(19) Евразийское патентное ведомство

(21) 202491546 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2024.10.31

(22) Дата подачи заявки
2022.12.20

(51) Int. Cl. *G06Q 20/40* (2012.01)

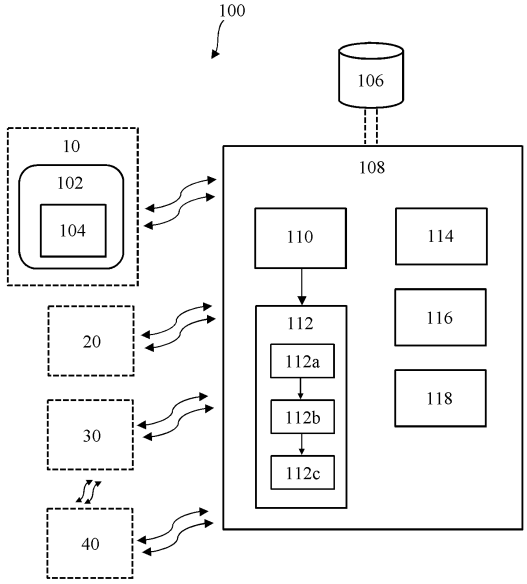
(54) СИСТЕМА БЕЗОПАСНОЙ ОБРАБОТКИ ТРАНЗАКЦИЙ И СПОСОБ ОСУЩЕСТВЛЕНИЯ ДАННОЙ ОБРАБОТКИ

(31) **202121060001**
(32) **2021.12.22**
(33) **IN**
(86) **PCT/IB2022/062520**
(87) **WO 2023/119144 2023.06.29**

(71)(72) Заявитель и изобретатель:
АГАШЕ МАНДАР (IN)

(74) Представитель:
Билык А.В., Поликарпов А.В., Соколова М.В., Путинцев А.И., Черкас Д.А., Игнатьев А.В., Дмитриев А.В., Бельтюкова М.В. (RU)

(57) В настоящем документе приведено описание системы (100) и способа (200) для безопасной обработки транзакций. Система (100) включает в себя платежное приложение (102), модуль памяти (106) и сервер транзакций (108), на котором размещено приложение (102). Приложение (102) позволяет зарегистрированному пользователю генерировать запрос на инициирование платежной операции. В модуле памяти (106) хранится список идентификаторов, связанных с зарегистрированными пользователями, и регистрационные данные, соответствующие каждому пользователю. Сервер транзакций (108) генерирует первый одноразовый проверочный код/PIN-код на основе запроса на транзакцию и отправляет его приложению (102). Сервер транзакций (108) получает второй проверочный код/PIN-код через второй пользовательский интерфейс (20), сравнивает эти два кода/PIN-кода и отправляет данные транзакции в банк-эмитент (30) первого пользователя через банк-эквайер (40) для завершения платежной операции, если коды/PIN-коды совпадают. Система (100) позволяет пользователям осуществлять платежные операции без ввода информации о своих конфиденциальных финансовых счетах.



202491546 A1

202491546 A1

СИСТЕМА БЕЗОПАСНОЙ ОБРАБОТКИ ТРАНЗАКЦИЙ И СПОСОБ ОСУЩЕСТВЛЕНИЯ ДАННОЙ ОБРАБОТКИ

СФЕРА, К КОТОРОЙ ОТНОСИТСЯ ОПИСЫВАЕМЫЙ СПОСОБ

Сведения, изложенные в настоящем документе, в основном относятся к платежным системам. В частности, данные сведения относятся к системе и способу безопасной обработки финансовых транзакций.

ОБЩИЕ ПОЛОЖЕНИЯ

Изложенные далее общие положения относятся к сведениям, приведенным в этом документе, но не обязательно относятся к уровню техники.

Как правило, платежные системы, применяемые в точках продаж (POS) или банкоматах (ATM), требуют для проведения денежных операций, чтобы пользователь использовал кредитные/дебетовые/предоплаченные карты. Подобным образом, интернет-платежные системы для осуществления онлайн денежных транзакций требуют от пользователей предоставления их финансовых данных, таких как информация о кредитных/дебетовых картах, учетных данные для интернет-банкинга или имя пользователя и пароль от финансового сервиса, например такого как PayPal. Интернет-платежные системы предоставляют доступ к финансовому счету пользователя и позволяют проводить транзакции без посещения банка и оформления транзакций с помощью бумажных документов.

Тем не менее, при проведении платежной транзакции в точке продаж (POS), банкомате (ATM) или в интернете пользователю необходимо либо вставить платежную карту в POS-терминал продавца или банкомат, либо в интерфейсе приложения или на веб-сайте продавца ввести свои финансовые данные вручную. Помимо этого, на данных веб-сайтах/интерфейсах может сохраняться часть финансовых данных, таких как номера карт, непосредственно или в виде токена. Для хранения данных карты в виде токена с помощью сервиса хранения карт в файле, клиенту хотя бы один раз необходимо ввести на веб-сайте полные данные карты, что технически создает возможность кражи этих данных с веб-сайта. Каждый раз пользователю для проведения транзакции необходимо вводить другие данные, такие как код проверки карты (CVV). Это означает, что финансовые данные пользователя становятся доступными для продавцов или сторонних поставщиков услуг, в связи с чем

повышается вероятность мошеннических действий во время проведения транзакций. Помимо этого, через публичные сети Интернет обычно передается конфиденциальная информация, такая как банковские реквизиты, данные счета, номер дебетовой карты, номер предоплаченной карты, номер кредитной карты, сведения о сроке действия карты, проверочное значение карты (CVV), идентификатор входа в систему интернет-банкинга, учетные данные, связанные со счетом финансовых услуг, идентификатор виртуального платежного адреса (VPA)/интерфейса унифицированных платежей (UPI), идентификатор PayPal, идентификатор Zelle и другие идентификаторы транзакций. Подобная передача данных часто подвержена различным видам хакерских атак, в результате которых конфиденциальность финансовой информации может быть нарушена.

Таким образом возникла потребность в системе и способе безопасной обработки транзакций, которые устраняют вышеупомянутые недостатки.

ЦЕЛИ

Ниже перечислены некоторые цели изложенного материала, которые соответствуют по меньшей мере одному из условий:

Задачей данного изложенного материала является устранение одной или нескольких проблем предшествующего уровня техники или, по меньшей мере, обеспечение полезной альтернативы.

Объектом данного материала является система для безопасной обработки транзакций и способ осуществления такой обработки.

Другим объектом данного материала является создание системы для безопасной обработки транзакций, которая для осуществления платежных операций не требует от пользователя ввода финансовых учетных данных (например, таких как номер, номер кредитной карты, данные о действии карты, проверочное значение карты (CVV), идентификатор входа в интернет-банк, учетные данные, связанные со счетом финансового сервиса, идентификатор виртуального платежного адреса (VPA)/интерфейса унифицированных платежей (UPI), идентификатор PayPal, идентификатор Zelle и другие идентификаторы транзакций).

Еще одним объектом данного материала является система для безопасной обработки транзакций и способ ее осуществления. Система для безопасной обработки транзакций и

способ ее осуществления предлагают пользователю безопасный и удобный способ проведения транзакций.

Следующим объектом данного материала является система для безопасной обработки транзакций и способ ее осуществления, которые снижают вероятность подверженности хакерским атакам.

Также, объектом данного материала является система для обработки транзакций и способ ее осуществления, которые позволяют пользователям выполнять транзакции в точке продажи (POS) или в банкомате без использования финансовой карты.

Другие объекты и преимущества данного материала станут более очевидными из нижеследующего описания при прочтении в сочетании с сопроводительными диаграммами, предназначением которых не является ограничение объема настоящего материала.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

В настоящем документе раскрыта система, предназначенная для обеспечения безопасной обработки транзакций. Система включает в себя платежное приложение, модуль памяти и сервер транзакций, на котором размещено платежное приложение. Приложение сконфигурировано таким образом, чтобы при запуске на электронном устройстве предоставлять первый пользовательский интерфейс для обеспечения возможности регистрации пользователей и добавления финансовых счетов при осуществлении безопасных платежных операций. Помимо этого, платежное приложение сконфигурировано таким образом, чтобы с помощью платформы токенизации обеспечить возможность зарегистрированному пользователю произвести токенизацию финансовых счетов. Модуль памяти сконфигурирован для хранения базы данных, содержащей первую таблицу поиска. Первая таблицу поиска содержит список идентификаторов зарегистрированных пользователей и регистрационные данные для каждого из них, при этом регистрационные данные содержат личную информацию и финансовые счета зарегистрированных пользователей, а также токены этих счетов.

Личные сведения выбираются из группы данных, состоящей из имени, номера мобильного телефона, идентификатора электронной почты и информации, связанной соответствующим человеком. Финансовые счета выбираются из группы данных, включающих в себя банковские реквизиты, данные счета, номер дебетовой карты, номер предоплаченной карты, номер

кредитной карты, сведения о сроке действия карты, проверочное значение карты (CVV), идентификатор входа в систему интернет-банкинга, учетные данные, связанные со счетом финансовых услуг, идентификатор виртуального платежного адреса (VPA)/интерфейса унифицированных платежей (UPI), Идентификатор PayPal, идентификатор Zelle и другие идентификаторы транзакций или токены финансовых счетов.

Модуль генерации кода проверки сконфигурирован для генерации на основе каждого полученного запроса на транзакцию первого одноразового кода проверки/PIN-кода для финансовых счетов или маркера финансовых счетов. Первый одноразовый проверочный код/PIN-код может быть цифровым или буквенно-цифровым кодом. Модуль генерации проверочного кода сконфигурирован таким образом, что оба проверочных кода сохраняются во второй таблице поиска. Модуль генерации проверочного кода сконфигурирован для отправки первого одноразового проверочного кода/PIN-кода в платежное приложение с целью его отображения на первом пользовательском интерфейсе.

Модуль контроля проверочного кода включает в себя компаратор, модуль извлечения и модуль авторизации. Компаратор сконфигурирован для приема второго проверочного кода/PIN-кода, введенного через второй пользовательский интерфейс, и сравнения первого одноразового проверочного кода/PIN-кода со вторым проверочным кодом/PIN-кодом из второй таблицы поиска. Модуль извлечения сконфигурирован для извлечения сохраненных финансовых счетов или токенов финансовых счетов, ассоциирующихся с первым одноразовым проверочным кодом/PIN-кодом. Модуль извлечения сконфигурирован для последующей отправки данных финансового счета или данных токена в банк-эквайер или платежный шлюз для утверждения. Далее банк-эквайер или платежный шлюз отправляет сведения о транзакции в платежное приложение зарегистрированного пользователя.

Модуль авторизации сконфигурирован для отправки запроса на проведение транзакции и сведений о транзакции в платежное приложение зарегистрированного пользователя для получения подтверждения на проведение транзакции, которое осуществляется проведением пальцем влево или вправо, либо с использованием биометрических данных или PIN-кода приложения. Модуль авторизации сконфигурирован для последующей отправки статуса проверки транзакции платежному шлюзу или банку-эквайеру, и далее платежный шлюз или банк-эквайер отправляет транзакцию в банк-эмитент для одобрения или банк-эквайер или платежный шлюз отправляет сведения о транзакции в банк-эмитент, где банк-эмитент для одобрения транзакции отправляет запрос на ввод одноразового

пароля (OTP) для транзакции зарегистрированному пользователю банка. Зарегистрированный пользователь одобряет транзакцию, вводя одноразовый пароль (OTP) на платежном шлюзе, а платежный шлюз или банк-эквайер отправляет в модуль авторизации статус транзакции.

Модуль уведомления сконфигурирован для взаимодействия с модулем авторизации с целью получения статуса одобренной транзакции в платежном приложении зарегистрированного пользователя. Данные о транзакции содержат идентификатор зарегистрированного пользователя, по меньшей мере один из идентификаторов транзакции, финансовый счет зарегистрированного пользователя, сумму транзакции, данные онлайн/оффлайн продавца или банкомата, либо несколько регистрационных данных второго зарегистрированного пользователя, с которым осуществляется платежная операция.

Кроме того, банк-эмитент проверяет полученные от модуля экстрактора данные о транзакциях и выполняет аутентификацию пользователя второго уровня, генерируя и отправляя на электронное устройство зарегистрированного в банке пользователя одноразовый пароль. Зарегистрированный пользователь может ввести полученный пароль на электронном устройстве в платежном шлюзе, например, по SMS или электронной почте, через первый пользовательский интерфейс или второй пользовательский интерфейс. После этого банк-эмитент может проверить, совпадает ли полученный от зарегистрированного пользователя банка пароль со сгенерированным паролем, и аутентифицировать пользователя.

В одном из вариантов реализации модуль памяти представляет собой область хранения на сервере транзакций. В качестве альтернативы, модуль памяти может быть реализован как независимое устройство хранения данных, коммуникативно связанное с сервером транзакций.

