

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

Институт информационных систем

Кафедра «Информационные системы»

Пояснительная записка

к расчетно-графической работе по дисциплине
«Методы и средства проектирования информационных систем»

Выполнил:

ст.гр. ИС/б-20-1-о

Галенин А. К.

Проверил:

доцент каф. ИС Карлусов В. Ю.

Севастополь

2023 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	3
1 ОПИСАНИЕ И АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ	5
2 ОБЗОР НОТАЦИЙ ДЛЯ ПОСТРОЕНИЯ ДИАГРАММ.....	6
2.1 Нотация DFD (DataFlowDiagrams – Диаграмма Поточков Данных)	6
2.2 Нотация IDEF0 (Integration Definition for Function Modeling).....	7
2.3 Нотация IDEF1X (Integration Definition for Information Modeling).....	8
2.4 Нотация IDEF3 (Integration DEFinition for Process Description Capture Method)	10
2.5 Нотация BPMN (Business Process Model and Notation)	11
3 ПРИМЕНЕНИЕ МЕТОДОЛОГИЙ ПОСТРОЕНИЯ ДИАГРАММ ДЛЯ ПРОЕКТИРОВАНИЯ СИСТЕМЫ «СИСТЕМА ПЕРЕВОДА СРЕДСТВ МЕЖДУ ЭЛЕКТРОННЫМИ КОШЕЛЬКАМИ НА ОСНОВЕ АЛГОРИТМОВ ZKP» С ИСПОЛЬЗОВАНИЕМ CASE СРЕДСТВ.....	13
3.1 Диаграммы в нотации DFD.....	13
3.2 Диаграмма в нотации IDEF0.....	14
3.3 Диаграммы в нотации IDEF1X.....	15
3.4 Диаграммы в нотации IDEF3	20
3.5 Диаграмма в нотации BPMN	24
ЗАКЛЮЧЕНИЕ	27

ВВЕДЕНИЕ

В современном мире наблюдается рост тенденций на внедрение блокчейн технологий в различных отраслях, в том числе и в экономической сфере. Это связано с тем, что данные технологии позволяют не только упростить и увеличить эффективность финансовых операций, но и обеспечить безопасность и прозрачность транзакций, что является неотъемлемым аспектом при проведении операций, связанных с денежными средствами.

При использовании приложений для электронных платежей остро стоит проблема о конфиденциальности данных, об их секретности. Большинство таких систем включают в себя сервисы для аутентификации, невозможности отрицания авторства. Такие возможности могут быть реализованы при помощи простых криптографических протоколов, например, TLS (Transport Layer Security). Протокол TLS – это протокол шифрования и аутентификации, он работает на транспортном уровне сетевой модели OSI, где отвечает за создание безопасных сессий обмена данными между браузером и сервером.

Однако существуют такие операции, которые невозможно защитить при помощи простых протоколов шифрования, вроде TLS. К таким операциям можно отнести электронные платежи, при проведении которых сохранение конфиденциальности является неотъемлемой частью, ведь при несоответствии приложения стандартам безопасности возникают риски утечки личных и финансовых данных пользователей. Также участники таких систем могут стать жертвой мошенничества, поскольку простые протоколы шифрования могут иметь уязвимости, из-за которых становится возможным получить доступ к персональным данным пользователей.

Более тонкие операции, такие как проведение электронных платежей, требуют внедрения более сложных криптографических алгоритмов, чтобы избежать возможности утечки пользовательских данных.

В связи с этим, актуальным является задача разработки системы перевода средств между электронными кошельками на основе алгоритмов доказательства с нулевым разглашением (Zero Knowledge Proof), что и является целью расчётно-графической работы. Доказательство с нулевым разглашением (ZKP) представляет собой криптографический протокол, который позволяет одной стороне (доказывающему, prover, P) убедить другую сторону (проверяющего, verifier, V) в истинности какого-либо утверждения, не раскрывая при этом никакой информации, подтверждающей это утверждение. ZKP может быть интерактивным, когда доказывающий повторяет процесс доказательства для каждого проверяющего, а также неинтерактивным, когда доказывающий создаёт доказательство, которым может воспользоваться каждый человек, использующий то же доказательство.

1 ОПИСАНИЕ И АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

Предметная область настоящей расчётно-графической работы – Система перевода средств между электронными кошельками на основе алгоритмов ZKP.

Основной целью данной области является обеспечение приватности и безопасности проводимых финансовых транзакций, путём внедрения в систему сложных криптографических протоколов, а именно алгоритмов доказательства с нулевым разглашением.

Одной из задач криптографии является двусторонняя интерактивная игра, в которой доказывающая сторона доказывает истинность некоторого утверждения другой стороне, проверяющей, не раскрывая сущности доказательства. Такая игра называется протоколом интерактивного доказательства или IP-протоколом (interactive proof – IP). Доказательство, получаемое при помощи такого IP-протокола, является секретным, потому что, во-первых, проверяющая сторона, убедившись в истинности доказанного утверждения, не способна самостоятельно повторить доказательство, и, во-вторых, после завершения протокола никто извне не способен понять сообщения, которыми обменивались стороны в процессе доказательства.

Такая конфиденциальность необходима во многих приложениях, в которых проводятся операции с использованием персональных данных, раскрытие которых может привести к фальсификации, подделыванию или краже личных данных. Например, при проведении голосований необходимо сохранять анонимность голосующих, чтобы предотвратить возможное принуждение или подтасовывание результатов, или при проведении электронных платежей, в процессе которых используются финансовые данные пользователей.

2 ОБЗОР НОТАЦИЙ ДЛЯ ПОСТРОЕНИЯ ДИАГРАММ

В данном разделе представлена теоретическая информация о следующих нотациях: DFD, IDEF0, IDEF1X, IDEF3, BPMN.

