УДК 004.853

Проектирование архитектуры системы электронных денег

Р.В. Мальчева, К.А. Терещенко
ГОУВПО «Донецкий национальный технический университет»
E-mail: malcheva.raisa@yandex.ru

Аннотация
Рассмотрены базовые онлайн и офлайн архитектуры систем для внедрения механизмов и протоколов электронных денег. Рассмотрены основные схемы передачи платежей и проанализированы их узкие места. Предложен альтернативный подход, состоящий в распределении банковских обязанностей. Описана сервис-ориентированная архитектура SOA – многоуровневая архитектура, позволяющая оптимизировать как внутренние, так и внешние процессы. Выполнено моделирование бизнес-процессов в соответствии с принятой архитектурой. Определены ключевые факторы в модели облачных вычислений для систем электронных денег.

Введение

Новые технологии являются самым заметным признаком изменения экономических систем, в т.ч. банковских [1]. Некоторые авторы [2] предполагали, и с этим трудно не согласиться, что в 2018-2020 гг. закончится индустриальная фаза роста мировой экономики, и ее дальнейшее развитие будет осуществляться под все большим воздействием когнитивных факторов и производств, основанных на принципах аддитивных, нано- и биотехнологий. Основными направлениями такого развития будут [3, 4]:

- реализация концепции электронного правительства;
- воплощение идеи «цифрового города», что обусловлено комплексной информатизацией транспорта, ЖКХ и др.;
- воплощение идеи строительства «умного» и экологически безопасного дома, что потребует большого объема новых отделочных и строительных материалов;
- распространение разного рода альтернативных и свободных форм занятости в таких сферах, как бухгалтерские услуги, программирование, творческая деятельность и др.;
- создание многочисленных профессиональных сетей, где потенциальный работодатель размещает заказы.

Современная банковская система развивается в рамках общей стратегии развития и цифровизации Российской федерации, которая подразумевает [3, 5]:

- создание ИТ решений на базе открытых, модульных платформ;
- создание целевых платформ (ППС, ЕИСПД и др.);
- внедрение современных интеграционных ИТ решений и корпоративной интеграционной сервисной шины;
- внедрение инструментов автоматизации бизнес-процессов (BPM);
- развитие каналов взаимодействия, форматов и интерфейсов;
- организацию полнофункциональных личных кабинетов для клиентов Банка России и внедрение единых стандартов обмена (XBRL и др.).

До сих пор основное внимание в исследованиях электронных денег уделялось удовлетворению требований безопасности; вопросам архитектуры и реализации уделялось ограниченное внимание.

Ключевые требования, которые необходимо учитывать при проектировании распределенной архитектуры, включают: масштабируемость, открытость, неоднородность, безопасность, доступность, и производительность.

Целью данной статьи является анализ особенностей функционирования объектов и процессов компьютерной сети банка и проектирование архитектуры системы электронных денег.

Анализ архитектур систем электронных денег

Важным аспектом проектирования архитектуры системы электронных денег является применимость к реальному контексту и задачам. По сути, чтобы новая схема оплаты была принята профессионалами, она должна либо обеспечить значительное снижение затрат, чтобы оправдать инвестиции в необходимую

новую инфраструктуру, либо предоставить клиентам заметные дополнительные услуги.

Базовая онлайн-архитектура

Базовый стиль онлайн-архитектуры можно рассматривать как своего рода архитектуру по умолчанию, которая систематически использовалась во многих работах для внедрения механизмов и протоколов электронных денег. Базовая онлайн-архитектура обычно включает три типа ролей: Банк, Плательщик и Получатель платежа (рис. 1).

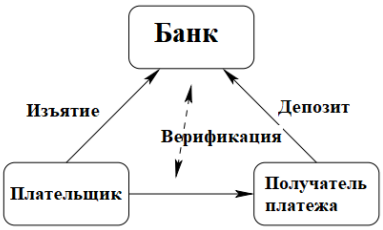

Рисунок 1 – Базовая онлайн-архитектура

В этой конфигурации потребителем является плательщик, который владеет монетами и использует их для покупки товаров или услуг. Получатель платежа получает монеты в обмен на оказанную услугу. Банк означает финансовое учреждение, которое выпускает и продает монеты потребителям, оказывает поддержку в проверке подлинности и целостности монет и выкупает монеты по запросу продавцов.