В одном из вариантов реализации сервер транзакций включает в себя модуль регистрации, сконфигурированный для получения регистрационных данных от пользователей через первый пользовательский интерфейс с последующей регистрацией пользователей путем создания связанных с ними уникальных идентификаторов и хранением регистрационных данных с уникальными идентификаторами пользователей в первой таблице поиска. Модуль регистрации настроен на хранение зашифрованных с помощью механизма шифрования регистрационных данных.

Сервер транзакций также включает модуль входа в систему, который сконфигурирован для обеспечения возможности пользователю генерации и задания учетных данных для входа в систему через первый пользовательский интерфейс, и далее сконфигурирован для выполнения аутентификации зарегистрированного пользователя на основе учетных данных для входа в систему, после чего зарегистрированный пользователь получает разрешение использовать платежное приложение для инициирования платежной операции. Учетные данные могут быть выбраны из группы, состоящей из идентификатора и пароля, предварительно установленного PIN-кода и биометрической подписи зарегистрированного пользователя, включая по меньшей мере один из следующих способов: отпечатки пальцев, биометрические данные лица, рисунок радужной оболочки глаза, рисунок сетчатки глаза, рисунок вен пальцев, рисунок вен ладони или образец голоса.

В одном из вариантов реализации, данные о транзакции содержат идентификатор зарегистрированного пользователя, по меньшей мере один из идентификаторов транзакции, финансовый счет зарегистрированного пользователя, сумму транзакции, данные онлайн/оффлайн продавца или банкомата, либо несколько регистрационных данных второго зарегистрированного пользователя, с которым осуществляется платежная операция.

Модуль уведомления сконфигурирован для получения сообщения о статусе транзакции от платежного шлюза или банка-эквайера второго зарегистрированного пользователя и далее сконфигурирован для уведомления зарегистрированного пользователя и второго зарегистрированного пользователя о статусе транзакции соответственно через первый пользовательский интерфейс и второй пользовательский интерфейс.

В одном из вариантов реализации система позволяет пользователю безопасно выполнять транзакции в режиме онлайн, в интернет-магазине, в торговых точках, в одноранговых сетях (P2P) и банкоматах.

Настоящее изобретение также предусматривает способ безопасной обработки транзакций.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

Система для безопасной обработки транзакций и способ ее осуществления, изложенные в настоящем материале, далее будут описаны с помощью сопровождающих чертежей, на которых:

на **Фиг. 1** показана блок-схема системы для обеспечения безопасной обработки транзакций в соответствии с изложенным материалом;

Фиг. 2A и **2B** иллюстрируют блок-схему способа для обеспечения возможности безопасной обработки транзакций в соответствии с изложенным материалом;

на **Фиг. 3A** показана блок-схема системы, изображенной на **Фиг. 1**, которая предназначена для безопасной обработки транзакций между клиентом и продавцом в соответствии с изложенным материалом;

на **Фиг. 3B** показана блок-схема системы, изображенной на **Фиг. 1**, для обеспечения безопасной обработки транзакций между людьми (P2P) в соответствии с изложенным материалом;

Фиг. 4A-4J иллюстрируют примерный поток клиентов на веб-сайте продавца в соответствии с одним из вариантов реализации изложенного материала;

Фиг. 5A-5G иллюстрируют примерный поток клиентов через кассовый аппарат продавца в соответствии с одним из вариантов реализации изложенного материала;

Фиг. 6A-6J иллюстрируют примерный поток клиентов в одноранговой сети, в соответствии с одним из вариантов реализации изложенного материала; и

Фиг. 7A-7H иллюстрируют пример потока клиентов на веб-сайте продавца в соответствии с одним из вариантов реализации изложенного материала.

СПИСОК УСЛОВНЫХ ОБОЗНАЧЕНИЙ

100 - Система
10/50 - Электронное устройство
10a - Электронное устройство первого пользователя
10b - Электронное устройство второго пользователя
20 - Второй пользовательский интерфейс
30 - Банк-эмитент
40 - Банк-эквайер
60 - Веб-сайт интернет-магазина
70 - Сервер продавца
102 - Приложение

104 - Первый пользовательский интерфейс

104a - Интерфейс приложения первого пользователя

104b - Интерфейс приложения второго пользователя

106 - Модуль памяти

108 - Сервер транзакций

110 - Модуль генерации проверочного кода

112 - Модуль контроля проверочного кода

112a - Компаратор

112b - Модуль экстрактора

112c - Модуль авторизации

114 - Модуль регистрации

116 - Модуль входа в систему

118 - Модуль уведомлений

ПОДРОБНОЕ ОПИСАНИЕ

Варианты реализации данного изобретения будут описаны со ссылкой на сопроводительные чертежи.

Варианты реализации изобретения представлены таким образом, чтобы всесторонне и в полной мере раскрыть содержание этого изобретения специалистам в данной области. Многочисленные подробные сведения, относящиеся к конкретным компонентам и способам, изложены для обеспечения полного понимания вариантов реализации данного изобретения. Специалистам в данной области будет очевидно, что детали, представленные в вариантах реализации изобретения, не должны быть истолкованы как ограничивающие спектр применения данного изобретения. В некоторых вариантах реализации не приводится подробное описание известных процессов, известных конструкций устройств и известных методик.

Терминология, используемая в данном описании изобретения, служит только для объяснения конкретного варианта реализации, и такая терминология не должна рассматриваться как ограничивающая сферу применения данного изобретения. При изложении описания настоящего изобретения, термины упомянутые в единственном числе могут включать также формы множественного числа, если контекст явно не предполагает иного. Термины «включающий» и «имеющий» являются переходными фразами с открытым концом и поэтому указывают на наличие указанных признаков, целых чисел,

этапов, операций, элементов или компонентов, но не запрещают наличие или добавление одного или нескольких других признаков, целых чисел, этапов, операций, элементов, компонентов или их групп. Конкретная последовательность этапов, раскрытых в способе и процессе данного изобретения, не должна быть истолкована как обязательно требующая их выполнения в строгом соответствии с описанием или иллюстрациями. Следует также понимать, что можно использовать дополнительные или альтернативные этапы.

Используемый в настоящем документе, термин «и/или» включает любые комбинации одного или нескольких соответствующих перечисленных элементов.

Как правило, платежные системы, применяемые в точках продаж (POS) или банкоматах (ATM), требуют для проведения денежных операций, чтобы пользователь использовал кредитные/дебетовые/предоплаченные карты. Подобным образом, платежные системы в интернете или интернет-магазинах для проведения денежных транзакций требуют от пользователей предоставления их финансовых данных (таких как банковские реквизиты, данные счета, номер дебетовой карты, номер предоплаченной карты, номер кредитной карты, сведения о сроке действия карты, проверочное значение карты (CVV), идентификатор входа в систему интернет-банкинга, учетные данные, связанные со счетом финансовых услуг, идентификатор виртуального платежного адреса (VPA)/интерфейса унифицированных платежей (UPI), Идентификатор PayPal, идентификатор Zelle и другие идентификаторы транзакций). Интернет-транзакции предоставляют доступ к финансовому счету пользователя и позволяют проводить транзакции без посещения банка и оформления транзакций с помощью бумажных документов.

Тем не менее, при проведении платежной транзакции в точке продаж (POS), банкомате (ATM) или в интернет-магазине, пользователю необходимо либо вставить платежную карту в устройство, либо в интерфейсе приложения или на веб-сайте продавца ввести данные о финансовых счетах вручную. Подобным образом, пользователь, совершающий одноранговую онлайн-транзакцию с помощью сервиса, должен ввести в интерфейсе приложения сервиса идентификатор входа в систему и информацию о счетах отправителя и получателя. Кроме того, пользователь должен вводить финансовую информацию на всех веб-сайтах или во всех интерфейсах, где он или она желает провести транзакцию. Помимо этого, на данных веб-сайтах/интерфейсах может сохраняться часть финансовых данных, таких как номера карт, непосредственно или в виде токена. Для хранения данных карты в виде токена с помощью сервиса хранения карт в файле, клиенту хотя бы один раз

необходимо ввести на веб-сайте полные данные карты, что технически создает возможность кражи этих данных. Это означает, что финансовые данные пользователя становятся доступными для продавцов и сторонних поставщиков услуг, в связи с чем повышается вероятность мошеннических действий во время проведения транзакций. Помимо этого, основным недостатком интернет-транзакций является то, что через публичные сети Интернет передается конфиденциальная информация, такая как банковские реквизиты, данные счета, номер дебетовой карты, номер предоплаченной карты, номер кредитной карты, сведения о сроке действия карты, проверочное значение карты (CVV), идентификатор входа в систему интернет-банкинга, учетные данные, связанные со счетом финансовых услуг, идентификатор виртуального платежного адреса (VPA)/интерфейса унифицированных платежей (UPI), Идентификатор PayPal, идентификатор Zelle и другие идентификаторы транзакций. Подобная передача данных часто подвержена различным видам хакерских атак и возможности ненадлежащего использования, в результате которых конфиденциальность финансовой информации может быть нарушена.

Для решения вышеупомянутых проблем в данном изобретении предлагается система (далее "система 100") для обеспечения возможности безопасной обработки транзакций и способ ее осуществления (далее "способ 200"). Далее система 100 и способ 200 описываются со ссылкой на диаграммы **Фиг. 1 - Фиг. 4J**.

В соответствии с **Фиг. 1**, система 100 включает в себя платежное приложение 102 (также именуемое «HydePay$^{(TM)}$ App»), модуль памяти 106 и сервер транзакций 108 (также именуемый «HydePay$^{(TM)}$ Server»), на котором размещено платежное приложение 102. Платежное приложение 102 может быть как мобильным приложением, так и веб-приложением. Платежное приложение 102 выполняется в электронном устройстве 10, таком как мобильный телефон, планшет, компьютер, ноутбук и любое другое электронное устройство, способное обрабатывать данные для доступа к финансовым продуктам, услугам или информации, хранящейся на сервере 108 и в модуле памяти 106. После запуска платежное приложение 102 настроено таким образом, что оно отображает первый пользовательский интерфейс 104, с целью обеспечения возможности пользователям регистрации и добавления финансовых счетов на сервере транзакций 108 для проведения безопасных платежных операций. Платежное приложение 102 сконфигурировано таким

образом, чтобы с помощью платформы токенизации обеспечить возможность зарегистрированному пользователю токенизацию финансовых счетов.

В одном из вариантов реализации для обеспечения возможности регистрации пользователя платежное приложение 102 сконфигурировано таким образом, чтобы через первый пользовательский интерфейс 104 предложить пользователю ввести регистрационные данные. Регистрационные данные включают в себя персональные данные и финансовые счета пользователей. Личные данные могут быть выбраны из группы, состоящей, в частности, из имени, номера мобильного телефона, идентификатора электронной почты и информации, связанной с личностью, такой как фотография, номер постоянного счета и дата рождения. Финансовые счета могут быть выбраны из таких данных, как банковские реквизиты, данные счета, номер дебетовой карты, номер предоплаченной карты, номер кредитной карты, сведения о сроке действия карты, проверочное значение карты (CVV), идентификатор входа в систему интернет-банкинга, учетные данные, связанные со счетом финансовых услуг, идентификатор виртуального платежного адреса (VPA)/интерфейса унифицированных платежей (UPI), Идентификатор PayPal, идентификатор Zelle и другие идентификаторы транзакций или токены финансовых счетов. Платежное приложение 102 сконфигурировано для отправки полученных данных на сервер транзакций 108 после получения регистрационных данных.

Модуль памяти 106 настроен для хранения базы данных и включает в себя первую таблицу поиска, содержащую список идентификаторов зарегистрированных пользователей и регистрационные данные для каждого из них, при этом регистрационные данные содержат личную информацию, финансовые счета зарегистрированных пользователей, а также токены этих счетов.

В одном из вариантов реализации модуль памяти 106 представляет собой область хранения на сервере транзакций 108. В качестве альтернативы, модуль памяти 106 может быть реализован как независимое устройство хранения данных, коммуникативно связанное с сервером транзакций 108.

Сервер транзакций 108, на котором размещено платежное приложение 102.

Сервер транзакций 108 включает в себя модуль генерации проверочного кода 110, модуль контроля проверочного кода 112 и модуль уведомлений 118.

Модуль генерации проверочного кода 110 сконфигурирован для генерации первого одноразового проверочного кода/PIN-кода для финансовых счетов или токена финансовых счетов на основе каждого полученного запроса на транзакцию и сохранения обоих во второй таблице поиска , модуль генерации проверочного кода 110 сконфигурирован для последующей отправки первого одноразового проверочного кода/PIN-кода в платежное приложение 102 для отображения его через первый пользовательский интерфейс 104.

Модуль контроля проверочного кода 112 включает в себя компаратор 112a, модуль извлечения 112b и модуль авторизации 112c.