2.1 Нотация DFD (DataFlowDiagrams – Диаграмма Поточков Данных)

Основная цель DFD состоит в создании абстрактной, но наглядной модели системы, которая обеспечивает понимание основных процессов и потоков данных внутри неё. DFD широко применяется на этапе анализа системы для выявления ключевых компонентов и их взаимосвязей.

Диаграммы DFD состоят из следующих компонентов:

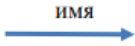
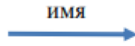



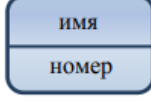
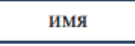
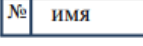
Компонента	Нотация Йордона-де Марко	Нотация Гейна-Сарсона
Поток данных		
Внешняя сущность		
Процесс		
Накопитель данных		

Рисунок 1 – Графическое представление элементов DFD-диаграмм

1. Потоки данных. Поток данных определяет качественный характер информации, передаваемой от источника к приемнику. Потоки данных на диаграммах DFD изображаются линиями со стрелкой на одном из ее концов или

на обоих концах. Стрелка показывает направление информационного потока в системе.

2. Внешние сущности. Внешняя сущность представляет собой материальный объект, например, заказчики, персонал, поставщики, клиенты, склад, изображают входы в систему и/или выходы из системы и указывают на место, организацию или человека, которые участвуют в процессе обмена информацией с системой, но располагаются за рамками диаграммы. Внешние сущности изображаются в виде прямоугольника с тенью и обычно располагаются по краям диаграммы.

3. Процессы (работы). В DFD работы обозначают функции или процессы системы, которые обрабатывают и изменяют информацию (преобразуют входы в выходы). Процессы изображаются прямоугольниками с закругленными углами, (смысл их совпадает со смыслом работ IDEF0 и IDEF3). Процессы в DFD-нотации имеют входы и выходы (не поддерживают управления и механизмы, как IDEF0). В каждую работу может входить и выходить по несколько стрелок.

4. Хранилища данных. Хранилища данных представляют собой данные, к которым осуществляется доступ. Эти данные могут быть созданы или изменены работами. Хранилища данных изображают информацию в покое, изображаются прямоугольными блоками с двумя полями. В левом поле указывается номер или идентификатор хранилища.

2.2 Нотация IDEF0 (Integration Definition for Function Modeling)

Основной целью IDEF0 является создание структурированного и иерархического представления функций в системе. Это позволяет детально описывать бизнес-процессы, выявлять их структуру, входы, выходы, и взаимосвязи между функциональными элементами.

Функциональный блок (ActivityBox, рисунок 2.1) – графически изображается в виде прямоугольника и олицетворяет собой некоторую конкретную функцию в рамках рассматриваемой системы.

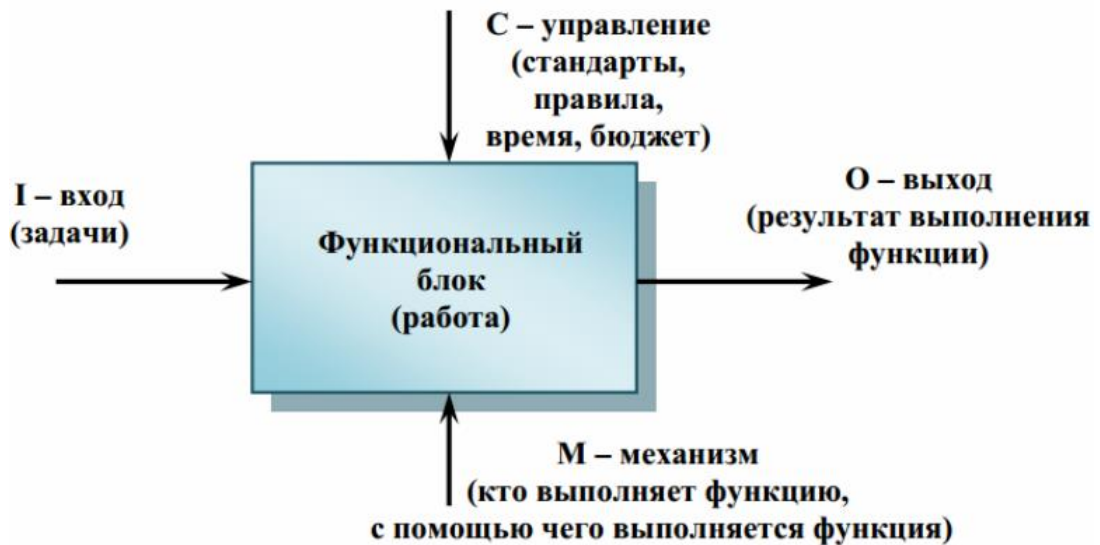


Рисунок 2 – Функциональный блок и интерфейсные дуги IDEF0-диаграммы

Каждая из четырех сторон функционального блока имеет своё определенное значение (роль), при этом:

- верхняя сторона – «Управление» (Control);
- левая сторона – «Вход» (Input);
- правая сторона – «Выход» (Output);
- нижняя сторона – «Механизм» (Mechanism).

Функциональный блок: представляют собой конкретные функции или деятельности, выполняемые в системе. Блоки функций могут быть декомпозированы на более низкий уровень для более детального анализа.

Стрелки потока данных: изображают потоки данных, которые передаются между различными функциональными блоками. Стрелки указывают направление передачи данных и содержат описание данных, которые передаются.

2.3 Нотация IDEF1X (Integration Definition for Information Modeling)

Основной целью IDEF1X является предоставление формальной и точной нотации для создания моделей данных. Это включает в себя определение

сущностей, их атрибутов, отношений между сущностями, а также ограничений и правил для баз данных.