Электронные деньги, предлагаемые в большинстве современных онлайн-схем, могут быть представлены, в целом, в виде пары (*s, s0*), где *s* — ключ, который держится в секрете и *s0* это уникальный номер, который может быть обнародован и часто упоминается в качестве серийного номера. Обычно *s0* получается из *s* с использованием однонаправленной хеш-функции.

Для типичного изъятия плательщик генерирует (*s, s0*) и отправляет *s0* вместе с суммой монеты и дополнительной информацией в банк. Банк проверяет личность потребителя и остаток на счете. Если средств достаточно, банк дебетует счет и обновляет базу данных монет, перечисляя *s0* в качестве эталона для действительной монеты.

Для оплаты заказчик отправляет монету (*s, s0*) получателю платежа, который проверит действительность монеты, отправив ее в банк. Это позволяет избегать двойных расходов. В случае, если клиент пытается повторно использовать электронные деньги в другом месте, операция будет отклонена, потому что пароль будет недействителен.

Таким образом, получение права собственности на монету гарантирует получателю монеты, что ее действительность подтверждается банком, и что он является единственным владельцем.

Базовая онлайн-архитектура по своей сути является централизованной архитектурой, в которой большая часть коммуникаций проходит через банк. Постоянное участие банка делает его узким местом в производительности и единой точкой отказа, что является важным недостатком в распределенной среде. С другой стороны, это дает преимущество с точки зрения безопасности, поскольку позволяет обнаруживать двойные траты в режиме реального времени. Однако добиться невозможности отслеживания платежей с помощью базовой архитектуры может оказаться очень сложной задачей.

В некоторых предложениях базовая архитектура расширена за счет введения четвертой роли, которую играет доверенная третья сторона, например Центральный банк. В этих случаях некоторые обязанности банка передаются центральному банку, например, выпуск или публикация монет. Иногда такое распределение ответственности не только повышает эффективность системы за счет снижения нагрузки на банк, но и позволяет реализовать некоторые необходимые свойства, такие как анонимность или справедливость.

Процедура оплаты, используемая в этой схеме, аналогична описанной выше, с той разницей, что в этом случае монеты выпускаются отдельной организацией, отличной от банка - Эмитентом. Но сговор между банком и эмитентом, что не исключено, может привести к раскрытию личности потребителя.

То же самое можно сказать и о свойстве справедливости, которое зависит от готовности участников, таких как банк или эмитент, соблюдать протокол. Кроме того, хотя предложенная схема позволяет повторно использовать монеты в нескольких платежах перед их погашением, участие банка в этих операциях ставит под сомнение утверждение о переносимости.

Можно смягчить ограничения онлайн-платежей (например, единая точка отказа и узкое место в производительности) путем распределения накладных расходов на проверку монет между несколькими Эмитентами.

В целом базовая онлайн-схема предоставляет несколько практических преимуществ, когда речь идет о реализации ключевых функций безопасности, таких как предотвращение двойных расходов в режиме реального времени.

Однако это связано с потерей эффективности и масштабируемости из-за центральной роли, которую играет банк. Альтернативы могут состоять, например, в распределении роли, которую играет банк, между несколькими игроками или просто в устранении или уменьшении центрального положения, которое играет банк.

Базовая оффлайн-архитектура

Базовые автономные схемы возникли в результате попытки устранить некоторые недостатки, отмеченные ранее в онлайн схемах, за счет большей гибкости и автономии транзакций с электронными деньгами. Базовые автономные схемы также основаны на трехсторонней модели с теми же ролями, что и в предыдущей модели. Основное различие между обеими моделями заключается в том, что платежные операции происходят только между получателем и плательщиком, без участия банка.

Таким образом, банк больше не является узким местом в производительности и единой точкой отказа. Однако двойные траты могут быть обнаружены только постфактум, что может иметь некоторые негативные последствия.