Компаратор 112a сконфигурирован для приема второго проверочного кода/PIN-кода, введенного через второй пользовательский интерфейс, и сравнения первого одноразового проверочного кода/PIN-кода со вторым проверочным кодом/PIN-кодом из второй таблицы поиска. Второй пользовательский интерфейс 20 может быть веб-сайтом продавца или пользовательским интерфейсом платежного приложения 102, которое запущено на электронном устройстве другого пользователя (например, второго зарегистрированного пользователя/получателя транзакции).

Модуль извлечения 112b сконфигурирован для извлечения данных финансовых счетов или токенов , хранящихся в соответствии с первым одноразовым проверочным кодом/PIN-кодом, и для отправки данных финансовых счетов или токенов в банк-эквайер 40 или на платежный шлюз для утверждения, после чего банк-эквайер 40 или платежный шлюз отправляет детали транзакции в платежное приложение 102 зарегистрированного пользователя.

Модуль авторизации 112c сконфигурирован для взаимодействия с модулем извлечения 112b для отправки запроса транзакции, содержащего детали транзакции, в платежное приложение 102 зарегистрированного пользователя для проверки транзакции путем проведения пальцем влево или вправо или с помощью биометрического или цифрового PIN-кода, и далее сконфигурирован для отправки статуса проверки транзакции в платежный шлюз или банк-эквайер 40, после чего платежный шлюз или банк-эквайер 40 отправляет транзакцию в банк-эмитент 30 для одобрения. Банк-эквайер 40 или платежный шлюз направляют детали транзакции в банк-эмитент 30, где банк-эмитент 30 отправляет зарегистрированному пользователю банка одноразовый пароль (OTP) для запроса на проведение транзакции с целью осуществления авторизации транзакции, а

зарегистрированный пользователь подтверждает транзакцию путем ввода одноразового пароля (OTP) на платежном шлюзе, после чего платежный шлюз или банк-эквайер передают статус транзакции в модуль авторизации 112c.

Модуль уведомления 118 сконфигурирован для взаимодействия с модулем авторизации 112c с целью получения статуса одобренной транзакции в платежном приложении 112 зарегистрированного пользователя.

В одном из вариантов реализации личные сведения выбираются из группы данных, состоящей из имени, номера мобильного телефона, идентификатора электронной почты и информации, связанной соответствующим человеком.

В одном из вариантов реализации, финансовые счета выбираются из группы данных, включающих в себя банковские реквизиты, данные счета, номер дебетовой карты, номер предоплаченной карты, номер кредитной карты, сведения о сроке действия карты, проверочное значение карты (CVV), идентификатор входа в систему интернет-банкинга, учетные данные, связанные со счетом финансовых услуг, идентификатор виртуального платежного адреса (VPA)/интерфейса унифицированных платежей (UPI), Идентификатор PayPal, идентификатор Zelle и другие идентификаторы транзакций или токены финансовых счетов.

В одном из вариантов реализации сервер транзакций 108 позволяет пользователю зарегистрироваться на сервере 108 в качестве клиента или продавца. В одном из вариантов реализации сервер транзакций 108 настроен на хранение регистрационных данных клиента и регистрационных данных продавца в разных устройствах памяти. В другом варианте сервер транзакций 108 сконфигурирован таким образом, что регистрационные данные клиента и регистрационные данные продавца хранятся в одном и том же запоминающем устройстве. Идентификатор, сгенерированный для каждой регистрационной информации, является уникальным. В одном из вариантов реализации идентификатор указывает на то, (i) является ли зарегистрированный пользователь клиентом или продавцом или обоими, и (ii) на идентичность клиента или продавца, которым соответствуют регистрационные данные.

В одном из вариантов реализации сервер транзакций 118 включает в себя модуль регистрации 114, сконфигурированный для получения регистрационных данных от пользователей через первый пользовательский интерфейс 104 с последующей регистрацией пользователей путем создания связанных с ними уникальных идентификаторов и

хранением регистрационных данных с уникальными идентификаторами пользователей в первой таблице поиска.

В одном из вариантов реализации, модуль регистрации 114 настроен на хранение зашифрованных с помощью механизма шифрования регистрационных данных. Сервер транзакций 108 включает в свой состав модуль входа в систему 116, который сконфигурирован для обеспечения возможности пользователю генерации и задания учетных данных для входа в систему через первый пользовательский интерфейс 104, и далее сконфигурирован для выполнения аутентификации зарегистрированного пользователя на основе учетных данных для входа в систему, после чего зарегистрированный пользователь получает разрешение использовать приложение 102 для инициирования платежной операции.

В одном из вариантов реализации, учетные данные могут быть выбраны из группы, состоящей из идентификатора и пароля, предварительно установленного PIN-кода и биометрической подписи зарегистрированного пользователя, включая по меньшей мере один из следующих способов: отпечатки пальцев, биометрические данные лица, рисунок радужной оболочки глаза, рисунок сетчатки глаза, рисунок вен пальцев, рисунок вен ладони или образец голоса. Например, в одном из вариантов реализации сервер транзакций 108 может обеспечить возможность зарегистрированному пользователю создание или настройку идентификатора входа и пароля и использование идентификатора входа и пароля в качестве учетной записи для безопасного входа в платежное приложение 102. В другом варианте реализации сервер транзакций 108 может выполнять аутентификацию (т.е. способствовать безопасному входу в систему) путем проверки/контроля предварительно установленного безопасного PIN-кода, введенного зарегистрированным пользователем, или путем идентификации биометрического признака/функции зарегистрированного пользователя.

В одном из вариантов реализации, данные о транзакции содержат идентификатор зарегистрированного пользователя, по меньшей мере один из идентификаторов транзакции, финансовый счет зарегистрированного пользователя, сумму транзакции, данные онлайн/оффлайн продавца или банкомата, либо несколько регистрационных данных второго зарегистрированного пользователя, с которым осуществляется платежная операция.

В одном из вариантов реализации модуль уведомлений 118 сконфигурирован для получения сообщения о статусе транзакции от платежного шлюза или банка-эквайера 40 второго зарегистрированного пользователя и далее сконфигурирован для уведомления зарегистрированного пользователя и второго зарегистрированного пользователя о статусе транзакции соответственно через первый пользовательский интерфейс 104 и второй пользовательский интерфейс 20.

В одном из вариантов реализации система позволяет пользователю безопасно выполнять транзакции в режиме онлайн, в интернет-магазине, в торговых точках, в одноранговых сетях (P2P) и банкоматах.

В одном из вариантов реализации модуль памяти 106 взаимодействует с сервером транзакци й 108 для хранения базы данных и включает в себя первую таблицу поиска, содержащую список идентификаторов зарегистрированных пользователей и регистрационные данные для каждого из них, при этом регистрационные данные содержат личную информацию, финансовые счета зарегистрированных пользователей, а также токены этих счетов.

Банк-эмитент 30 может дополнительно выполнить (второй уровень) аутентификации пользователя после проверки данных о транзакциях / финансовых счетах зарегистрированного пользователя. Банк-эквайер 40 или платежный шлюз направляют детали транзакции в банк-эмитент 30, где банк-эмитент 30 отправляет зарегистрированному пользователю банка одноразовый пароль (OTP) для запроса на проведение транзакции с целью осуществления авторизации транзакции, а зарегистрированный пользователь подтверждает транзакцию путем ввода одноразового пароля (OTP) на платежном шлюзе. Таким образом, первая степень аутентификации будет выполнена сервером транзакций 108, а вторая степень аутентификации будет выполнена банком-эквайером 40.

Преимуществом данного подхода является, что модуль регистрации 114, модуль входа 116, модуль генерации проверочного кода 110, модуль контроля проверочного кода 112, модуль уведомления 118 могут быть реализованы с помощью одного или нескольких процессоров сервера транзакций 108. Процессор может быть процессором общего назначения, программируемой на месте логической матрицей (FPGA), интегральной схемой для конкретных приложений (ASIC), цифровым сигнальным процессором (DSP) и т. п.

Процессор может быть сконфигурирован для получения данных из памяти и/или записи данных в память. Память может быть, например, памятью с произвольным доступом (RAM), буфером памяти, жестким диском, базой данных, стираемой программируемой памятью только для чтения (EPROM), электрически стираемой программируемой памятью только для чтения (EEPROM), памятью только для чтения (ROM), флеш-памятью, жестким диском, дискетой, облачным хранилищем и/или так далее.

В настоящем изобретении также раскрывается способ 200, обеспечивающий безопасную обработку транзакций. Как продемонстрировано на **Фиг. 2A** и **2B**, способ 200 включает в себя следующие этапы:

На этапе 202, предоставление пользователям возможности регистрироваться и добавлять финансовые счета для выполнения безопасных платежных транзакций на электронном устройстве 10, используя первый пользовательский интерфейс 104 платежного приложения 102.

На этапе 204, предоставление зарегистрированным пользователям возможности осуществлять токенизацию финансовых счетов с помощью платформы для токенизации, используя первый пользовательский интерфейс 104 платежного приложения 102.

На этапе 206, сохранение в блоке памяти 106, база данных включает в себя первую таблицу поиска, содержащую список идентификаторов зарегистрированных пользователей и регистрационные данные для каждого из них, при этом регистрационные данные содержат личную информацию и финансовые счета зарегистрированных пользователей, а также токены этих счетов.

На этапе 208, создание модулем 110 генерации проверочного кода на сервере транзакций 108 первого одноразового проверочного кода/PIN-кода для финансовых счетов или токена финансовых счетов на основании каждого полученного запроса на проведение транзакции, а также их сохранение во второй таблице поиска.

На этапе 210, передача модулем 110 генерации проверочного кода на сервере транзакций 108 первого одноразового проверочного кода/PIN-кода в платежное приложение 102 с целью его отображения на первом пользовательском интерфейсе 104.

На этапе 212, получение введенного через второй пользовательский интерфейс 20 второго проверочного кода/PIN-кода модулем 112 контроля проверочного кода на сервере транзакций 108.

На этапе 214, сравнение первого одноразового проверочного кода/PIN-кода со вторым проверочным кодом/PIN-кодом из второй таблицы поиска, выполняемое компаратором 112a модуля 112 контроля проверочного кода.

На этапе 216, извлечение значения 216 финансовых счетов или токена, сохраненных для первого одноразового проверочного кода/PIN-кода, модулем извлечения 112b, водящим в состав модуля контроля проверочного кода 112.

На этапе 218, отправка данных о финансовом счете или токене модулем извлечения 112b, входящим в состав модуля контроля проверочного кода 112, в банк-эквайер 40 или платежный шлюз для одобрения, с последующей отправкой банком-эквайером 40 или платежным шлюзом деталей транзакции в платежное приложение 102 зарегистрированного пользователя.

На этапе 220, модуль авторизации 112c, входящий в состав модуля контроля проверочного кода 112, отправляет запрос на проведение транзакции и сведения о транзакции в платежное приложение 102 зарегистрированного пользователя для получения подтверждения на проведение транзакции, которое осуществляется проведением пальцем влево или вправо, либо с использованием биометрических данных или PIN-кода приложения.

На этапе 222, отправка модулем авторизации 112c, входящим в состав модуля контроля проверочного кода 112, статуса проверки транзакции в платежный шлюз или банк-эквайер 40, после чего платежный шлюз или банк-эквайер 40 отправляют транзакцию в банк-эмитент 30 для получения одобрения.

На этапе 224, банк-эквайер 40 или платежный шлюз направляют детали транзакции в банк-эмитент 30, где банк-эмитент 30 отправляет одноразовый пароль (OTP) для запроса на проведение транзакции зарегистрированному пользователю банка с целью осуществления авторизации транзакции, а зарегистрированный пользователь подтверждает транзакцию путем ввода одноразового пароля (OTP) на платежном шлюзе, после чего платежный шлюз или банк-эквайер передают статус транзакции в модуль авторизации.

На этапе 226, получение модулем уведомлений 118 информации о статусе подтвержденной транзакции на платежном приложении 102 зарегистрированного пользователя.

В одном из вариантов реализации изобретения этап 202 обеспечения возможности регистрации пользователей для осуществления безопасных платежных операций через первый пользовательский интерфейс 104 включает в себя:

- получение регистрационным модулем 114, входящим в состав сервера транзакций 108, регистрационных данных от пользователей через первый пользовательский интерфейс 104; и
- регистрация, с помощью модуля регистрации 114, пользователей путем создания уникальных идентификаторов, связанных с пользователями, и хранение регистрационных данных с уникальными идентификаторами в базе данных.

В одном из вариантов реализации, хранение зашифрованных с помощью механизма шифрования регистрационных данных.