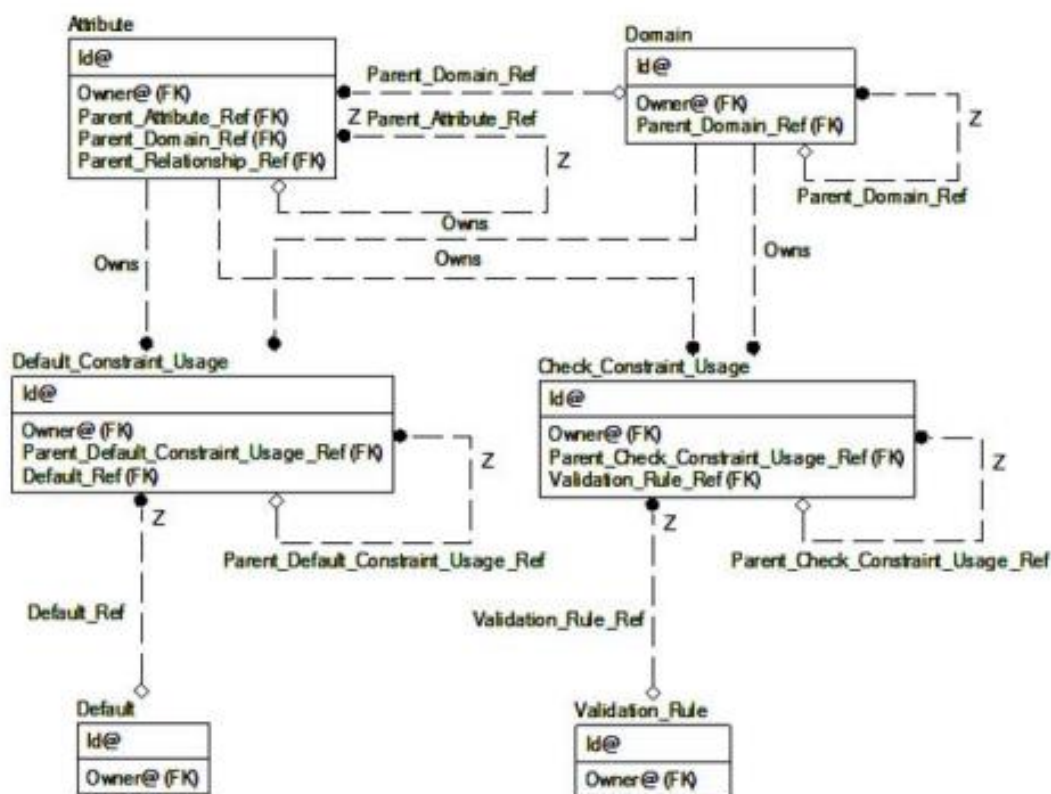


Рисунок 3 – Пример IDEF1X-диаграммы

Компоненты диаграммы:

Сущности (эллипсы): представляют собой объекты в системе, о которых хранится информация. Каждая сущность имеет атрибуты, описывающие её свойства.

Атрибуты (прямоугольники): представляют свойства сущностей и содержат информацию, которая хранится о каждой конкретной сущности. Атрибуты могут быть простыми или составными.

Отношения (линии между сущностями): изображают связи между сущностями и указывают на то, как данные между ними взаимодействуют. Отношения также могут иметь атрибуты, отражающие дополнительную информацию о связи.

Ключи (подчеркнутые атрибуты): подчеркнутые атрибуты обозначают ключевые атрибуты, которые уникальны для каждой записи, в сущности, и используются для идентификации.

2.4 Нотация IDEF3 (Integration DEfinition for Process Description Capture Method)

Основной целью IDEF3 является предоставление средства для описания и анализа процессов в организации. Методология помогает выявить, описать и документировать взаимосвязи между функциональными элементами в системе, а также последовательность выполнения операций.

Любая IDEF3-диаграмма может содержать: работы, связи, перекрестки (соединения), объекты ссылок.



Рисунок 4 – Изображение работы в IDEF3

Работа – изображается прямоугольником с прямыми углами и имеет имя, а также номер (идентификатор). Все стороны работы равнозначны. В каждую работу может входить и выходить ровно по одной стрелке.

Связи – предназначены для выделения существенных взаимоотношений между действиями. Все связи в IDEF3 являются однонаправленными, и, хотя стрелка может начинаться или заканчиваться на любой стороне блока, обозначающего действие, диаграммы IDEF3 обычно организовываются слева

направо таким образом, что стрелки начинаются на правой и заканчиваются на левой стороне блоков.

Перекрестки (соединения) – завершение одного действия может инициировать начало выполнения сразу нескольких других действий, или, наоборот, определенное действие может требовать завершения нескольких других действий для начала своего выполнения.

2.5 Нотация BPMN (Business Process Model and Notation)

Основной целью BPMN является предоставление общего языка для представления бизнес-процессов, который был бы понятен как бизнес-специалистам, так и ИТ-специалистам. Методология предоставляет средства для создания наглядных диаграмм, на которых можно отобразить основные элементы и взаимосвязи в процессах.



Рисунок 5 – Примерный вид BPMN диаграммы хореографии.

Нотация BPMN включает в себя такие графические объекты, как:

1. Действие – общий термин, обозначающий работу, выполняемую исполнителем. Действия могут быть либо элементарными, либо неэлементарными (составными). Выделяют следующие виды действий, являющихся частью модели Процесса: Процесс (Process), Подпроцесс (Sub-Process) и Задача (Task). Задача и Подпроцесс изображаются в виде прямоугольника с закругленными углами.

2. Событие – это то, что происходит в течение бизнес-процесса и оказывает влияние на его ход. Чаще всего событие имеет причину (триггер) или воздействие (результат). Изображается в виде круга со свободным центром, предназначенным для дифференцировки внутренними маркерами различных триггеров или их результатов.

3. Шлюзы используются для контроля расхождений и схождений потока операций. Таким образом, данный термин подразумевает ветвление, раздвоение, слияние и соединение маршрутов. Внутренние маркеры указывают тип контроля развития бизнес-процесса.

4. Потоки – описание действия, характеризующего обмен информацией между участниками (пулами) взаимодействия.