Поскольку повышенная гибкость и автономия базовых автономных схем достигается за счет безопасности, заключающейся в обнаружении двойных расходов. Основное внимание в этих работах уделялось разработке надежных механизмов безопасности (например, схема со слепой подписью Чаумана [7] или улучшение через протоколы Шнорра, основанные на использовании доказательств с нулевым разглашением), которые устраняли бы это ограничение.

К сожалению, в целом эти механизмы безопасности оказались громоздкими и сложными, что фактически «свело на нет» прирост производительности и масштабируемости, достигнутый за счет предложенных схем. Таким образом, в распределенной обработке, где одинаково важны как безопасность, так и эффективность, необходимо найти правильный баланс, используя соответствующие компромиссы при разработке и развертывании базовых автономных схем.

Базовая переносимая архитектура

В базовой переносимой архитектуре участвуют как минимум четыре типа участников (рис. 2): Первоначальный плательщик, Конечный получатель, Платежный посредник, и Банк.

Рисунок 2 – Базовая переносимая архитектура

Первоначальный плательщик, Конечный получатель, и Банк играют ту же роль, что и в предыдущих схемах. Платежный посредник - это агент, который будет играть роль Получателя платежа или Плательщик по типу сделок.

Например, одна из первых переносимых схем включает банк *B* и *n* физических лиц *{Ci | 1 ≤ i ≤ n}*, которые могут играть роли потребителей или торговцев. *C1* берет монету из банка *B* и покупает какой-то предмет с *C2*, передав ему монету. Позже, *C2* повторно использует ту же монету при покупке с *C3*. Тот же процесс повторяется несколько раз, переходя от *Ci* к *Ci+1*. Окончательно после получения монеты последний человек в цепочке *Cn*, положит ее в банк.

Следует обратить внимание, что все промежуточные шаги в этой последовательности транзакций не используют обращение в банк. Хотя этот подход предлагает подходящую почву для автономной и распределенной обработки, он может обеспечить значительную масштабируемость и проблемы с производительностью.

Основная проблема при разработке переводимой схемы заключается в обнаружении двойных расходов. Поскольку передаваемые схемы по своей сути работают в автономном режиме, обнаружение двойных расходов происходит постфактум. Поэтому, если нет ограничения на количество разрешенных переводов, стоимость мошеннических транзакций (обнаруженных постфактум) может стать значительной. Таким образом, передаваемые схемы нуждаются в некоторых механизмах отслеживания для выявления мошенников и, как таковые, не могут одновременно гарантировать полную анонимность и безопасность.

Для решения данной проблемы можно использовать модель, состоящую из двух частей:

- фиксированный компонент, подписанный эмитентом, основанный на традиционном формате электронных денег;
- переменный компонент, подписанный во время транзакции, который записывает информацию о транзакции для обеспечения прослеживаемости.

Переменная составляющая позволяет защититься от двойных расходов за счет того, что личность каждого участника фиксируется в монете, в списке транзакций. Каждый элемент в списке транзакций состоит из фиксированного числа пар, полученных в результате разделения секрета на основе личности участника.

Для обеспечения конфиденциальности и выявления возможных двойных расходов, список случайным образом скрывается таким образом, что будущие участники не могут узнать личность предыдущих участников. Кроме того, в случае двойной траты вероятность того, что одни и те же предметы были случайно скрыты, будет низкой. С одной парой на элемент транзакции вероятность обнаружения мошенничества составляет 50 %. В то же время для достижения

вероятности обнаружения мошенничества, равной 98 %, потребуется 6 пар.

Этот способ обнаружения двойных расходов очень интересен, но для его реализации требуется доверенная третья сторона, называемая в модели устройством точки продажи (POS). Оно отвечает за сокрытие и подписание второй части монеты. Рассмотренную модель можно отнести к категории работающих в автономном режиме в том смысле, что присутствие банка не требуется, но все же необходимо присутствие внешней стороны, которая не является ни плательщиком, ни получателем платежа.