В одном из вариантов реализации изобретения способ 200 дополнительно включает в себя:

- Предоставление регистрационным модулем 116, входящим в состав сервера транзакций 108, возможности генерировать набора учетных данных через первый пользовательский интерфейс 104; и
- выполнение модулем входа 116 аутентификации зарегистрированного пользователя на основе учетных данных перед тем, как разрешить зарегистрированному пользователю использовать первый пользовательский интерфейс 104 для инициирования платежной операции, где учетные данные выбраны из группы, состоящей из идентификатора входа и пароля, предварительно установленного PIN-кода и биометрической подписи зарегистрированного пользователя, включая по меньшей мере один из следующих вариантов: отпечатки пальцев, лицевая биометрия, рисунок радужки глаза, рисунок сетчатки глаза, рисунок вен пальцев, рисунок вен ладони и образец голоса.

Кроме того, способ 200 включает в себя следующие этапы:

- получение банком-эмитентом 30 данных о транзакции зарегистрированного пользователя;
- проверка банком-эмитентом 30 полученных данных о транзакции на основе предварительно сохраненных данных о клиенте;
- генерирование банком-эмитентом 30 первого одноразового пароля после проверки данных транзакции;

- отправка банком-эмитентом 30 сгенерированного первого одноразового пароля на электронное устройство 10 зарегистрированного пользователя банка для аутентификации пользователя;
- предоставление зарегистрированным пользователем банка платежному шлюзу данных для аутентификации;
- отправка платежным шлюзом полученного второго одноразового пароля в банк-эмитент 30; и
- сравнение банком-эмитентом 30 сгенерированного первого одноразового пароля со вторым одноразовым паролем, полученным от платежного шлюза, для аутентификации транзакции.

В одном из вариантов реализации, способ 200 включает в себя следующие этапы:

- получение модулем уведомления 118, входящим в состав сервера транзакций 108, сообщения о состоянии транзакции от платежного шлюза/банка-эквайера 40 второго зарегистрированного пользователя; и
- уведомление модулем уведомления 118 зарегистрированного пользователя и второго зарегистрированного пользователя о статусе транзакции через, соответственно, первый пользовательский интерфейс 104 и второй пользовательский интерфейс 20.

В одном из демонстрационных вариантов реализации, который отображен на **Фиг. 3A** и **Фиг. 4A-4J**, зарегистрированный клиент (т.е. клиент, зарегистрированный на сервере транзакций 108) использует платежное приложение 102 для выполнения защищенной транзакции с зарегистрированным продавцом (т.е. продавцом, зарегистрированным на сервере транзакций 108). Для обеспечения безопасных транзакций интернет-магазинов в режиме онлайн, сервер транзакций 108 с помощью средств связи соединен с серверами 70 зарегистрированных продавцов. На каждом торговом сервере 70 может быть размещен веб-сайт интернет-магазина 60.

Зарегистрированный клиент с электронного устройства 50 заходит на веб-сайт интернет-магазина 60 продавца. Веб-сайт интернет-магазина 60 предоставляет покупателю интерфейс 20 для добавления товаров в корзину и нажатия кнопки «оформить заказ», как показано на **Фиг. 4A**. Данное действие приведет покупателя на страницу оформления заказа. Как показано на **Фиг. 4B**, страница позволяет клиенту выбрать способ оплаты для

проведения транзакции. На странице отображается возможность «Оплатить с помощью HydePay(TM)» как один из вариантов проведения платежной операции. Клиент выбирает вариант оплаты, нажимая на вариант «оплатить с помощью HydePay(TM)», и попадает на страницу оплаты, показанную на **Фиг. 4C**, где ему/ей будет предложено ввести уникальный проверочный код/PIN-код (также именуемый "код/PINHydePay(TM) ").

Чтобы получить уникальный проверочный код/PIN-код, клиент открывает платежное приложение / приложение HydePay(TM) 102. Как показано на **Фиг. 4D**, платежное приложение 102 предлагает клиенту выбрать финансовый счет для проведения транзакции. После выбора финансового счета сервер транзакций 108 генерирует одноразовый проверочный код/PIN-код (т.е. первый одноразовый проверочный код/PIN-код) для карты и отображает сгенерированный код/PIN-код через интерфейс 104 платежного приложения 102, как показано на **Фиг. 4E**. Как показано на **Фиг. 4F**, клиент вводит этот проверочный код/PIN-код (т.е. второй проверочный код/PIN-код) на странице оплаты интерфейса веб-сайта 20.

В одном из вариантов реализации пользователь может подтвердить подлинность транзакции, проведя пальцем влево или вправо по выбранной платформе приложения, или введя проверочный код приложения/PIN-код или PIN-код приложения, либо используя биометрические данные.

В альтернативном варианте, как показано на **Фиг. 4G**, банк-эмитент 30 проводит дополнительную аутентификацию перед списанием средств со счета клиента. И/или банк-эквайер 40/платежный шлюз отправляет детали транзакции в банк-эмитент 30, где банк-эмитент 30 отправляет одноразовый пароль (OTP) для запроса транзакции зарегистрированному пользователю банка для одобрения транзакции, как показано на **Фиг. 4H**. Как показано на **Фиг. 4I**, клиент (зарегистрированный пользователь) одобряет транзакцию, вводя одноразовый пароль (OTP) через интерфейс сайта интернет-магазина 20. Зарегистрированный пользователь подтверждает транзакцию, вводя одноразовый пароль (OTP) на платежном шлюзе. Платежный шлюз и платежный шлюз или банк-эквайер 40 отправляет статус транзакции, как показано на **Фиг. 4J**. И/или банк-эмитент 30 отправляет клиенту SMS-сообщение, чтобы проинформировать его о статусе транзакции.

Демонстрационный псевдокод, изображающий реализацию способа 200 для обработки платежных транзакций интернет-магазина -

Выполните **ЭТАП А**

{

покупатель должен добавить товары в корзину и нажать кнопку «Оформить заказ»;

покупатель выбирает способ оплаты транзакции;

выбирает вариант оплаты, нажав на кнопку «Оплатить через HydePay(TM)»;

покупатель входит в платежное приложение 102, вводя свои безопасные учетные данные;

}

Если (успешный вход покупателя == ДА) **ЭТАП В**

{

выбрать финансовый счет для проведения операции;

сгенерировать проверочный код/PIN-код;

покупатель вводит полученный одноразовый пароль в интерфейс сайта интернет-магазина;

нажать на кнопку «Оплатить»;

}

Иначе

{

Вход в систему не удался;

ПЕРЕЙТИ К ЭТАПУ А;

}

Если (проверочный код/PIN-код, сгенерированный покупателем, == проверочному коду/PIN-коду, введенному на веб-сайте интернет-магазина) **ЭТАП С**

{

отправляет запрос на авторизацию покупателю, чтобы он авторизировал транзакцию, проведя пальцем вправо или влево;

и/или

банк-эмитент отправляет покупателю (зарегистрированному пользователю банка) одноразовый пароль (OTP) для одобрения транзакции;

покупатель вводит одноразовый пароль (OTP) на веб-сайте интернет-магазина, чтобы подтвердить подлинность транзакции;

}

Иначе

{

проверочный код/PIN-код не совпадает;

транзакция отклоняется;

ПЕРЕЙТИ К ЭТАПУ B;

}

В соответствии с другим аспектом настоящего изобретения, со ссылкой на **Фиг. 3B** и **Фиг. 6A-6J**, система 100 используется для обработки одноранговых (P2P) платежных транзакций. В одном из вариантов реализации второй пользователь запросил платеж в размере «x» и отправил запрос первому пользователю, как показано на **фиг. 6A**, первый пользователь вошел в платежное приложение 102, введя свои учетные данные для безопасного входа, как показано на **фиг. 6B**. Как показано на **фиг. 6C**, платежное приложение 102 предоставляет первый пользовательский интерфейс 104a, чтобы обеспечить возможность первому пользователю сделать выбор финансового счета для осуществления транзакции и сгенерировать соответствующий финансовому счету проверочный код/PIN-код для транзакции. Как показано на **Фиг. 6D**, первый пользователь отправляет сгенерированный проверочный код/PIN-код второму пользователю через SMS, электронную почту, службу обмена сообщениями (например, Whatsapp) или любое другое средство связи. Чтобы получить платеж, второй пользователь на своем устройстве 10b запускает платежное приложение 102. После запуска платежное приложение 102 предоставляет второй пользовательский интерфейс 104b, чтобы позволить второму зарегистрированному пользователю войти в свое приложение 102 путем ввода защищенных учетных данных. Как показано на **Фиг. 6E**, второй зарегистрированный пользователь на втором пользовательском интерфейсе 104b своего платежного приложения 102 вводит проверочный код/PIN-код, полученный от первого пользователя, и вводит сумму «x». Далее второй пользователь отправляет запрос на авторизацию запрашиваемой суммы «x» первому пользователю. Сервер транзакций 108 сравнивает проверочный код/PIN-код, сгенерированный первым пользователем, с проверочным кодом/PIN-кодом, полученным от второго пользователя, и одобряет транзакцию, если они совпадают. Как показано на **Фиг. 6F**, после одобрения/успешной проверки сервер транзакций 108 отправляет первому пользователю осуществить запрос на авторизацию через интерфейс платежного приложения 104, чтобы обеспечить возможность первому пользователю произвести авторизацию транзакции. Авторизация может быть выполнена с помощью одного или нескольких способов, описанных в настоящем документе. И/или банк-эквайер

40/платежный шлюз отправляет детали транзакции в банк-эмитент 30, где банк-эмитент 30 отправляет одноразовый пароль (OTP) для запроса транзакции, как показано на **Фиг. 6G**, зарегистрированному пользователю банка для одобрения транзакции, как показано на **Фиг. 6H**. Первый пользователь вводит одноразовый парль (OTP) на платежном шлюзе для авторизации транзакции, как показано на **Фиг. 6I** и **Фиг. 6J**.

Демонстрационный псевдокод, изображающий реализацию способа 200 для обработки одноранговых (P2P) платежных транзакций -

Выполните **ЭТАП А**

{

второй пользователь запросил оплату суммы «x» и отправил запрос первому пользователю;

Первый или второй пользователь входит в платежное приложение 102, вводя свои безопасные учетные данные;

}

Если (успешный вход первого пользователя == ДА) **ЭТАП В**

{

выбрать финансовый счет для проведения операции;

сгенерировать проверочный код/PIN-код для транзакции;

первый пользователь отправляет сгенерированный проверочный код/PIN-код второму пользователю;

}

Иначе

{

Вход в систему не удался;

ПЕРЕЙТИ К ЭТАПУ А;

}

Если (успешный вход второго пользователя == ДА) **ЭТАП С**

{

второй зарегистрированный пользователь вводит проверочный код/PIN-код, полученный от первого пользователя;

второй пользователь вводит сумму «x»;

второй пользователь отправляет запрос на авторизацию запрашиваемой суммы «x» первому;

}

Иначе

{

Вход в систему не удался;

ПЕРЕЙТИ К ЭТАПУ A;

}

Если (первый пользователь получает запрос от второго пользователя)

{

первый пользователь должен авторизировать транзакцию, проведя пальцем вправо или влево;

И/или

банк-эмитент отправляет первому пользователю (зарегистрированному пользователю банка) одноразовый пароль (OTP) для одобрения транзакции;

Первый пользователь вводит одноразовый пароль (OTP) через платежный шлюз для авторизации транзакции;

}

Иначе

{

транзакция отклоняется;

}

В соответствии с еще одним аспектом данного изобретения, со ссылкой на **фиг. 5A-5G**, система 100 используется для обработки транзакций в розничном магазине. В одном из вариантов реализации клиент, желающий совершить платеж продавцу на сумму «x» с помощью приложения/платежного приложения 102 HydePay$^{(TM)}$, входит в приложение 102, введя свои безопасные учетные данные. Продавец выставляет счет за приобретенный клиентом товар и просит клиента оплатить его, как показано на **Фиг. 5A**. После этого клиент выбирает финансовый счет для проведения транзакции и генерирует соответствующий финансовому счету проверочный код/PIN-код для транзакции, как показано на **Фиг. 5B** и **5C**. Затем покупатель передает продавцу проверочный код/PIN-код. Чтобы получить платеж, продавец входит в свое платежное приложение 102, введя

защищенные учетные данные. Как показано на **Фиг. 5C**, продавец затем вводит проверочный код/PIN-код, полученный от клиента через интерфейсе 104 и своего платежного приложения 102 и вводит сумму «x». Сервер транзакций 108 сравнивает проверочный код/PIN-код, сгенерированный клиентом, с проверочным кодом/PIN-кодом, полученным от продавца, и одобряет транзакцию, если они совпадают. Как показано на **Фиг. 5D** и **5E**, после одобрения/успешной проверки сервер транзакций 108 отправляет клиенту запрос на авторизацию через интерфейс платежного приложения 104, чтобы обеспечить возможность клиенту произвести авторизацию транзакции. Авторизация может быть выполнена с помощью одного или нескольких способов, описанных в настоящем документе. И/или банк-эквайер 40 или платежный шлюз отправляет детали транзакции в банк-эмитент 30, где банк-эмитент (30) отправляет клиенту (зарегистрированному пользователю) банка одноразовый пароль (OTP) для одобрения транзакции, как показано на **Фиг. 5F**, где клиент (зарегистрированный пользователь) одобряет транзакцию путем ввода одноразового пароля (OTP) на платежном шлюзе продавца, как показано на **Фиг. 5G**.

