$$

Пусть a и b – произвольные целые числа и n – натуральное число. Будем говорить, что a *сравнимо с* b *по модулю* n, и будем писать $a \equiv b (mod\ n)$, если разность $a - b$ делится на n, то есть если $a = b + kn$ для некоторого целого числа k.

Для любого натурального числа a *функция Эйлера* от него будет равна количеству натуральных чисел не превосходящих a и взаимно простых с ним. Обозначается как $\varphi(a)$.

Группа, образованная множеством $\{[0],\ [1], \dots,\ [n-1]\}$ классов вычетов по модулю n с операцией сложения по модулю, называется *группой классов вычетов по модулю* n и обозначается $\mathbb{Z}_n$ [6, 7].

[6] Виноградов, И. М. Основы теории чисел [Электронный ресурс] / И. М. Виноградов. – Москва-Ленинград : Из-во Технико-Теоретической Литературы, 1952. - 184 с. - Загл. с экрана. - Яз. рус.

[7] Лидл, Р. Конечные поля. В 2 т. Т. 1. / Р. Лидл. – М. : Мир, 1988. - 808 с.

Во 2 разделе подробно рассматривается устройство платёжных систем, которые непосредственно реализуются протоколами электронных денег.

Платёжная система – это сервис, устанавливающий определённый набор правил, программных, аппаратных и технических средств, для перевода электронных денег от одной стороны другой.

В платёжных системах задействованы три участника: покупатель, магазин и банк. *Покупатель* применяет электронные деньги при осуществлении платежа. *Магазин* обменивает некоторый товар на электронные деньги. *Банк* выдаёт электронные деньги в обмен на наличные деньги, и наоборот. Покупатель и магазин являются *клиентами* банка и имеют счёт в нём.

Далее рассматриваются три основные транзакции платёжных систем: снятие со счёта, платёж и депозит. Транзакция *снятия со счёта* позволяет клиенту банка получить электронные деньги на запрошенную сумму. При этом счёт клиента уменьшается на эту сумму. С помощью транзакции *платежа* покупатель оплачивает покупки, обменивая их на электронные деньги. Транзакция *депозита* позволяет клиентам банка положить свои электронные деньги на счёт[8].

В 3 разделе даётся определение протоколам электронных денег, а также их систематизация по определённым свойствам.

Протоколами электронных денег называются специальные криптографические протоколы, разрабатываемые для работы с электронными деньгами.

Существуют различные виды протоколов электронных денег. *Диалоговые* системы требуют, чтобы магазин связывался с банком при каждой продаже, что очень похоже на сегодняшний протокол для дебетовых карточек. Если возникает

[8] Chaum, D. Security Without Identification: Transaction Systems to Make Big Brother Obsolete / D. Chaum // Communications of the ACM. - 1985. - V. 28, № 10. - P. 1030–1044.

какая-нибудь проблема, банк не принимает деньги. В этом случае у покупателя нет возможности совершить мошенничество[9, 10].

Автономные системы не требуют соединения между магазином и банком до окончания транзакции между магазином и покупателем. Эти системы не помешают покупателю смошенничать, но позволят определить злоумышленника постфактум. Покупатель, зная, что он будет раскрыт, не мошенничает[11, 12].

Протоколы электронных денег можно разделить и по другому признаку. В *неделимых* системах номинал электронных денег фиксирован, поэтому клиентам нужен ряд электронных монет различных номиналов. В *делимых* же используются электронные чеки, которые могут быть использованы для любых сумм до заданного максимума, а не потраченный остаток может быть возвращён на счёт.

В 4 разделе описываются диалоговые делимые и неделимые схемы электронных денег в виде протоколов. В них используется слепая цифровая подпись, в основе которой лежит схема подписи RSA.

Протокол. Генерация слепой подписи.

Вход. У Боба есть открытый ключ e, закрытый ключ d и открытый модуль n. Алиса хочет, чтобы Боб вслепую, не читая, подписал сообщение m.

Выход. Алиса получает подпись s сообщения m.

1) Алиса генерирует случайное число k, такое что $1 < k < n$.