3 ПРИМЕНЕНИЕ МЕТОДОЛОГИЙ ПОСТРОЕНИЯ ДИАГРАММ ДЛЯ ПРОЕКТИРОВАНИЯ СИСТЕМЫ «СИСТЕМА ПЕРЕВОДА СРЕДСТВ МЕЖДУ ЭЛЕКТРОННЫМИ КОШЕЛЬКАМИ НА ОСНОВЕ АЛГОРИТМОВ ZKP» С ИСПОЛЬЗОВАНИЕМ CASE СРЕДСТВ

В данном разделе представлены построенные диаграммы различных нотаций для проектирования системы перевода средств между электронными кошельками на основе алгоритмов ZKP.

3.1 Диаграммы в нотации DFD

Был проведен анализ внешних событий (определены внешние сущности) исследуемой предметной области, оказывающих влияние на функционирование системы.

Выделены потоки данных, которыми обменивается процесс и внешние сущности.

На основе этого была построена DFD-диаграмма главного (основного) процесса (рисунок 6). Также была произведена декомпозиция и построена DFD-диаграмма декомпозированного основного процесса, которая изображена на рисунке 7.

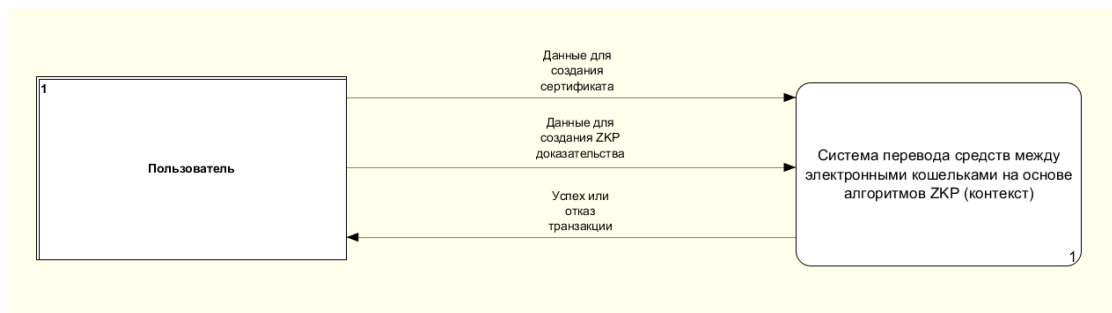


Рисунок 6 – DFD-диаграмма верхнего уровня

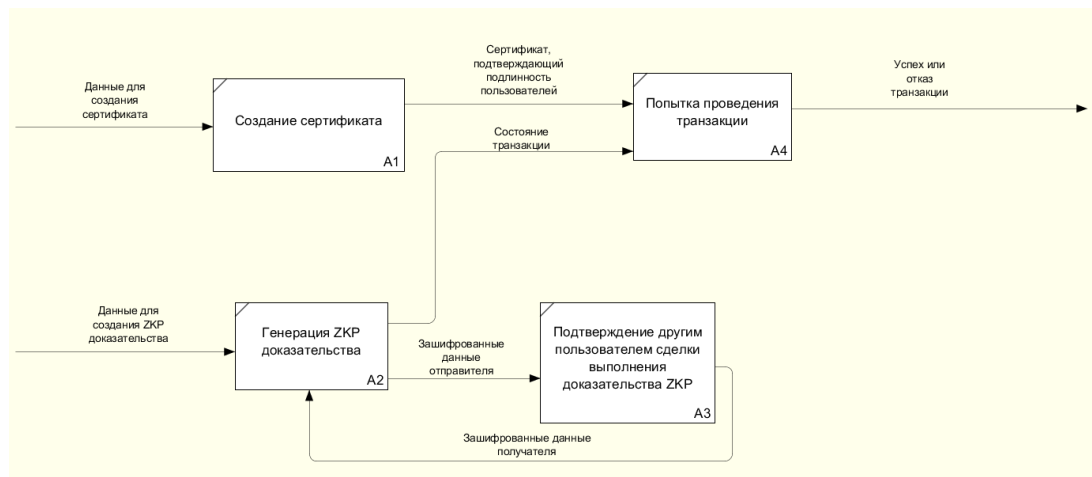


Рисунок 7 – DFD-диаграмма декомпозиции основного процесса

Таким образом, после декомпозиции стала доступна детальная информация о процессах и потоках данных в разрабатываемой системе перевода средств между электронными кошельками на основе алгоритмов ZKP.

3.2 Диаграмма в нотации IDEF0

Была построена IDEF0-диаграмма основного процесса, которая представлена на рисунке 8, затем была произведена её декомпозиция и получена IDEF0-диаграмма первого уровня, которая изображена на рисунке 9.