Демонстрационный псевдокод, изображающий реализацию способа 200 для обработки платежных транзакций в розничном магазине -

Выполните **ЭТАП A**

{

продавец формирует счет и запрашивает проверочный код/PIN-код;

покупатель входит в платежное приложение 102, вводя свои безопасные учетные данные;

}

Если (успешный вход покупателя == ДА) **ЭТАП B**

{

сгенерировать проверочный код/PIN-код;

затем покупатель передает продавцу проверочный код/PIN-код;

}

Иначе

{

Вход в систему не удался;

ПЕРЕЙТИ К ЭТАПУ A;

}

Если (успешный вход продавца == ДА) **ЭТАП С**

{

вводит проверочный код/PIN-код, сообщенный покупателем;

вводит сумму «x»;

}

Иначе

{

Вход в систему не удался;

ПЕРЕЙТИ К ЭТАПУ А;

}

Пока (покупатель получил запрос на оплату от продавца)

{

отправляет запрос на авторизацию покупателю через интерфейс платежного приложения 104, чтобы покупатель авторизировал транзакцию, проведя пальцем вправо или влево;

И/или

банк-эмитент отправляет покупателю (зарегистрированному пользователю банка) одноразовый пароль (OTP) для одобрения транзакции;

Покупатель (зарегистрированный пользователь) подтверждает транзакцию, вводя одноразовый пароль (OTP) на платежном шлюзе продавца;

}

В одном из вариантов реализации, транзакция желаемой суммы может быть проведена с помощью кода Hydepin, при этом код Hydepin необходимо ввести через интерфейс банкомата и выбрать или ввести желаемую сумму для снятия.

В соответствии с еще одним аспектом данного изобретения, как показано на **Фиг. 7A-7H**, система 100 используется для обработки транзакций в банкомате (ATM). Сервер транзакций 108 связан с системами обработки банкоматов, чтобы обеспечить возможность проведения транзакций через платежное приложение/HydePay(TM) app 102. В одном из вариантов реализации зарегистрированный пользователь, желающий снять в банкомате сумму «x» с помощью приложения/платежного приложения 102 HydePay(TM), выбирает

опцию «снять с помощью HydePay(TM)» на интерфейсе банкомата, как показано на **Фиг. 7A**. При выборе этого варианта интерфейс банкомата предложит пользователю ввести проверочный код/PIN-код для снятия денег, как показано на **Фиг. 7B**. Для получения проверочного кода/PIN-код пользователь входит в платежное приложение 102, вводя свои безопасные учетные данные. После этого пользователь выбирает финансовый счет для проведения транзакции и генерирует соответствующий финансовому счету проверочный код/PIN-код для транзакции по снятию средств, как показано на **Фиг. 7C** и **7D**. Затем пользователь вводит через интерфейс банкомата проверочный код/PIN-код. Через интерфейс банкомата пользователь вводит сумму транзакции «x» для снятия и указывает проверочный код/PIN-код, как показано на **Фиг. 7F** и **Фиг. 7G**. Сервер транзакций 108 сравнивает проверочный код/PIN-код, сгенерированный пользователем, с проверочным кодом/PIN-кодом, полученным от интерфейса банкомата, и одобряет транзакцию, если они совпадают, как показано на **Фиг. 7H**. После одобрения/успешной проверки сервер транзакций 108 отправляет клиенту запрос на авторизацию через интерфейс платежного приложения 104, чтобы обеспечить возможность клиенту произвести авторизацию транзакции. Авторизация может быть выполнена с помощью одного или нескольких способов, описанных в настоящем документе. И/или банк-эквайер 40 или платежный шлюз отправляет детали транзакции в банк-эмитент 30, где банк-эмитент (30) отправляет клиенту (зарегистрированному пользователю) банка одноразовый пароль (OTP) для одобрения транзакции, где клиент (зарегистрированный пользователь) одобряет транзакцию путем ввода одноразового пароля (OTP) через интерфейс банкомата. Демонстрационный псевдокод, изображающий реализацию способа 200 для обработки платежных транзакций в банкомате -

Выполните **ЭТАП A**

{

покупатель входит в платежное приложение 102, вводя свои безопасные учетные данные;

}

Если (успешный вход покупателя == ДА) **ЭТАП B**

{

выбирает опцию «Снять деньги с помощью HydePay(TM)» на интерфейсе банкомата;

генерирует проверочный код/PIN-код;

клиент вводит на интерфейсе банкомата сумму операции «x» для снятия;

вводит через интерфейсе банкомата проверочный код/PIN-код для снятия денег;

}

Иначе

{

Вход в систему не удался;

ПЕРЕЙТИ К ЭТАПУ A;

}

Если (проверочный код/PIN-код, сгенерированный клиентом, == проверочному коду/PIN-коду, полученному от банкомата) **ЭТАП C**

{

одобряет транзакцию, если они совпадают;

}

Иначе

{

проверочный код/PIN-код не совпадает;

транзакция не проведена/отклоняется;

ПЕРЕЙТИ К ЭТАПУ B;

}

Пока (клиент получил запрос на оплату) **ЭТАП D**

{

отправляет запрос на авторизацию покупателю через интерфейс платежного приложения 104, чтобы покупатель авторизировал транзакцию, проведя пальцем вправо или влево;

И/или

банк-эмитент отправляет покупателю (зарегистрированному пользователю банка) одноразовый пароль (OTP) для одобрения транзакции;

клиент (зарегистрированный пользователь) подтверждает транзакцию, вводя одноразовый пароль (OTP) через интерфейс банкомата;

}

В соответствии с другим аспектом изобретения система 100 используется для обработки транзакций в традиционной розничной торговой точке, оснащенной системой для точек продаж. У продавца может не быть платежного приложения/приложения HydePay$^{(TM)}$ 102

или он может не знать, как использовать платежное приложение 102. В этом случае продавцу выдается платежная карта (также называемая «картой HydePay(TM)») для приема платежей от клиентов. В одном из вариантов реализации зарегистрированный клиент, желающий совершить платеж продавцу на сумму «x» с помощью приложения/платежного приложения 102 HydePay(TM) , входит в приложение 102, введя свои безопасные учетные данные. После этого клиент выбирает финансовый счет для проведения транзакции и генерирует соответствующий финансовому счету проверочный код/PIN-код для транзакции. Затем клиент передает продавцу проверочный код/PIN-код. Чтобы получить платеж, продавец вставляет свою карту HydePay(TM) в аппарат, расположенный на точке продажи (POS). POS-терминал настроен на распознавание карты HydePay(TM) и предлагает продавцу ввести проверочный код/PIN-код, после ввода которого продавец указывает сумму «x». Затем продавец вводит проверочный код/PIN-код, сообщенный клиентом, а также вводит сумму «x» через интерфейс POS-терминала. Затем POS-терминал отправляет полученный проверочный код/PIN-код на сервер транзакций 108 напрямую, либо через сервер продавца/эквайера. Сервер транзакций 108 сравнивает проверочный код/PIN-код, сгенерированный клиентом, с проверочным кодом/PIN-кодом, полученным от продавца, и одобряет транзакцию, если оба кода совпадают. После одобрения/успешной проверки сервер транзакций 108 отправляет запрос на транзакцию, включающий детали транзакции, в платежное приложение 102 зарегистрированного пользователя для подтверждения транзакции путем проведения пальцем влево или вправо, или с помощью биометрического или прикладного PIN-кода, либо банк-эквайер 40/платежный шлюз отправляет детали транзакции в банк-эмитент 30, где банк-эмитент 30 отправляет запрос одноразового пароля (OTP) транзакции зарегистрированному пользователю банка для одобрения транзакции, где зарегистрированный пользователь одобряет транзакцию путем ввода одноразового пароля (OTP) через интерфейс POS-терминала, а платежный шлюз или банк-эквайер 40 отправляет статус транзакции в модуль авторизации 112c.

В соответствии с еще одним аспектом данного изобретения, система 100 используется для хранения данных карты на онлайн-платформе в соответствии с правилами и нормами, установленными руководящими органами указанных стран, а также для их токенизации с целью проведения транзакции.

Демонстрационный псевдокод, изображающий реализацию способа 200 для обработки платежных транзакций в традиционной розничной торговой точке, оснащенной системой для точек продаж -

Выполните **ЭТАП A**

{

покупатель входит в платежное приложение 102, вводя свои безопасные учетные данные;

}

Если (успешный вход покупателя == ДА) **ЭТАП B**

{

выберите финансовый счет;

сгенерировать проверочный код/PIN-код;

клиент передает продавцу проверочный код/PIN-код;

}

Иначе

{

Вход в систему не удался;

ПЕРЕЙТИ К ЭТАПУ A;

}

Выполните **ЭТАП C**

{

Вставьте карту HydePay(TM) в терминал в точке продаж (POS);

}

Если (карта HydePay(TM) == действительна и распознана) **ЭТАП D**

{

запрос продавцу ввести проверочный код/ PIN-код;

затем продавец вводит проверочный код/PIN-код, сообщенный клиентом, а также вводит сумму «x»;

}

Иначе

{

Карта HydePay(TM) не действительна;

проверочный код/PIN-код не совпадает;

транзакция не проведена/отклоняется;

ПЕРЕЙТИ К ЭТАПУ C;

}

Если (проверочный код/PIN-код, сгенерированный клиентом, == проверочному коду/PIN-коду, полученному от банкомата) **ЭТАП E**

{

отправляет запрос на авторизацию покупателю, чтобы он авторизировал транзакцию, проведя пальцем вправо или влево;

и/или

банк-эмитент отправляет покупателю (зарегистрированному пользователю банка) одноразовый пароль (OTP) для одобрения транзакции;

покупатель вводит одноразовый пароль (OTP) через интерфейс POS-терминала, чтобы подтвердить подлинность транзакции;

}

Иначе

{

проверочный код/PIN-код не совпадает;

транзакция не проведена/отклоняется;

ПЕРЕЙТИ К ЭТАПУ D;

}

Система 100 позволяет клиенту совершать операции в онлайн, в интернет-магазинах, торговых точках и банкоматах без необходимости раскрывать какие-либо финансовые данные, такие как банковские реквизиты, реквизиты счета, номер дебетовой карты, номер предоплаченной карты, номер кредитной карты, данные о сроке действия карты, проверочное значение карты (CVV), идентификатор входа в систему интернет-банкинга, учетные данные, связанные со счетом финансового сервиса, идентификатор виртуального платежного адреса (VPA)/единого платежного интерфейса (UPI), идентификатор PayPal, идентификатор Zelle и другие идентификаторы транзакций в любой момент и в любой форме для стороннего сервиса, интерфейса приложения или продавца (например, через веб-

сайт интернет-магазина) во время транзакции. Когда система 100 используется для проведения платежных операций с продавцом, от клиента требуется сообщить продавцу только проверочный код/PIN-код (HydeCode/PIN). Другими словами, клиент использует приложение HydePay(TM), чтобы «скрыть» финансовые счета от продавца, а вместо финансовых счетов клиент вводит только одноразовый HydeCode(TM)/PIN-код на веб-сайте продавца. Платежное приложение 102 (т.е. приложение HydePay(TM)) также позволяет зарегистрированным клиентам безопасно токенизировать свои финансовые счета и хранить токен во второй таблице поиска, а также динамически генерировать уникальные проверочные коды/PIN-коды (т.е. HydeCodes/PIN) для проведения одноранговых транзакций от клиента клиенту (P2P), от клиента продавцу (P2M) или через банкомат (ATM). Такой подход обеспечивает полную безопасность и снижает риск мошенничества при проведении платежных операций.

В одном из вариантов реализации система 100 может быть интегрирована с любым из национальных и международных банковских приложений, мобильных кошельков или платежных приложений.

Описанные здесь средства связи могут относиться к средствам для передачи и приема электронных данных. Средства связи могут включать, например, Интернет, Всемирную паутину, интрасеть, кабель (в том числе оптоволоконный), магнитную связь, электромагнитную связь (в том числе радиочастотную, микроволновую и инфракрасную связь) и электронную связь. Средства беспроводной связи могут поддерживать различные протоколы и технологии беспроводных сетей связи, такие как Near Field Communication (NFC), Wi-Fi, Bluetooth, 4G Long Term Evolution (LTE), Code Division Multiplexing Access (CDMA), Universal Mobile Telecommunication System (UMTS) и Global System for Mobile Telecommunication (GSM).