2) Алиса отправляет Бобу число t, где $t = m * k^e (mod\ n)$. k^e – затемняющий множитель, которым Алиса маскирует сообщение m.

3) Боб отправляет Алисе число $b = t^d (mod\ n) = (m * k^e)^d (mod\ n) = = m^d * k (mod\ n)$. Боб подписывает сообщение t.

---

[9] Электронные платёжные системы на основе цифровых денег [Электронный ресурс]. - URL: https://intuit.ru/studies/courses/3580/822/lecture/30599?page=1 (дата обращения: 10.12.2021). - Загл. с экрана. - Яз. рус.

[10] Chaum, D. Online Cash Checks / D. Chaum // Advances in Cryptology - EUROCRYPT '89. - 1990. - P. 288–293.

[11] Ferguson, N. T. Single Term Off-Line Coins / N. T. Ferguson // Advances in Cryptology - EUROCRYPT '93. - 1994. - P. 318–328.

[12] Okamoto, T. An Efficient Divisible Electronic Cash Scheme / T. Okamoto // Advances in Cryptology - CRYPTO '95. - 1996. - P. 438–451.

4) Алиса вычисляет число $s = b * k^{-1}(mod\ n) = m^d(mod\ n)$, которое является подписью сообщения m. Алиса снимает затемняющий множитель и получает подпись Боба. ■

Проверка корректности подписи заключается в проверке на равенство сообщения m и s^e по модулю n.

В 5 разделе находится автономный неделимый протокол электронных денег, в основе которого лежит схема разделения секрета и так называемая случайная слепая подпись, благодаря которой можно получать подпись на случайное число, при этом на случайность выбора этого числа могут влиять и клиент, и банк. Получаемая здесь электронная монета содержит данные конкретного клиента. Из этого следует, что её можно использовать для платежа только один раз.

Протокол. Транзакция платежа.

Вход. У покупателя есть электронные монеты, состоящие из чисел a, b, c, k, v, $(C^kA)^{v^{-1}}$ и $(C^UB)^{v^{-1}}$, и идентифицирующая его информация U. Он хочет купить товар по цене, которая меньше суммы номиналов его электронных монет. Функция f с индексом является общедоступной.

Выход. Покупатель получает товар и сдачу, а магазин прибыль в кассу.

1) Покупатель отправляет магазину числа a, b, c, k и v каждой монеты.

2) Магазин генерирует и отправляет случайное число $x \in \mathbb{Z}_N$ неравное нулю.

3) Покупатель вычисляет и отправляет магазину $r = kx + U(mod\ v)$ и $(C^rA^xB)^{v^{-1}} = \left((C^kA)^{v^{-1}}\right)^x * (C^UB)^{v^{-1}}(mod\ N)$ для каждой монеты.

4) Магазин проверяет, что для каждой монеты выполняется сравнение по модулю $(f_c(c)^r f_a(a)^x f_b(b)) \equiv \left((C^rA^xB)^{v^{-1}}\right)^v(mod\ N)$. Если все проверки пройдены, то магазин кладёт для каждой монеты в кассу семёрку чисел $\left(a, c, k, v, (C^kA)^{v^{-1}}, x, r\right)$.

5) Магазин вычисляет сдачу, набирает монетами из кассы её сумму и способом, описанным на шагах с 1 по 4, возвращает сдачу покупателю.

6) Магазин выдаёт товар покупателю. ■

Протокол. Транзакция снятия со счёта.

Вход. У банка есть открытый ключ v, закрытый ключ v^{-1}, открытый модуль N, открытые числа g_a, g_b и g_c большого порядка в $\mathbb{Z}_N$, открытые односторонние функции $f: \mathbb{Z}_N \to \mathbb{Z}_v$ и $f_1: \mathbb{Z}_v \to \mathbb{Z}_N$, открытое простое число p, такое что $p \equiv 1(mod\ N)$, и открытые числа h_b и h_c порядка N в $\mathbb{Z}_p$.

Выход. Клиент получает электронную монету в виде набора из семи чисел. Такие наборы и идентифицирующая информация U клиента используются в качестве входных данных для протокола транзакции платежа.