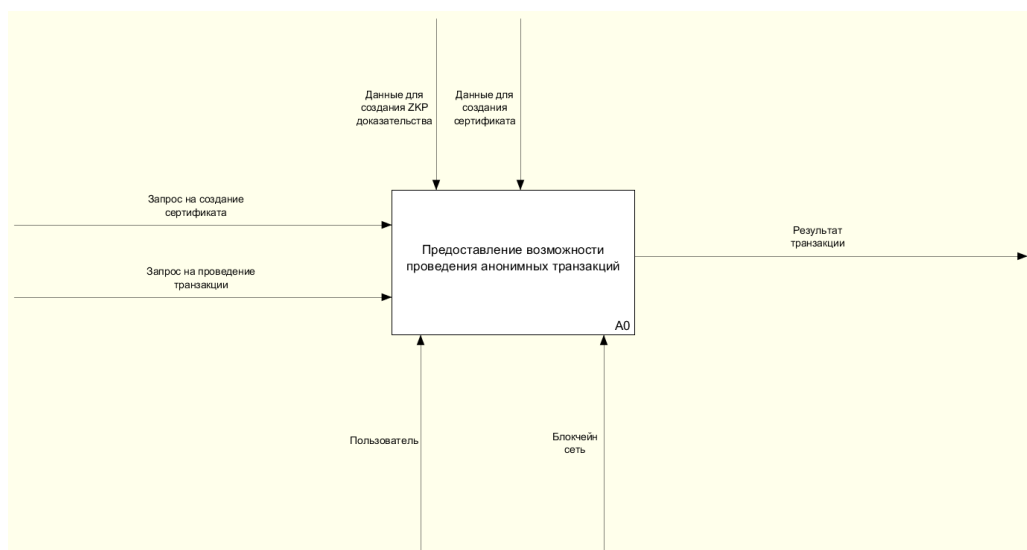


Рисунок 8 – IDEF0-диаграмма основного процесса

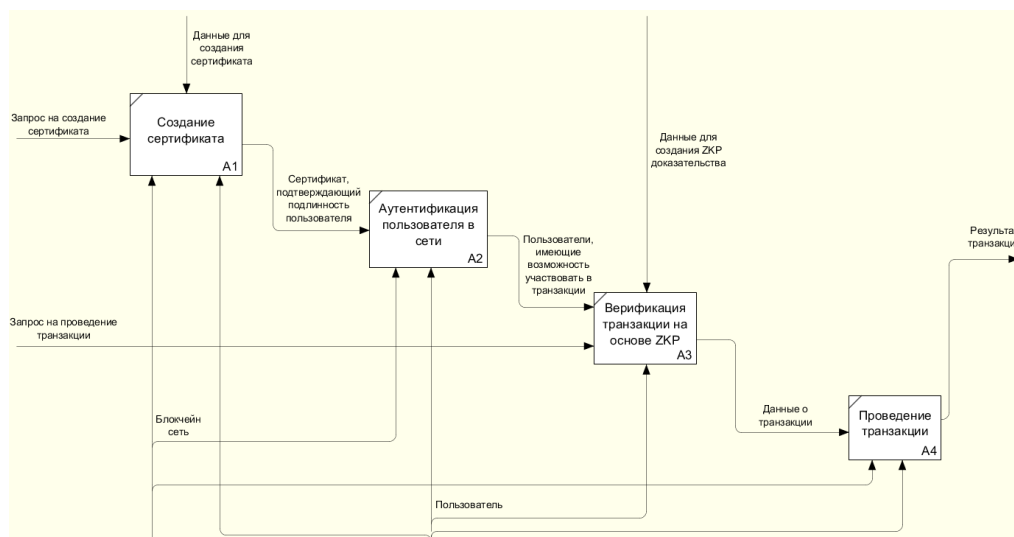


Рисунок 9 – IDEF0-диаграмма декомпозиции первого уровня

После чего была произведена декомпозиция процесса «Создание сертификата», результат продемонстрирован на рисунке 10.

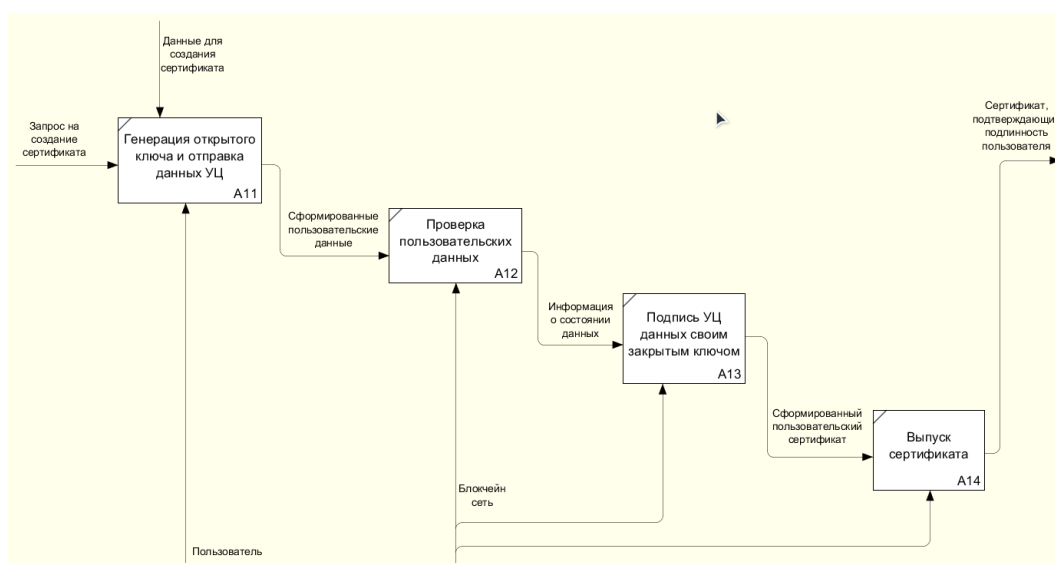


Рисунок 10 – IDEF0-диаграмма декомпозиции второго уровня

3.3 Диаграммы в нотации IDEF1X

Был определен список (пул) информационных объектов (словарь данных) для проектируемой системы и составлена таблица потенциальных сущностей.

Таблица 1 – Список потенциальных сущностей

№	Название сущности	Описание
1	Пользователь	Лицо, участвующее в создании цифрового сертификата, а также в проведении транзакций
2	Сертификат	Документ, отвечающий за подтверждение личности пользователя
3	Транзакция	Перевод средств между пользователями сети, без раскрытия информации о самой транзакции или о пользователях
4	Организация	Служит для объединения пользователей в группы, а также позволяет проводить конфиденциальные транзакции внутри ограниченного круга пользователей

Далее список сущностей был разделен на сущности и их атрибуты, результат представлен в таблице 2.