Функции, описанные в настоящем документе, могут быть реализованы в аппаратном обеспечении, программном обеспечении, выполняемом процессором, встроенном программном обеспечении или в любой их комбинации. Если функции реализованы в программном обеспечении, выполняемом процессором, они могут быть сохранены или переданы в виде одной или нескольких инструкций или кода на считываемом компьютером носителе. Другие примеры и варианты осуществления находятся в рамках и духе описания изобретения и прилагаемой формулы изобретения. Например, в силу природы программного обеспечения, описанные выше функции могут быть реализованы с помощью

программного обеспечения, выполняемого процессором, аппаратного обеспечения, встроенного программного обеспечения, физического соединения или комбинации любого из них. Элементы, реализующие функции, также могут быть физически расположены в различных местах, в том числе распределены таким образом, что части функций реализуются в различных физических местах.

Приведенное выше описание вариантов реализации изобретения было представлено для целей иллюстрации и не предназначено для ограничения спектра применения данного изобретения. Отдельные компоненты конкретной реализации, как правило, не ограничиваются этим конкретным воплощением, а являются взаимозаменяемыми. Такие изменения не должны рассматриваться как отклонения от описания данного изобретения, и все такие модификации считаются находящимися в рамках данного изобретения.

ТЕХНИЧЕСКИЕ УСОВЕРШЕНСТВОВАНИЯ

Описанное выше изобретение имеет ряд технических преимуществ, включая, но не ограничиваясь этим, реализацию системы для безопасной обработки транзакций и способа ее реализации, которые:

- не требуют от пользователя для проведения платежной транзакции ввода финансовых счетов (включая такие данные, как банковские реквизиты, данные счета, номер дебетовой карты, номер предоплаченной карты, номер кредитной карты, сведения о сроке действия карты, проверочное значение карты (CVV), идентификатор входа в систему интернет-банкинга, учетные данные, связанные со счетом финансовых услуг, идентификатор виртуального платежного адреса (VPA)/интерфейса унифицированных платежей (UPI), Идентификатор PayPal, идентификатор Zelle и другие идентификаторы транзакций;
- предлагают пользователю безопасный и удобный способ совершения онлайн, офлайн или одноранговых транзакций;
- позволяют пользователям совершать онлайн или офлайн транзакции в точках продаж (POS) или банкоматах без использования финансового счета;
- снижают вероятность подверженности хакерским атакам;
- позволяют избежать несанкционированных платежных операций;
- предлагают высокий процент успешно проведенных платежей;
- предлагают удобный способ проведения платежей;

- предлагают интуитивно понятный интерфейс для проведения платежей; и
- обеспечивают безопасный платежный интерфейс для простой и мгновенной транзакции.

Варианты реализации данного изобретения, а также различные особенности и детали усовершенствований описаны со ссылкой на не накладывающие ограничений варианты реализации в далее приведенном описании. Описания известных компонентов и способов обработки опущены, чтобы без необходимости не загромождать информацией приведенные здесь варианты реализации. Примеры, используемые в настоящем документе, предназначены только для облегчения понимания способов, которыми могут быть реализованы варианты применения данного изобретения, а также для того, чтобы дать возможность специалистам в данной области практиковать варианты реализации описанного в данном документе изобретения. Соответственно, приведенные примеры не должны рассматриваться как ограничивающие спектр применения описанных здесь вариантов реализации.

Вышеприведенное описание конкретных вариантов реализации изобретения настолько полно раскрывает общий характер вариантов реализации изобретения, что другие специалисты могут, применяя современные знания, легко модифицировать и/или адаптировать для различных применений такие конкретные варианты реализации изобретения, не отступая от общей концепции, и, следовательно, такие адаптации и модификации должны и предназначены для понимания в рамках значения и диапазона эквивалентов раскрытых вариантов реализации изобретения. Следует понимать, что фразеология или терминология, используемая в данном документе, предназначена для описания возможностей, а не для указания ограничений. Таким образом, несмотря на то, что в настоящем документе описаны предпочтительные варианты реализации, специалисты в данной области поймут, что описанные здесь варианты реализации могут быть внедрены с изменениями в рамках духа и в рамках описанных здесь вариантов реализации.

Использование выражения «по меньшей мере» или «по меньшей мере один» предполагает использование одного или нескольких элементов или ингредиентов или единиц, в зависимости от варианта реализации изобретения, для достижения одного или нескольких желаемых целей или результатов.

Хотя в настоящем документе значительное внимание уделяется компонентам и составным частям предпочтительных вариантов реализации изобретения, следует признать, что можно

создать множество вариантов реализации изобретения и внести множество изменений в предпочтительные варианты реализации изобретения, не отступая от принципов, изложенных в описании. Эти и другие изменения в предпочтительном варианте реализации изобретения, а также в других вариантах описания станут очевидными для специалистов в данной области из описания, приведенного в настоящем документе, при этом следует четко понимать, что вышеприведенное описание должно быть истолковано только как иллюстрация возможной реализации, а не как ограничение.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Система (100) для обеспечения безопасной обработки транзакций, включающая в себя:

i. платежное приложение (102), сконфигурированное для предоставления первого пользовательского интерфейса (104), при запуске на электронном устройстве (10), для предоставления возможности пользователям осуществлять регистрацию и добавление финансовых счетов для проведения безопасных платежных операций, причем платежное приложение (102) дополнительно сконфигурировано для предоставления возможности зарегистрированному пользователю токенизации указанных финансовых счетов с помощью платформы токенизации;

ii. модуль памяти (106), который настроен для хранения базы данных и включает в себя первую таблицу поиска, содержащую список идентификаторов зарегистрированных пользователей и регистрационные данные для каждого из них, при этом регистрационные данные содержат личную информацию, финансовые счета зарегистрированных пользователей, а также токены этих финансовых счетов;

iii. сервер транзакций (108), на котором размещено указанное платежное приложение (102), причем сервер транзакций (108) включает в себя:

- модуль генерации проверочного кода (110, который сконфигурирован для генерации первого одноразового проверочного кода/PIN-кода для указанных финансовых счетов или указанного токена финансовых счетов на основе каждого полученного запроса на транзакцию и сохранения обоих во второй таблице поиска, модуль генерации проверочного кода (110) сконфигурирован для последующей отправки указанного первого одноразового проверочного кода/PIN-кода в платежное приложение (102) для отображения его через указанный первый пользовательский интерфейс (104); и

- модуль контроля проверочного кода (112), включающий в себя:

– компаратор (112a), который сконфигурирован для приема второго проверочного кода/PIN-кода, введенного через второй пользовательский интерфейс (20), и сравнения указанного первого одноразового

проверочного кода/PIN-кода с указанным вторым проверочным кодом/PIN-кодом из второй таблицы;

– модуль извлечения (112b), который сконфигурирован для извлечения данных указанных финансовых счетов или указанных токенов, хранящихся в соответствии с первым одноразовым проверочным кодом/PIN-кодом, а также для отправки данных указанных финансовых счетов или токенов в банк-эквайер (40) или на платежный шлюз для утверждения, после чего указанный банк-эквайер (40) или платежный шлюз отправляет детали транзакции в указанное платежное приложение (102) зарегистрированного пользователя;

– модуль авторизации (112c), который сконфигурирован для взаимодействия с указанным модулем извлечения (112b) для отправки запроса транзакции, содержащего детали транзакции, в указанное платежное приложение (102) зарегистрированного пользователя для проверки транзакции путем проведения пальцем влево или вправо или с помощью биометрического или цифрового PIN-кода, и далее сконфигурирован для отправки статуса проверки транзакции в указанный платежный шлюз или указанный банк-эквайер (40), после чего платежный шлюз или банк-эквайер (40 отправляет транзакцию в указанный банк-эмитент (30 для одобрения,

и/или указанный банк-эквайер (40) или платежный шлюз направляют детали транзакции в банк-эмитент (30), где указанный банк-эмитент (30) отправляет зарегистрированному пользователю банка одноразовый пароль (OTP) для запроса на проведение транзакции с целью осуществления авторизации транзакции, а зарегистрированный пользователь подтверждает транзакцию путем ввода одноразового пароля (OTP) на платежном шлюзе, после чего указанный платежный шлюз или банк-эквайер (40) передают статус транзакции в модуль авторизации (112c); и

- модуль уведомления (118), сконфигурированный для взаимодействия с модулем авторизации (112c) с целью получения статуса одобренной транзакции в указанном платежном приложении (102) зарегистрированного пользователя.

2. Система (100) по п.1, в которой указанная память (106) реализована в виде области хранения на указанном сервере транзакций (108) или независимого устройства хранения, коммуникативно связана с указанным сервером транзакций (108).

3. Система (100) по п. 1, в которой указанные личные сведения выбираются из группы данных, состоящей из имени, номера мобильного телефона, идентификатора электронной почты и информации, связанной соответствующим человеком.

4. Система (100) по п. 1, в которой указанные финансовые счета выбираются из группы данных, включающих в себя банковские реквизиты, данные счета, номер дебетовой карты, номер предоплаченной карты, номер кредитной карты, сведения о сроке действия карты, проверочное значение карты (CVV), идентификатор входа в систему интернет-банкинга, учетные данные, связанные со счетом финансовых услуг, идентификатор виртуального платежного адреса (VPA)/интерфейса унифицированных платежей (UPI), Идентификатор PayPal, идентификатор Zelle и другие идентификаторы транзакций или токены финансовых счетов.

5. Система (100) по п. 1, в которой указанный сервер транзакций 118 включает в себя модуль регистрации (114, сконфигурированный для получения регистрационных данных от пользователей через первый пользовательский интерфейс (104 с последующей регистрацией пользователей путем создания связанных с ними уникальных идентификаторов и хранением регистрационных данных с указанными уникальными идентификаторами пользователей в указанной первой таблице поиска.

6. Система (100) по п. 5, в которой указанный модуль регистрации (114) настроен на хранение зашифрованных с помощью механизма шифрования регистрационных данных.

7. Система (100) по п. 1, в которой указанный сервер транзакций (108) также включает в свой состав модуль входа в систему (116), который сконфигурирован для обеспечения возможности пользователю генерации и задания учетных данных для входа в систему через указанный первый пользовательский интерфейс (104), и далее сконфигурирован для выполнения аутентификации зарегистрированного пользователя на основе учетных данных для входа в систему, после чего зарегистрированный пользователь получает разрешение использовать указанное приложение (102) для инициирования платежной операции.

8. Система (100) по п. 7, в которой указанные учетные данные выбираются из группы, состоящей из идентификатора и пароля, предварительно установленного PIN-кода и биометрической подписи зарегистрированного пользователя, включая по меньшей мере один из следующих способов: отпечатки пальцев, биометрические данные лица, рисунок радужной оболочки глаза, рисунок сетчатки глаза, рисунок вен пальцев, рисунок вен ладони или образец голоса.

9. Система (100) по п. 1, в которой указанные данные о транзакции содержат идентификатор зарегистрированного пользователя, по меньшей мере одно из идентификатора транзакции, финансового счета зарегистрированного пользователя, суммы транзакции, данных онлайн/оффлайн продавца или банкомата, либо одних или более регистрационных данных второго зарегистрированного пользователя, с которым осуществляется платежная операция.

10. Система (100) по п. 1, в которой указанный модуль уведомлений (118) сконфигурирован для получения сообщения о статусе транзакции от платежного шлюза или банка-эквайера (40) второго зарегистрированного пользователя и далее сконфигурирован для уведомления зарегистрированного пользователя и второго зарегистрированного пользователя о статусе транзакции соответственно через первый пользовательский интерфейс (104) и второй пользовательский интерфейс (20).

11. Система (100) по любому из п.п. 1-10, которая позволяет пользователю безопасно выполнять транзакции в режиме онлайн, в интернет-магазине, в торговых точках, в одноранговых сетях (P2P) и банкоматах.