1) Клиент генерирует случайные числа $a_1, b_1, c_1 \in \mathbb{Z}_N$, которые являются клиентской частью базовых чисел подписей.

2) Клиент генерирует случайные числа $\sigma, \tau, \varphi \in \mathbb{Z}_v$, которые являются экспоненциальными маскирующими факторами.

3) Клиент генерирует случайные числа $\gamma, \alpha, \beta \in \mathbb{Z}_N$, которые являются мультипликативными маскирующими факторами.

4) Клиент выбирает и отправляет в банк одно из открытых чисел v, в зависимости от того, какого номинала он хочет получить электронную монету по соглашению.

5) Клиент вычисляет и отправляет в банк числа $\gamma^v c_1 g_c^{\sigma}(mod\ N)$, $\alpha^v a_1 g_a^{\tau}(mod\ N)$ и $\beta^v b_1 g_b^{\varphi}(mod\ N)$.

6) Банк генерирует случайные числа $a_2, b_2, c_2 \in \mathbb{Z}_N$, которые являются банковской частью базовых чисел подписей.

7) Банк вычисляет и отправляет клиенту числа $h_c^{c_2}(mod\ p)$, a_2 и $h_b^{b_2}(mod\ p)$.

8) Клиент генерирует случайное число $k_1 \in \mathbb{Z}_v$, которое является клиентской частью коэффициента полинома, разделяющего секрет.

9) Клиент вычисляет $e_c = f\left(h_c^{c_1 c_2}\right) - \sigma(mod\ v)$, $e_b = f\left(h_b^{b_1 b_2}\right) - -\varphi(mod\ v)$, $a = \left(a_1 a_2 * f_1(e_c, e_b)\right)^{k_1}(mod\ N)$ и $e_a = k_1^{-1} f(a) - \tau(mod\ v)$.

Любое сокращение по модулю на этом шаге должно быть исправлено в окончательной подписи путём умножения её на подходящие степени чисел g_a, g_b и g_c.

10) Клиент отправляет в банк числа e_a, e_b и e_c.

11) Банк вычисляет числа

$$\bar{A} = \alpha^v a_1 g_a^\tau * a_2 * f_1(e_c, e_b) * g_a^{e_a} (mod\ N),$$

$$\bar{B} = \beta^v b_1 g_b^\varphi * b_2 * g_b^{e_b} (mod\ N) \text{ и}$$

$$\bar{C} = \gamma^v c_1 g_c^\sigma * c_2 * g_c^{e_c} (mod\ N),$$

которые являются закрытыми версиями чисел A, B и C.

12) Банк генерирует случайное число $k_2 \in \mathbb{Z}_v$, которое является банковской частью коэффициента полинома, разделяющего секрет.

13) Банк отправляет клиенту числа b_2, c_2, k_2, $(\bar{C}^{k_2} * \bar{A})^{v^{-1}}$ и $(\bar{C}^U * \bar{B})^{v^{-1}}$.

14) Клиент вычисляет $c = c_1 c_2 (mod\ N)$, $b = b_1 b_2 (mod\ N)$, $k = k_1 k_2 (mod\ v)$, $C = c g_c^{f(h_c^c)} (mod\ N)$, $A = a g_a^{f(a)} (mod\ N)$, $B = b g_b^{f(h_b^b)} (mod\ N)$, $S_a = \left((\bar{C}^{k_2} * \bar{A})^{v^{-1}} / (\gamma^{k_2} \alpha)\right)^{k_1}$ и $S_b = (\bar{C}^U * \bar{B})^{v^{-1}} / (\gamma^U \beta)$, и затем проверяет два сравнения по модулю $S_a^v \equiv C^k A (mod\ N)$ и $S_b^v \equiv \equiv C^U B (mod\ N)$. Если проверка прошла успешно, то в качестве результата клиент берёт набор $(a, b, c, k, v, S_a, S_b)$, где S_a и S_b – случайные слепые подписи, индексы которых обозначают базовые числа подписей. ■

В 6 разделе описан созданный в рамках этой дипломной работы веб-сайт по работе с электронными деньгами. Для его создания потребовалось разработать дополнительно протоколы регистрации и аутентификации при входе в систему, так как в любой платёжной системе необходима привязка конкретного

аккаунта к конкретному счёту в банке. На рисунке 1, 2 и 3 представлены веб-страницы, на которых реализованы соответствующие протоколы[13, 14, 15, 16].