Таблица 2 – Список сущностей и их атрибутов

№	Название сущности	Атрибут
1	Пользователь	Id пользователя
		Имя пользователя
2	Сертификат	Id сертификата (RevocationHande)
		Атрибут организационного подразделения
		Атрибут роли
		EnrollmentId
3	Транзакция	Id транзакции
		Id сертификата отправителя
		Id сертификата получателя
4	Организация	Id организации
		Имя организации

После чего было составлено описание предметной области на естественном языке:

Каждый пользователь (сущность 1) может иметь один или более сертификатов (сущность 3)

Каждый пользователь (сущность 1) принадлежит одной или более организации (сущность 4)

Каждый пользователь (сущность 1) может проводить одну или более транзакцию (сущность 3)

Каждый сертификат (сущность 2) может принадлежать только одному пользователю (сущность 1)

Каждый сертификат (сущность 2) может быть использован при проведении одной или более транзакции (сущность 3)

Каждая транзакция (сущность 3) проверяется многими сертификатами (сущность 2)

Каждая организация (сущность 4) может содержать одного или многих пользователей (сущность 1)

Далее были определены имена отношений, типы связей между сущностями, заданы мощности связей между сущностями, результат представлен в таблице 3.

Таблица 3 – Матрица отношений между сущностями

	Пользователь	Сертификат	Транзакция	Организация
Пользователь		Имеет, (1:M)	Проводит, (1:M)	Принадлежит, (1:M)
Сертификат	Принадлежит, (1:1)		Используется, (1:M)	
Транзакция		Проверяется, (1:M)		
Организация	Состоит, (1:M)			

Были определены ключевые атрибуты для каждой сущности.

Таблица 4 – Список сущностей, атрибутов, ключевых атрибутов

№	Название сущности	Атрибут
1	Пользователь	<u>Id пользователя</u>
		Имя пользователя

2	Сертификат	<u>Id сертификата</u> (RevocationHande)
		Атрибут организационного подразделения
		Атрибут роли
		EnrollmentId
3	Транзакция	<u>Id транзакции</u>
		Id сертификата отправителя
		Id сертификата получателя
4	Организация	<u>Id организации</u>
		Имя организации

После чего была построена информационная модель уровня «сущность-связь» – ER-диаграмма в нотации П.Чена, которая изображена на рисунке 10.

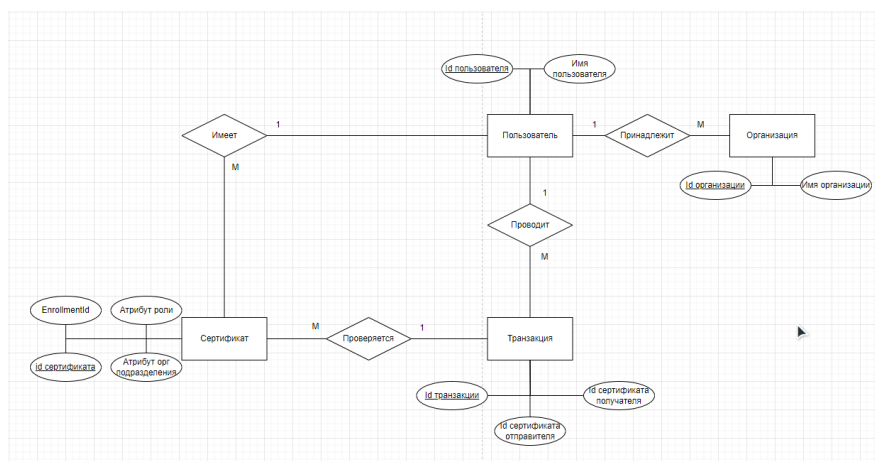


Рисунок 8 – ER-диаграмма в нотации П.Чена

Также были построены: модель данных, основанная на ключах, представленная на рисунке 11, а также полная атрибутивная модель в нотации IDEFIX1, которая изображена на рисунке 12.

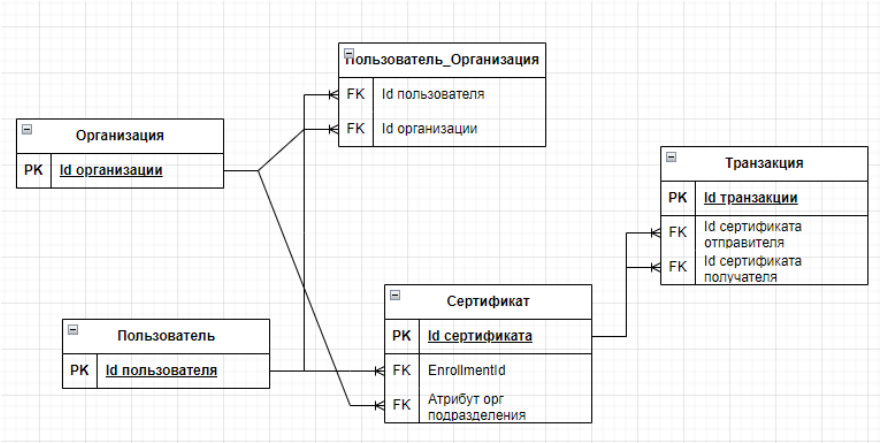


Рисунок 9 – IDEF1X-диаграмма

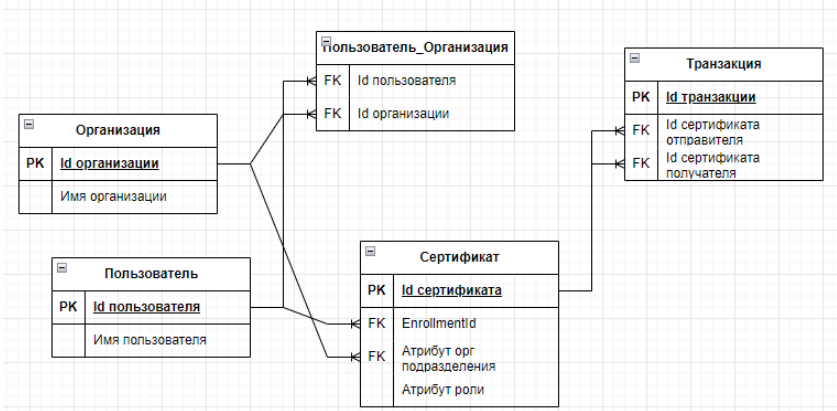


Рисунок 12 – Полная атрибутивная модель в нотации IDEF1X1

3.4 Диаграммы в нотации IDEF3

Исходя из исследуемой системы был составлен список действий и объектов, составляющих моделируемый процесс, который представлен в таблице 5.