12. Способ (200) обеспечения безопасной обработки транзакций, включающий в себя:

i. предоставление пользователям возможности (202) регистрироваться и добавлять финансовые счета для выполнения безопасных платежных транзакций на электронном устройстве (10), используя первый пользовательский интерфейс (104) платежного приложения (102);

ii. предоставление зарегистрированным пользователям возможности (204) осуществлять токенизацию указанных финансовых счетов с помощью платформы для токенизации, используя указанный первый пользовательский интерфейс (104) платежного приложения (102);

iii. сохранение (206), в блоке памяти (106), базы данных, которая включает в себя первую таблицу поиска, содержащую список идентификаторов зарегистрированных пользователей и регистрационные данные для каждого из них, при этом регистрационные данные содержат личную информацию и финансовые счета зарегистрированных пользователей, а также токены указанных финансовых счетов;

iv. создание (208) указанным модулем генерации проверочного кода (110) на сервере транзакций (108 первого одноразового проверочного кода/PIN-кода для указанных финансовых счетов или указанного токена финансовых счетов на основании каждого полученного запроса на проведение транзакции, а также их сохранение во второй таблице поиска;

v. передачу (210) указанным модулем генерации проверочного кода (110) на указанном сервере транзакций (108) первого одноразового проверочного кода/PIN-кода в платежное приложение (102) с целью его отображения на указанном первом пользовательском интерфейсе (104);

vi. получение (212) введенного через второй пользовательский интерфейс (20) второго проверочного кода/PIN-кода модулем контроля проверочного кода (112) на указанном сервере транзакций (108);

vii. сравнение (214) указанного первого одноразового проверочного кода/PIN-кода со вторым проверочным кодом/PIN-кодом из второй таблицы поиска, выполняемое компаратором (112a) указанного модуля контроля проверочного кода (112);

viii. извлечение значения (216) указанных финансовых счетов или указанного токена, сохраненных для указанного первого одноразового проверочного кода/PIN-кода, модулем извлечения (112b,) водящим в состав указанного модуля контроля проверочного кода (112);

ix. отправку (218) данных о финансовом счете или токене модулем извлечения (112b), входящим в состав указанного модуля контроля проверочного кода (112), в банк-эквайер (40) или платежный шлюз для одобрения, с последующей отправкой банком-эквайером (40) или платежным шлюзом деталей транзакции в указанное платежное приложение (102) зарегистрированного пользователя;

x. отправку (220) модулем авторизации (112c), входящим в состав указанного модуля контроля проверочного кода (112), запроса на проведение транзакции

и сведений о транзакции в платежное приложение (102) зарегистрированного пользователя для получения подтверждения на проведение транзакции, которое осуществляется проведением пальцем влево или вправо, либо с использованием биометрических данных или PIN-кода приложения;

xi. отправку (222) модулем авторизации (112c), входящим в состав указанного модуля контроля проверочного кода (112), статуса проверки транзакции в платежный шлюз или банк-эквайер (40), после чего указанный платежный шлюз или банк-эквайер (40) отправляют транзакцию в указанный банк-эмитент (30) для получения одобрения;

xii. отправку (224) указанным банком-эквайером (40) или платежным шлюзом деталей транзакции в банк-эмитент (30), где указанный банк-эмитент (30) отправляет одноразовый пароль (OTP) для запроса на проведение транзакции зарегистрированному пользователю банка с целью осуществления авторизации транзакции, а зарегистрированный пользователь подтверждает транзакцию путем ввода одноразового пароля (OTP) на платежном шлюзе, после чего указанный платежный шлюз или банк-эквайер передают статус транзакции в модуль авторизации; и

xiii. получение (226) модулем уведомлений (118) информации о статусе указанной подтвержденной транзакции на указанном платежном приложении (102) зарегистрированного пользователя.

13. Способ (200) по п.12, в котором указанные личные сведения выбирают из группы данных, состоящей из имени, номера мобильного телефона, идентификатора электронной почты и информации, связанной соответствующим человеком.

14. Способ (200) по п.12, в котором указанные финансовые счета выбирают из группы данных, включающих в себя банковские реквизиты, данные счета, номер дебетовой карты, номер предоплаченной карты, номер кредитной карты, сведения о сроке действия карты, проверочное значение карты (CVV), идентификатор входа в систему интернет-банкинга, учетные данные, связанные со счетом финансовых услуг, идентификатор виртуального платежного адреса (VPA)/интерфейса унифицированных платежей (UPI), идентификатор PayPal, идентификатор Zelle и другие идентификаторы транзакций или токены финансовых счетов.

15. Способ (200) по п.12, в котором, на указанном этапе обеспечения возможности (202), через указанный первый пользовательский интерфейс (104), регистрации пользователей для осуществления безопасных платежных операций включает следующие этапы:

- получение регистрационным модулем (114), входящим в состав указанного сервера транзакций (108), регистрационных данных от пользователей через указанный первый пользовательский интерфейс (104); и
- регистрацию, с помощью указанного модуля регистрации (114), пользователей путем создания уникальных идентификаторов, связанных с пользователями, и хранение указанных регистрационных данных с уникальными идентификаторами в базе данных.

16. Способ (200) по п.12, в котором осуществляют хранение регистрационных данных, зашифрованных с помощью механизма шифрования.

17. Способ (200) по п.12, который дополнительно включает в себя следующие этапы:

- предоставление регистрационным модулем (116), входящим в состав указанного сервера транзакций (108), возможности генерировать набора учетных данных через указанный первый пользовательский интерфейс (104); и
- выполнение указанным модулем регистрации (116) аутентификации зарегистрированного пользователя на основе учетных данных перед тем, как разрешить зарегистрированному пользователю использовать указанный первый пользовательский интерфейс (104) для инициирования платежной операции, где указанные учетные данные выбраны из группы, состоящей из идентификатора входа и пароля, предварительно установленного PIN-кода и биометрической подписи зарегистрированного пользователя, включая по меньшей мере один из следующих вариантов: отпечатки пальцев, лицевая биометрия, рисунок радужки глаза, рисунок сетчатки глаза, рисунок вен пальцев, рисунок вен ладони и образец голоса.

18. Способ (200) по п.12, который дополнительно включает в себя следующие этапы:

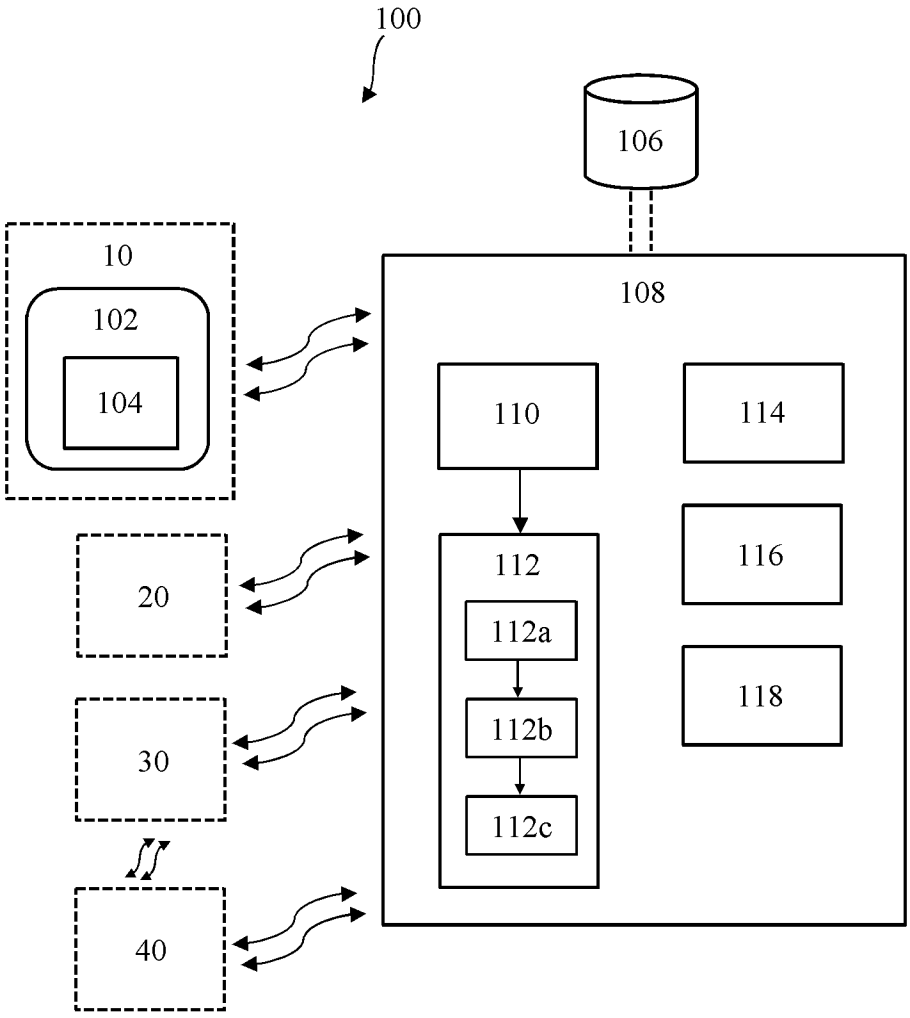
- получение банком-эмитентом (30) зарегистрированного пользователя указанных данных о транзакции;
- проверку банком-эмитентом (30) полученных данных о транзакции на основе предварительно сохраненных данных о клиенте;
- генерирование банком-эмитентом (30) первого одноразового пароля после проверки данных транзакции;
- отправку банком-эмитентом (30) сгенерированного первого одноразового пароля на электронное устройство (10) зарегистрированного пользователя банка для аутентификации пользователя;
- предоставление зарегистрированным пользователем банка платежному шлюзу данных для аутентификации;
- отправку платежным шлюзом полученного второго одноразового пароля в банк-эмитент (30); и
- сравнение банком-эмитентом (30) сгенерированного первого одноразового пароля со вторым одноразовым паролем, полученным от платежного шлюза, для аутентификации транзакции.

19. Способ (200) по п.17, который дополнительно включает в себя следующие этапы:

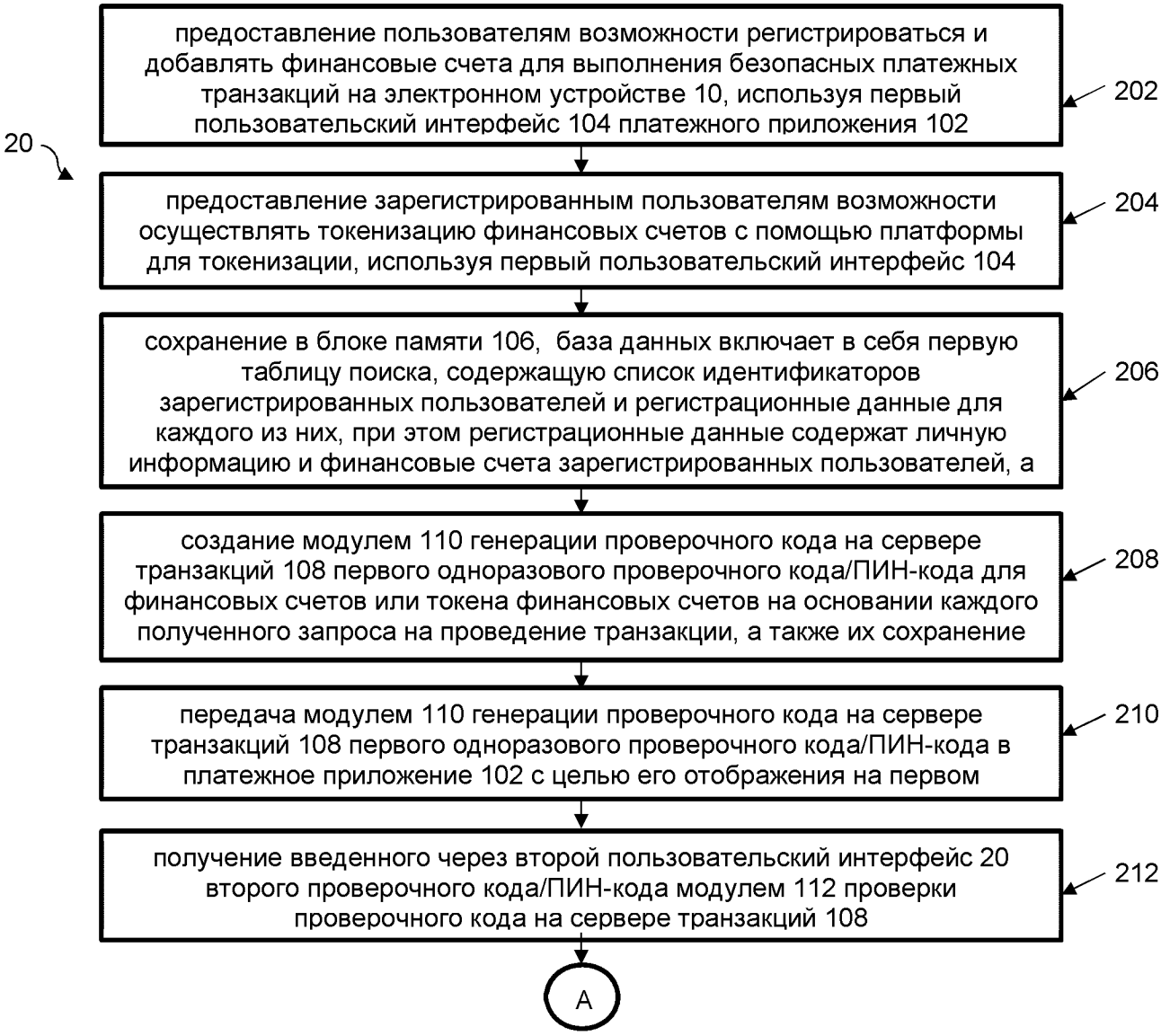
i. получение модулем уведомления (118), входящим в состав указанного сервера транзакций (108), сообщения о состоянии транзакции от платежного шлюза/банка-эквайера (40) второго зарегистрированного пользователя; и

ii. уведомление указанным модулем уведомления (118) зарегистрированного пользователя и второго зарегистрированного пользователя о статусе транзакции через, соответственно, первый пользовательский интерфейс (104) и второй пользовательский интерфейс (20).