Таким образом, защита от двойных расходов может быть достигнута только за счет компромисса с анонимностью. Кроме того, при ее реализации могут резко возрасти основные проблемы масштабируемости и производительности.

Распределенная архитектура

Учитывая, что в онлайн-схемах банк является основным узким местом, а офлайн-платежи представляют собой способ устранить узкое место, созданное банком, предложен альтернативный подход, который заключается в распределении банковских обязанностей (рис.3) .

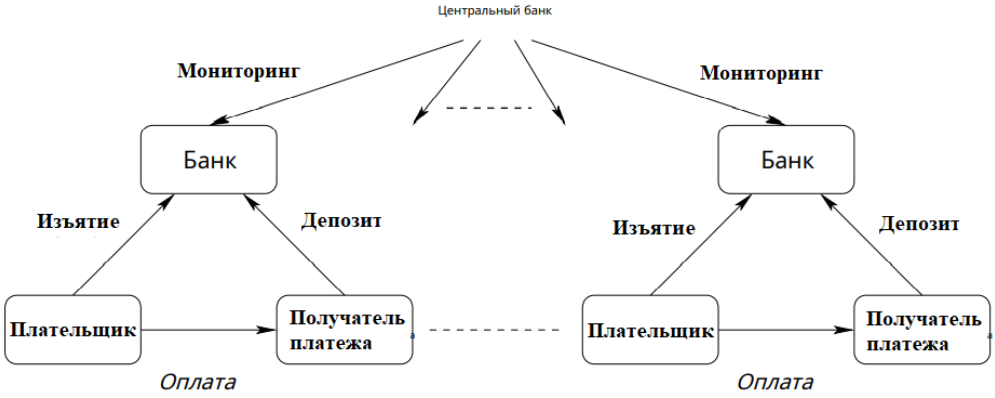

Рисунок 3 – Распределенная архитектура

Модель распределенного банкинга основана на том, что электронные платежные системы в настоящее время разрабатываются и управляются банками отдельно и независимо друг от друга. Т.е. каждый банк поддерживает свой собственный платежный шлюз и инфраструктуру аутентификации [8]. Это не лучший способ оптимизировать использование ресурсов и, как правило, усложняет клиринговые операции, необходимые для сверки транзакций, выполняемых в разных банках.

Модификация базовой трехсторонней модели с учетом того факта, что транзакции могут осуществляться через большую группу банков, контролируемый центральным банком (см. рис. 3) предполагает расширение схемы групповой подписи. Схемы групповых подписей позволяют члену группы подписывать от имени остальных членов группы, не раскрывая личность подписавшего и делая невозможным связать две разные подписи, выданные одним и тем же членом группы. Однако в случае разногласий в схеме участвует назначенный член группы, который может определить лицо, подписавшее документ.

Положительная особенность групповых подписей заключается в том, что проверку подписи можно выполнять с использованием одного открытого ключа группы. К сожалению, при начальных схемах размер открытого ключа имеет тенденцию к росту вместе с размером группы, что неприемлемо в ситуациях, когда требуется масштабируемость.

Позже была разработана система, позволяющая избегать роста размера ключа. Предложенная схема отличается не только тем, что позволяет нескольким банкам распределять электронные деньги, но и позволяет скрыть не только личность потребителя, но и его банк.

В предлагаемой схеме рассматриваются четыре роли: потребитель, продавец, банки, образующие группу, и менеджер группы, которым может быть, например, центральный банк. Чтобы купить монету, потребитель сначала генерирует монету и отправляет ее в свой банк для подписи. Банк снимает номинал монеты со счета потребителя, вслепую подписывает монету и отправляет ее потребителю.

Существует еще целый ряд архитектур, позволяющих существенно оптимизировать данный процесс.

Сервис-ориентированная архитектура (SOA) [9] возникла как метод проектирования, который позволяет поставщикам программного обеспечения создавать/обертывать различные программные системы в виде доступных сервисов, которые могут быть легко опубликованы и доступны для деловых партнеров и клиентов и, следовательно, освобождают различные модули и системы от

одинаковых функций. По сути, в SOA всегда задействованы три основных участника: поставщик услуг, потребитель услуг, и сервисный реестр.