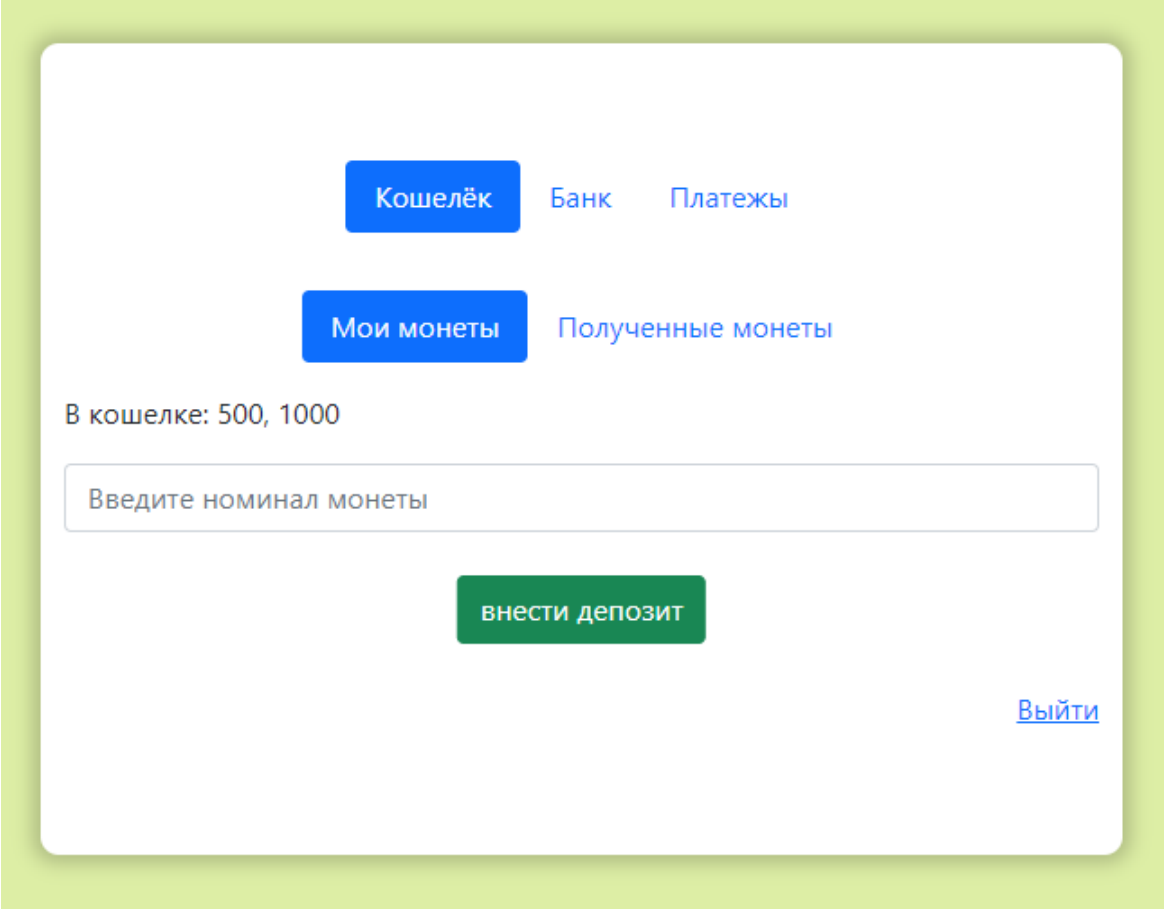

Рисунок 1 – Веб-страница для работы с кошельком

[13] IntelliJ IDEA [Электронный ресурс]. - URL: https://www.jetbrains.com/ru-ru/idea/ (дата обращения: 15.11.2021). - Загл. с экрана. - Яз. англ.