Таблица 5 – Список действий и объектов, составляющих моделируемый процесс

№ действия	Название действия
1	Предоставление возможности проведения анонимных транзакций
2	Аутентификация пользователя в сети

3	Создание пользовательских атрибутов и ключей
4	Подтверждение атрибутов
5	Создание сертификатов
6	Создание доказательства с нулевым разглашением
7	Создание организации
8	Добавление пользователя в организацию
9	Проверка транзакции при помощи сертификатов и доказательства с нулевым разглашением
10	Проведение транзакции
11	Отзыв сертификатов
12	Назначение пользователя администратором организации

Для каждого действия были установлены предшествующие действия и определены типы связи между ними, результат продемонстрирован в таблице 6.

Таблица 6 – Список действий с указанием предшествующих и последующих событий с указанием типа связи

Номер/номера предшествующих действий	Тип связи	№ действия	Тип связи	Номер/номера последующих действий
-	-	Действие 1	-	-
Действие 3, 4	Объектный поток	Действие 2	Временное предшествование	Действие 5, 6
-	-	Действие 3	Объектный поток	Действие 4

Действие 3	Объектный поток	Действие 4	Объектный поток	Действие 2, 5
Действие 2	Временное предшествование	Действие 5	Объектный поток	Действие 6
Действие 2, 5	Временное предшествование	Действие 6	Объектный поток	Действие 9, 10
Действие 12	Временное предшествование	Действие 7, 8	-	-
Действие 5, 6	Объектный поток	Действие 9	Объектный поток	Действие 10
Действие 9	Объектный поток	Действие 10	-	-
Действие 5	Объектный поток	Действие 11	-	-
-	-	Действие 12	Временное предшествование	Действие 7, 8

Для каждого действия установлен список действий, который должны быть выполнены до начала рассматриваемого действия. Были установлены отношения между началом и окончанием связанных соединений действий.

Таблица 7 – Список действий с указанием предшествующих и последующих событий с указанием установленных отношений

Номер/номера предшествующих действий	Вид казуального отношения	№ действия	Вид казуального отношения	Номер/номера последующих действий
Действие 3, 4	&	Действие 2	О	Действие 5, 6
Действие 5, 6	&	Действие 9	&	Действие 10

На основании контекстной диаграммы (А-0), построенные с помощью методологии IDEF0, были декомпозированы функциональные блоки модели окружения на 1-2 уровня вглубь до потоков, установлены связи с внешними системами и хранилищами с помощью методологии IDEF3. На рисунках 13-15 представлены разработанные диаграммы в нотации IDEF3.

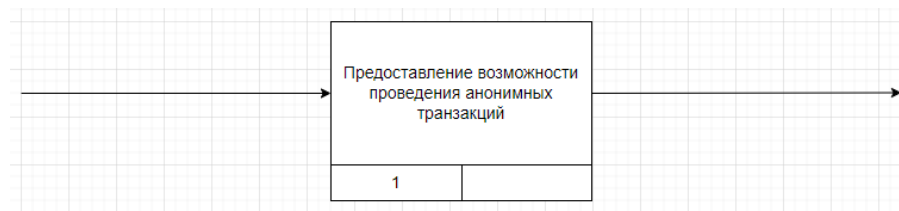


Рисунок 10 – Диаграмма IDEF3 первого уровня

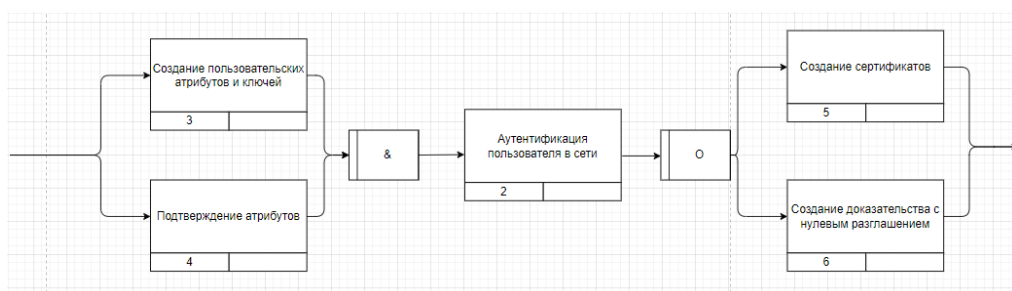


Рисунок 11 – Диаграмма IDEF3 декомпозиции первого уровня

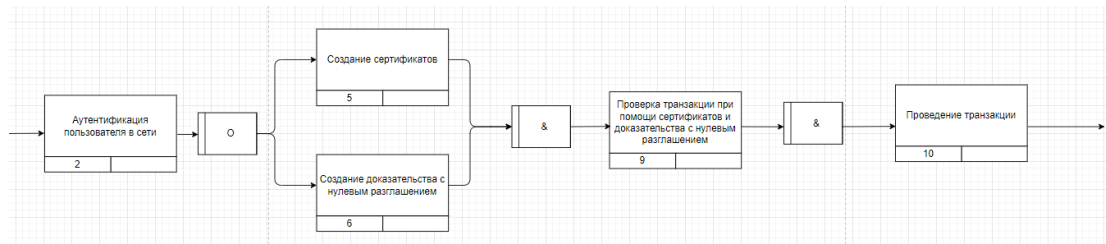


Рисунок 12 – Диаграмма IDEF3 декомпозиции действия 10

3.5 Диаграмма в нотации BPMN

Было произведено разделение задач между участниками процесса. Определены объекты данных и показатели эффективности необходимые или получающиеся в ходе выполнения задачи. Построена BPMN-диаграмма.