Поставщик услуг отвечает за создание, публикацию и обслуживание открытых сервисов.

Потребитель услуг несет ответственность за поиск услуг, отвечающих его деловым/техническим потребностям, с целью их использования.

Реестр услуг действует как посредник (база данных), который позволяет поставщику услуг регистрировать созданные услуги со всей необходимой информацией метаданных и инструкциями, которые могут помочь потребителям легко найти и использовать необходимую услугу.

SOA архитектура зависит от использования способов авторизации и веб-сервисов для совместной интеграции доступных (современных и устаревших) систем. Процесс интеграции разделен на две задачи [9]:

- интеграция интерфейсных систем вместе путем предоставления внутренних функций в виде набора веб-приложений;
- интеграция клиентских систем с серверной системой через интеграционную шину, которая будет действовать как единая точка доступа для всех запросов, поступающих от фронтенд-систем.

На рис. 4 приведен пример модели бизнес-процесса «Клиент выбирает продукт или услугу».

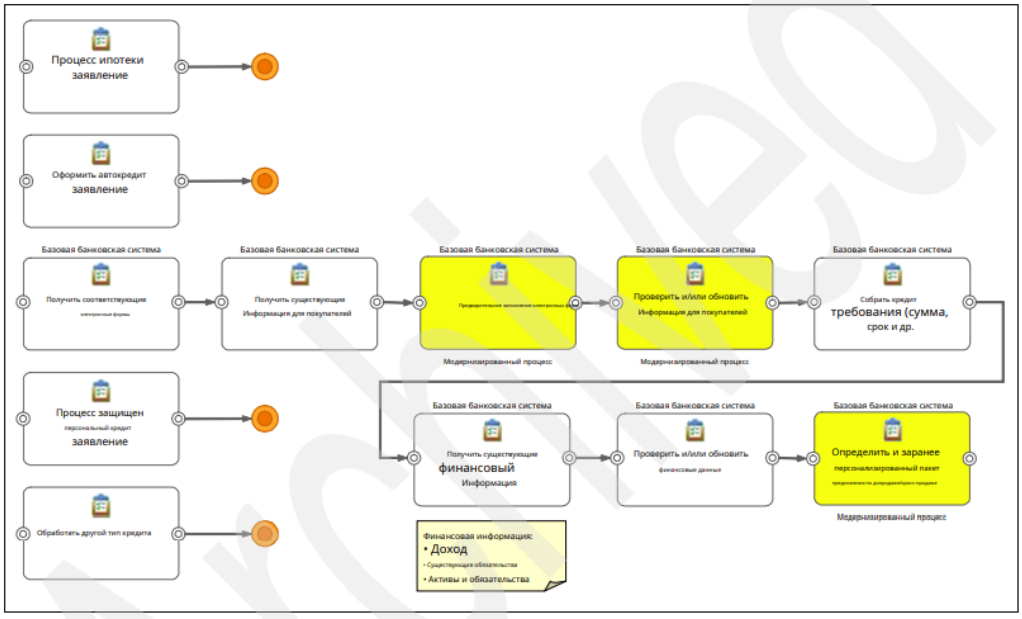

Рисунок 4 – Пример модели бизнес-процесса «Клиент выбирает продукт или услугу»

Использование облачных технологий

С точки зрения инфраструктуры можно выделить возможности, относящиеся к сервисной инфраструктуре и инструментам, которые могут предложить техническую основу для внедрения облака. В облачной инфраструктуре можно назвать такие элементы, как сервисы, предоставление и модель упаковки. С другой стороны, с точки зрения архитектуры есть возможности, которые определяют всю архитектуру и различные указания для включения в облако.

Бизнес- и стратегический компонент модели облачных вычислений позволяет реализовать облачную инициативу. Он охватывает такие элементы, как бизнес-инновации, желаемые выгоды, принципы координации, ожидаемые затраты.