[14] Spring [Электронный ресурс]. - URL: https://spring.io/ (дата обращения: 15.11.2021). - Загл. с экрана. - Яз. англ.

[15] Spring initializr [Электронный ресурс]. - URL: https://start.spring.io/ (дата обращения: 15.11.2021). - Загл. с экрана. - Яз. англ.

[16] Oracle Java Downloads [Электронный ресурс]. - URL: https://www.oracle.com/java/technologies/downloads/#java8 (дата обращения: 15.11.2021). - Загл. с экрана. - Яз. англ.

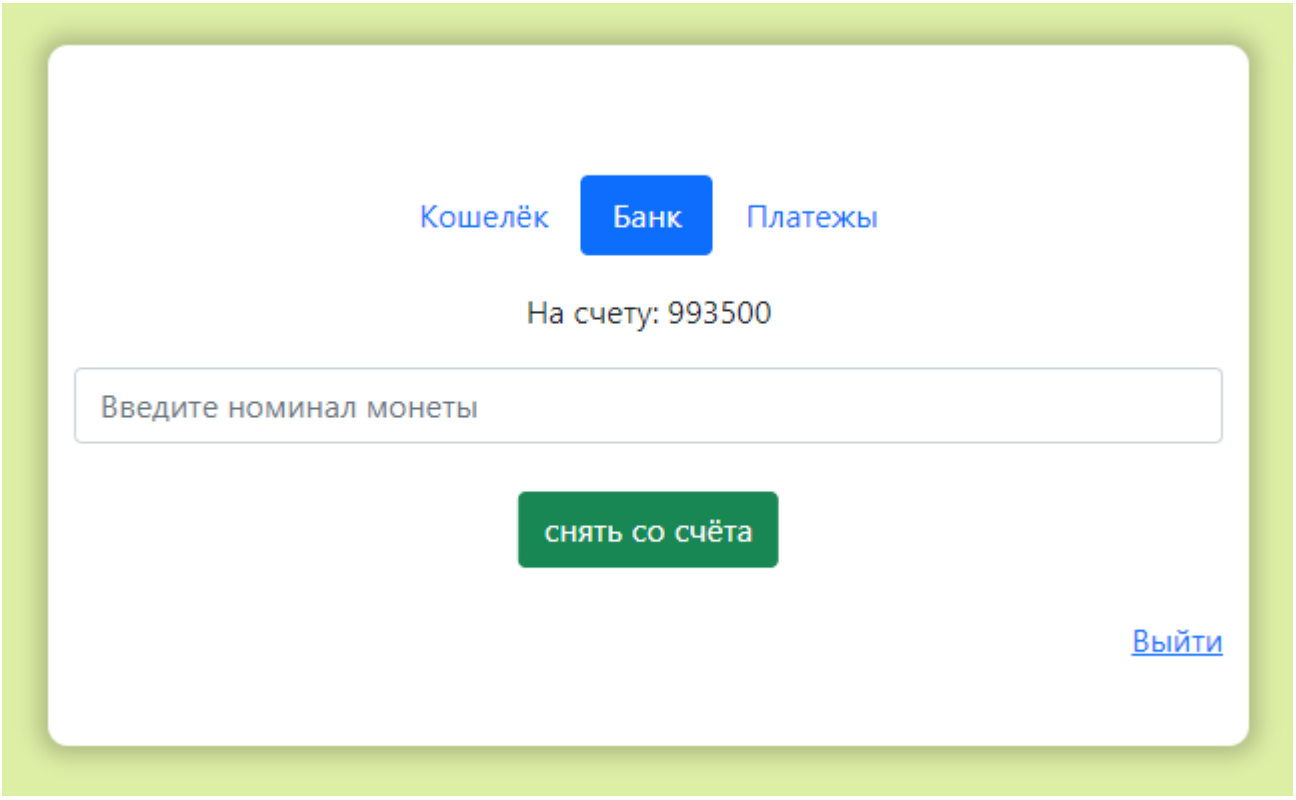

Рисунок 2 – Веб-страница для работы с банком

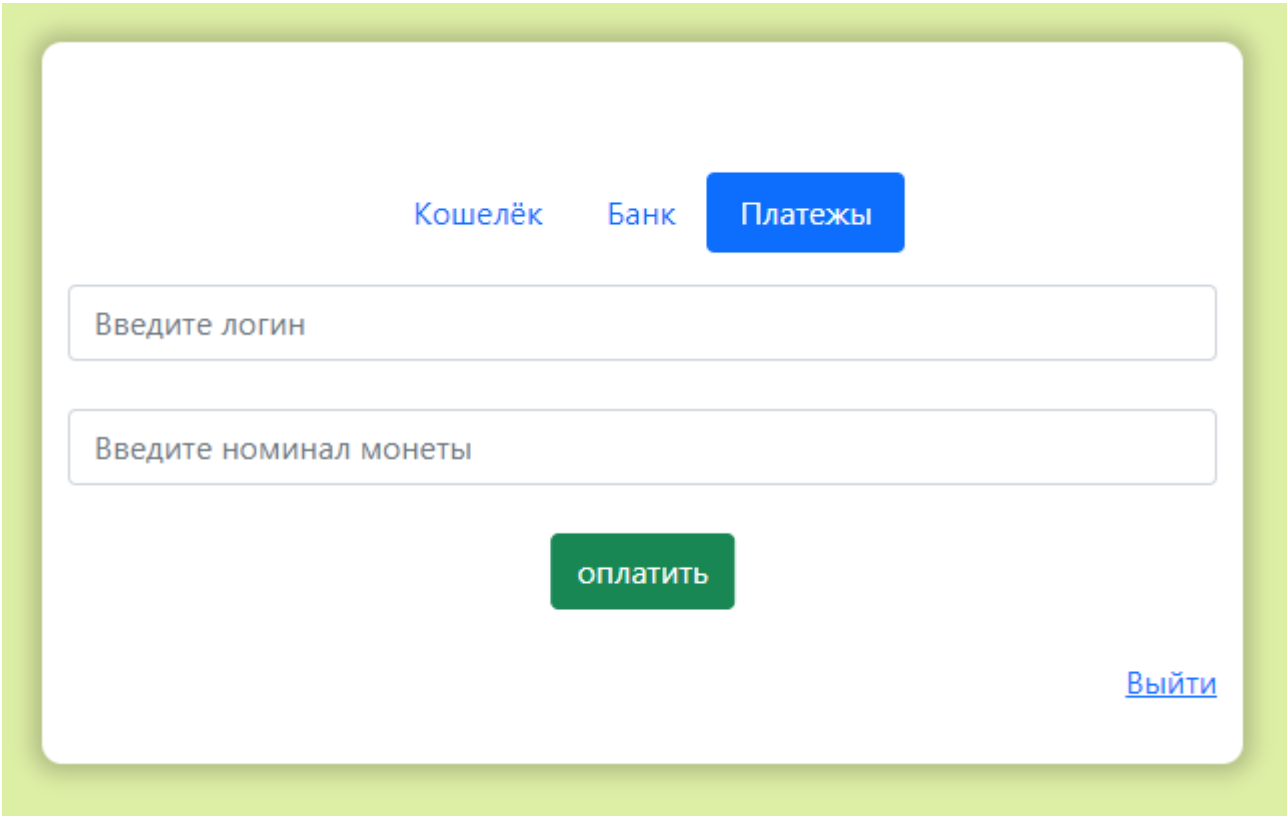

Рисунок 3 – Веб-страница для платежей

ЗАКЛЮЧЕНИЕ

В данной работе были проанализированы и сформулированы в виде протоколов системы электронных денег. Также был создан сервис по работе с электронными деньгами, реализующий всю функциональность, которую они предоставляют. Важным выводом этой работы является тот факт, что протоколы электронных денег действительно способны на основе современных технологий создать платёжную систему, которая будет полноценной альтернативой наличных денег. Таким образом, все поставленные задачи полностью выполнены, цель работы можно считать достигнутой.