Таблица 8 – Список задач, действующих лиц, объектов данных и показателей эффективности

№ задач и	Название задачи	Список действий, составляющих решение задачи	Участник, составляющий решение задачи	Объекты данных
1	Аутентификация пользователя	Генерация пользовательских атрибутов и ключей и дальнейшая проверка их УЦ	Пользователь, блокчейн-сеть	Распределенный реестр пользователей
2	Создание организации	Ввод названия организации	Пользователь	Распределенный реестр организаций
3	Добавление пользователей в организацию	Отправка приглашения пользователю, а	Пользователь	Распределенный реестр

		также назначение ему роли		пользователей и организаций
4	Выпуск сертификатов	Получение пользовательски х данных, их шифрация УЦ	Пользователь, блокчейн-сеть	Распределенны й реестр сертификатов
5	Проведение транзакции	Подтверждение пользовательски х сертификатов, а также выполнения ZKP алгоритма	Пользователь, блокчейн-сеть	Распределенны й реестр транзакций

Далее были построены упрощенная модель бизнес-процесса, изображенная на рисунке 16, а также усложненная модель бизнес-процесса (BPMN-диаграмма), которая представлена на рисунке 17.

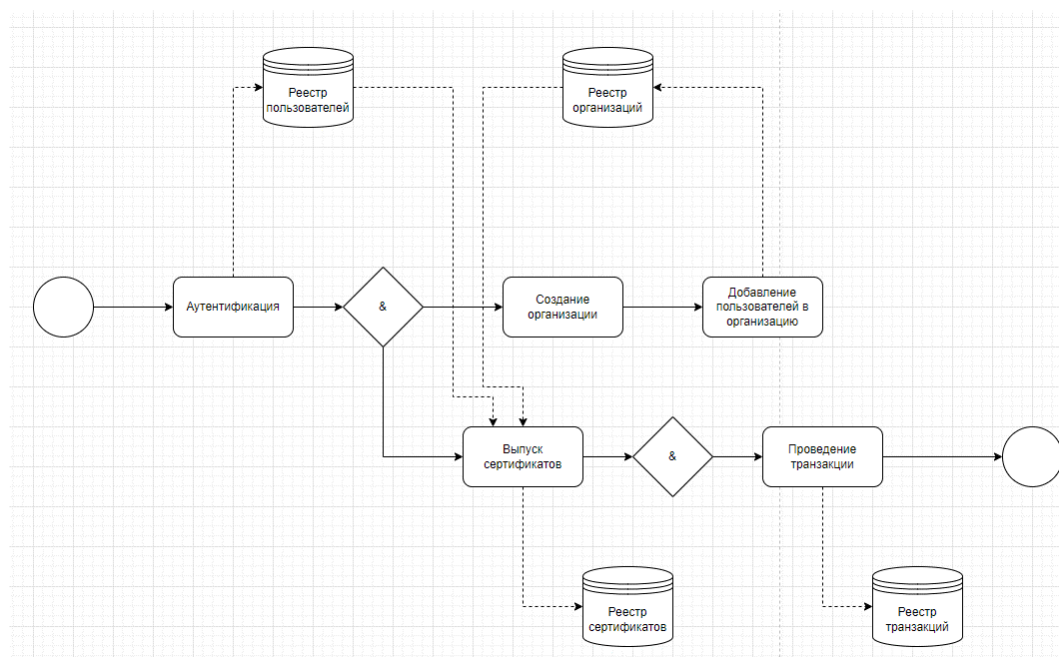


Рисунок 16 – Упрощенная модель бизнес-процесса

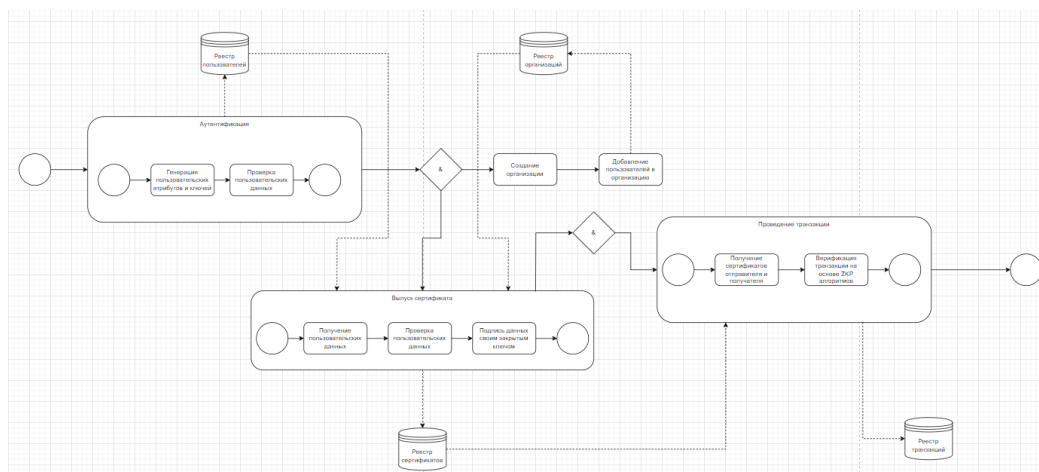


Рисунок 17 – Усложненная модель бизнес-процесса (BPMN-диаграмма)

ЗАКЛЮЧЕНИЕ

В ходе выполнения данной расчетно-графической работы было произведено проектирование системы перевода средств между электронными кошельками на основе алгоритмов ZKP.

В процессе выполнения расчетно-графической работы был выполнен ряд задач, а именно:

1. Произведен анализ предметной области системы перевода средств между электронными кошельками на основе алгоритмов ZKP, а также выделены основные сущности и функции такой системы.

2. Проведен обзор некоторых методологий построения диаграмм, приведено теоретическое описание исследованных нотаций.

3. Произведено построение диаграмм в нотациях DFD, IDEF0, IDEF1X, IDEF3, BPMN.

По итогам выполненной работы был сделан вывод о том, что диаграммы различных нотаций позволяют глубже понять предметную область и выделить ключевые компоненты системы, что в дальнейшем будет полезно для последующего анализа и разработки.