Возможности, которые приобретают важное значение в облачной инициативе, представлены соглашениями о выборе услуг и уровне обслуживания. Ключевые факторы в модели облачных вычислений могут быть определены в таких компонентах, как: гибкость, снижение барьера для входа, стоимость и эффективность.

Традиционное развертывание приложения с административной точки зрения предполагает указание, закупку, настройку и развертывание аппаратного компонента, развертывание базы данных и приложения, а также настройку параметров.

Облачное развертывание можно охарактеризовать с точки зрения платформы, управляемой пользователем (платформа как развертывание службы) и с точки зрения портала развертывания: запрос на развертывание приложения, корректировка мощности по мере изменения спроса, отключение приложения, когда оно не требуется.

Облачное развертывание является распределенным, поскольку облачные системы

являются важной платформой для распределенных приложений.

В 2011 г. P. Mell и T. Grance предложили четыре модели развертывания как часть облачной модели для доступа к общему пулу вычислительных ресурсов: Частное облако, Облако сообщества, Публичное облако, Гибридное облако [10].

Для большинства банков первым крупным шагом в облачные вычисления станут частные облака. Созданы частные облака услуги связи для внутренних бизнес-пользователей. Эти сервисные компоненты очень эластичны и непрерывно расширяются. Банки могут заключать контракты по мере необходимости для удовлетворения требований к уровню обслуживания.

Технологии, лежащие в основе облака и относящиеся к ресурсам пулы, представлены виртуализацией, кластеризацией и сеткой. Виртуализация серверов и кластеризация обеспечивают объединение ресурсов и эластичную масштабируемость. Виртуализация определяет один ресурс как несколько виртуальных ресурсов.

Технология кластеризации делает один ресурс одним виртуальным ресурсом. Преимуществами этих технологий являются высокая эффективность, качество обслуживания и гибкость.

У клиентов есть выбор: развертывать эти технологии публично или использовать частные облака. Облачная технология упрощает динамическую замену узлов в кластере. Это позволяет легко и эффективно поддерживать уровни обслуживания при дальнейшем снижении затрат за счет улучшения оптимизация.

В то время как некоторые крупные банки с оптимизмом смотрят на внедрение облачных технологий, другие проявляют осторожность и ждут ответов на вопросы безопасности и регулирования.

В ходе одного из опросов специалистов по банковским технологиям [11] банкиров, выразивших интерес к облачным вычислениям, спросили, почему их это волнует. Большинство, 73%, указали на способность быстро удовлетворять потребности пользователей и масштабироваться в облаке.

Крупные организации могут воспользоваться этими услугами так же, как малые или начинающие предприятия. В то время как преимущество доступа к вычислительным услугам без больших капитальных затрат является очевидной привлекательностью для небольших компаний, крупные компании также могут извлечь выгоду из переноса некритичных для бизнеса вычислительных мощностей и приложений, не требующих большого объема данных, в облако. Некоторые из основных отмеченных преимуществ:

- лучший денежный поток и большая финансовая прозрачность, так как основное внимание уделяется операционным расходам, а не капитальным затратам;
- быстрое предоставление и эластичное масштабирование услуг;
- позволяет ИТ-отделу сосредоточиться на компетенциях, которые являются ключевыми для бизнеса;
- экологические преимущества [11].

Заключение

Модель распределенного банкинга пытается устранить узкое место в производительности, созданное банком, путем перераспределения и оптимизации выполняемых задач. Она обеспечивает лучшую масштабируемость по сравнению с базовой онлайн-моделью, сохраняя при этом тот же уровень безопасности.

Подход SOA в процессе интеграции означает не только создание набора веб-сервисов, но и способ, которым эти веб-сервисы будут встроены, чтобы позволить максимальному количеству потребителей их использовать, т. е. какие компоненты будут представлены как сервисы, структура этих услуг и то, как потребители смогут ими пользоваться.

Литература

1. Мальчева, Р. В. Компьютерные технологии – основа цифровой экономики // Бизнес-инжиниринг сложных систем: модели, технологии, инновации. Сборник материалов III международной научно-практической конференции. – Донецк: ДОННТУ, 2018. - С. 102-105.

2. Паньшин, Б. Цифровая экономика: особенности и тенденции развития [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/tsifrovaya-ekonomika-osobennosti-i-tendentsii-razvitiya

3. Терещенко, К. А. Анализ особенностей функционирования и развития объектов и процессов компьютерной сети банка / К. А. Терещенко, Р. В. Мальчева // Материалы XIII Международной научно-технической конференции в рамках VIII Международного Научного форума Донецкой Народной Республики ИУСМКМ-2022. - Донецк, ДОННТУ, 2022. – С. 392-395.

4. Дремач, К. Как банки подстраиваются под ситуацию [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Конференция:Конференция_ИТ_в_банках_2020?

5. Основные направления Стратегии ИТ Банка России [Электронный ресурс]. – Режим

доступа: https://ib8.ib-bank.ru/files/files/2016/03_kruchkov.pdf

6. Чеботарев, В. А. Проектирование компьютерной системы рейтингования деятельности банков [Электронный ресурс] / В. А. Чеботарев, Н. П. Путивцева // Инновационные аспекты развития науки и техники : материалы X Международной научно-практической конференции. – Режим доступа: https://cyberleninka.ru/article/n/proektirovanie-kompyuternoy-sistemy-reytingovaniya-deyatelnosti-bankov/

7. Молдовян А. А. Криптография: скоростные шифры / А. А. Молдовян и др. - СПб.: БХВ-Петербург, 2002. - 496 с.: ил. – URL: https://books.4nmv.ru/books/kriptografiya_skorostnye_shifry_3642800.pdf

8. Терещенко, К. А. Проектирование распределенной архитектуры компьютерной сети банка / К. А. Терещенко, Р. В. Мальчева // Информационное пространство Донбасса: проблемы и перспективы : материалы V Респ. С междунар. Участием науч.-практ. Конф., 27 окт. 2022 г. – Донецк : ГО ВПО «ДонНУЭТ», 2022. – С. 131 -134.

9. Service-oriented architecture [Electronic resource] – URL: htpps://learn.microsoft.com/en-us/dotnet/architecture/microservices/architect-microservice-container-applications/service-oriented-architecture

10. Mell, P. The NIST Definition of Cloud Computing [Electronic resource] / P. Mell, T. Grance // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD. - URL: http://dx.doi.org/10.6028/nist.sp.800-145.

11. BS&T Survey: Banks Take to Cloud Computing [Electronic resource] – URL: htpps://banktech.com/infrastructure/bsandt-survey-banks-take-to-cloud-computing/d/d-id/1293984d41d.html

Мальчева Р. В., Терещенко К. А. Проектирование архитектуры системы электронных денег. *Рассмотрены базовые онлайн и офлайн архитектуры систем для внедрения механизмов и протоколов электронных денег. Рассмотрены основные схемы передачи платежей и проанализированы их узкие места. Предложен альтернативный подход, состоящий в распределении банковских обязанностей. Описана сервис-ориентированная архитектура SOA – многоуровневая архитектура, позволяющая оптимизировать как внутренние, так и внешние процессы. Выполнено моделирование бизнес-процессов в соответствии с принятой архитектурой. Определены ключевые факторы в модели облачных вычислений для систем электронных денег.*

Ключевые слова: *архитектура, электронные деньги, моделирование, облачные технологии*

Malcheva R. V., Tereshchenko K. A. Designing the architecture of the electronic money system. *The basic online and offline architectures of systems for the implementation of mechanisms and protocols of electronic money are considered. The main payment transfer schemes are considered and their bottlenecks are analyzed. An alternative approach is proposed, consisting in the distribution of banking responsibilities. The service-oriented architecture of SOA is described – a multi-level architecture that allows optimizing both internal and external processes. Modeling of business processes in accordance with the accepted architecture is performed. The key factors in the cloud computing model for electronic money systems are identified.*

Keywords: *architecture, electronic money, modeling, cloud computing*

Статья поступила в редакцию 05.03.2023
Рекомендуется к публикации профессором Аноприенко А.Я.