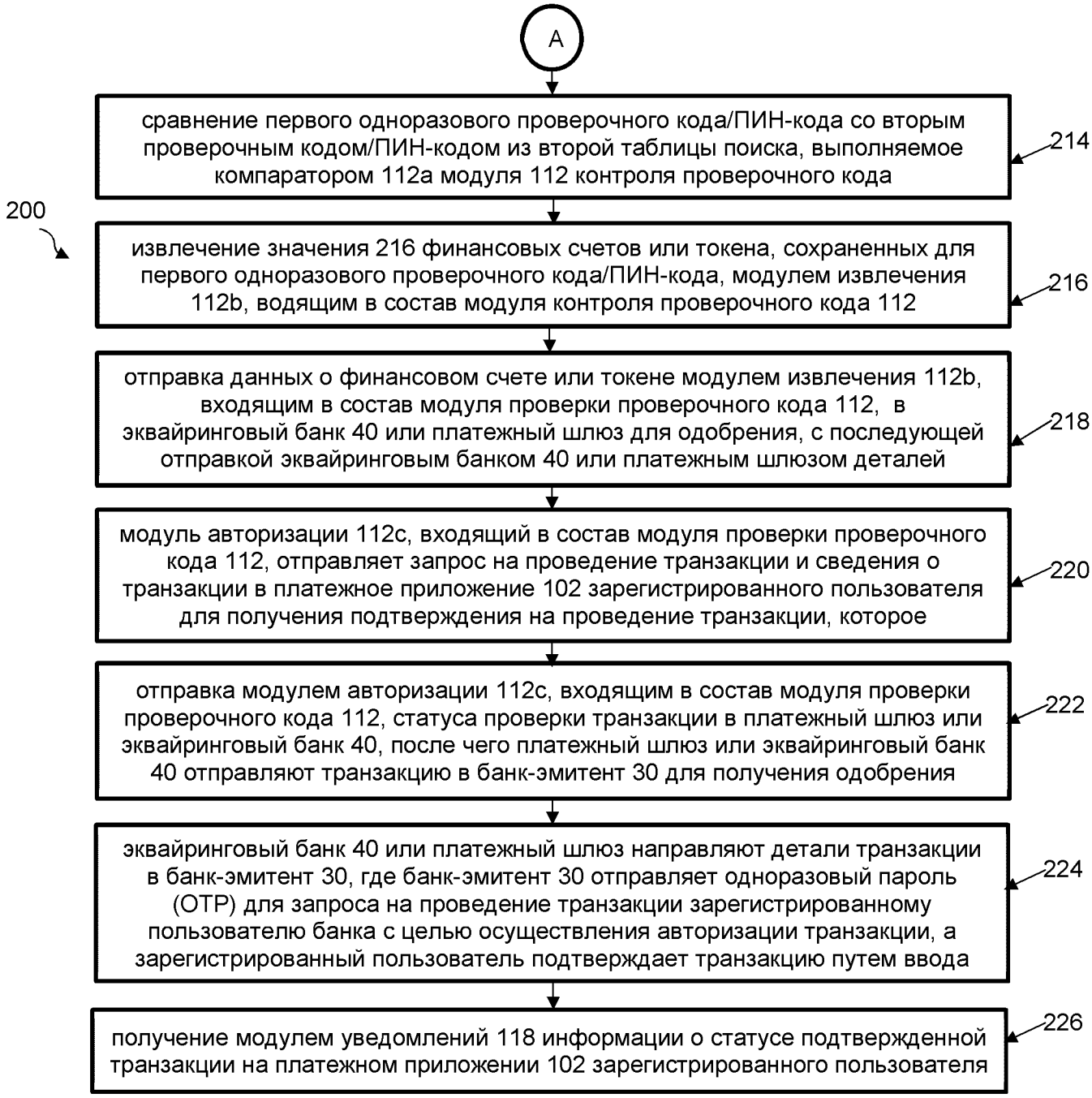
20. Способ (200) по п.12, в котором указанные данные о транзакции содержат по меньшей мере одно из идентификатора транзакции, финансового счета зарегистрированного пользователя, суммы транзакции и одних или более регистрационных данных второго зарегистрированного пользователя, с которым осуществляется платежная операция.


100
106
10
102
104
108
110
114
112
116
112a
118
112b
112c
20
30
40

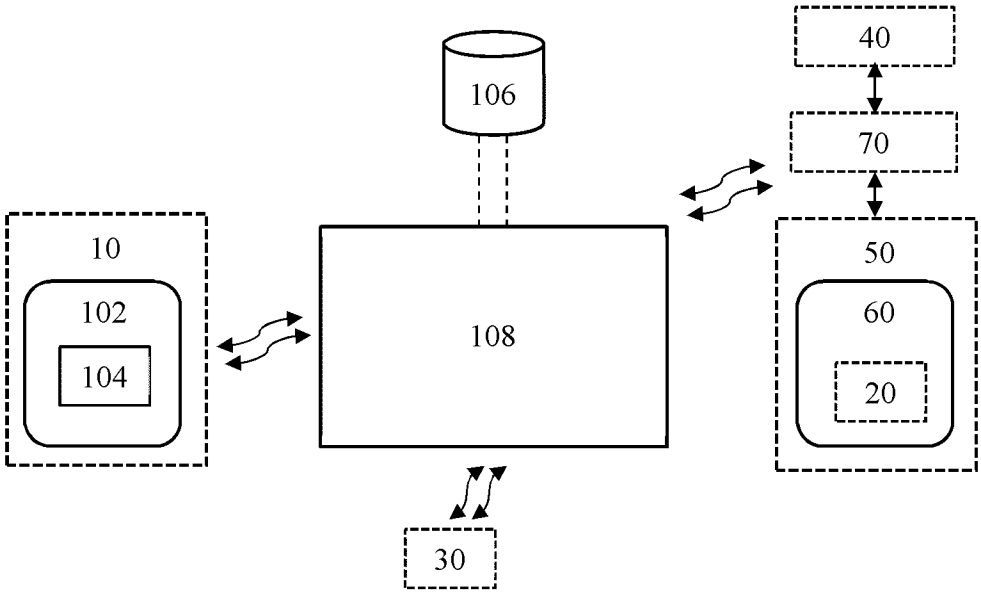
Фиг. 1


20
предоставление пользователям возможности регистрироваться и добавлять финансовые счета для выполнения безопасных платежных транзакций на электронном устройстве 10, используя первый пользовательский интерфейс 104 платежного приложения 102
202
предоставление зарегистрированным пользователям возможности осуществлять токенизацию финансовых счетов с помощью платформы для токенизации, используя первый пользовательский интерфейс 104
204
сохранение в блоке памяти 106, база данных включает в себя первую таблицу поиска, содержащую список идентификаторов зарегистрированных пользователей и регистрационные данные для каждого из них, при этом регистрационные данные содержат личную информацию и финансовые счета зарегистрированных пользователей, а
206
создание модулем 110 генерации проверочного кода на сервере транзакций 108 первого одноразового проверочного кода/ПИН-кода для финансовых счетов или токена финансовых счетов на основании каждого полученного запроса на проведение транзакции, а также их сохранение
208
передача модулем 110 генерации проверочного кода на сервере транзакций 108 первого одноразового проверочного кода/ПИН-кода в платежное приложение 102 с целью его отображения на первом
210
получение введенного через второй пользовательский интерфейс 20 второго проверочного кода/ПИН-кода модулем 112 проверки проверочного кода на сервере транзакций 108
212
A

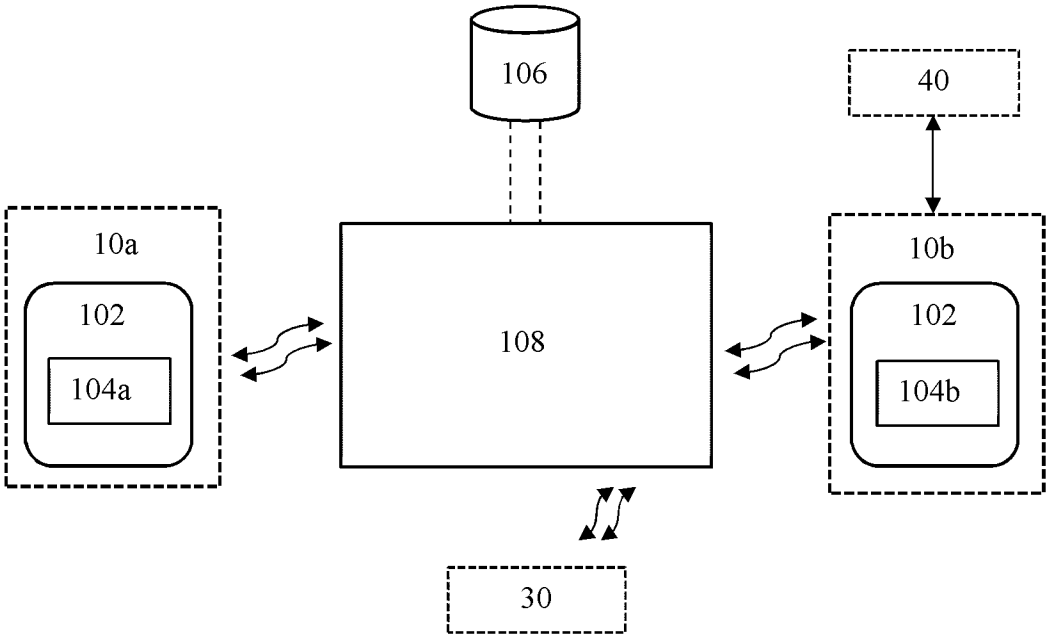
Фиг. 2A


A
сравнение первого одноразового проверочного кода/ПИН-кода со вторым проверочным кодом/ПИН-кодом из второй таблицы поиска, выполняемое компаратором 112a модуля 112 контроля проверочного кода
214
200
извлечение значения 216 финансовых счетов или токена, сохраненных для первого одноразового проверочного кода/ПИН-кода, модулем извлечения 112b, водящим в состав модуля контроля проверочного кода 112
216
отправка данных о финансовом счете или токене модулем извлечения 112b, входящим в состав модуля проверки проверочного кода 112, в эквайринговый банк 40 или платежный шлюз для одобрения, с последующей отправкой эквайринговым банком 40 или платежным шлюзом деталей
218
модуль авторизации 112c, входящий в состав модуля проверки проверочного кода 112, отправляет запрос на проведение транзакции и сведения о транзакции в платежное приложение 102 зарегистрированного пользователя для получения подтверждения на проведение транзакции, которое
220
отправка модулем авторизации 112c, входящим в состав модуля проверки проверочного кода 112, статуса проверки транзакции в платежный шлюз или эквайринговый банк 40, после чего платежный шлюз или эквайринговый банк 40 отправляют транзакцию в банк-эмитент 30 для получения одобрения
222
эквайринговый банк 40 или платежный шлюз направляют детали транзакции в банк-эмитент 30, где банк-эмитент 30 отправляет одноразовый пароль (OTP) для запроса на проведение транзакции зарегистрированному пользователю банка с целью осуществления авторизации транзакции, а зарегистрированный пользователь подтверждает транзакцию путем ввода
224
получение модулем уведомлений 118 информации о статусе подтвержденной транзакции на платежном приложении 102 зарегистрированного пользователя
226

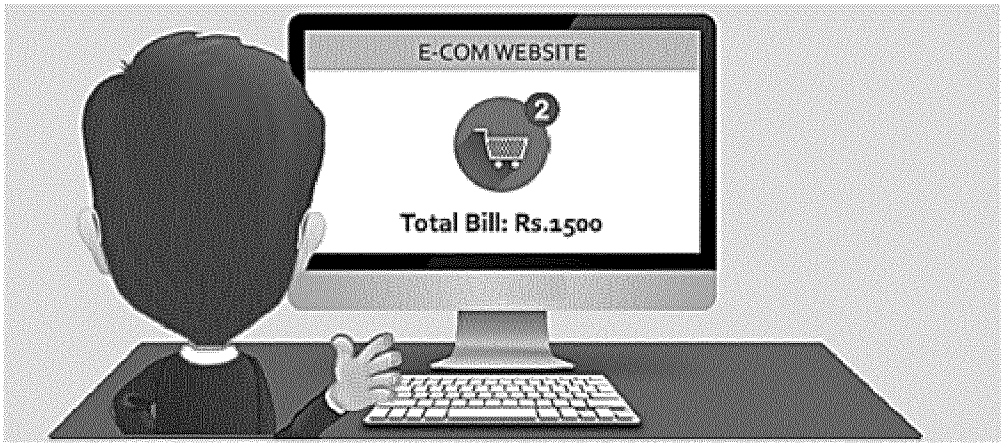
Фиг. 2B



Фиг. 3A

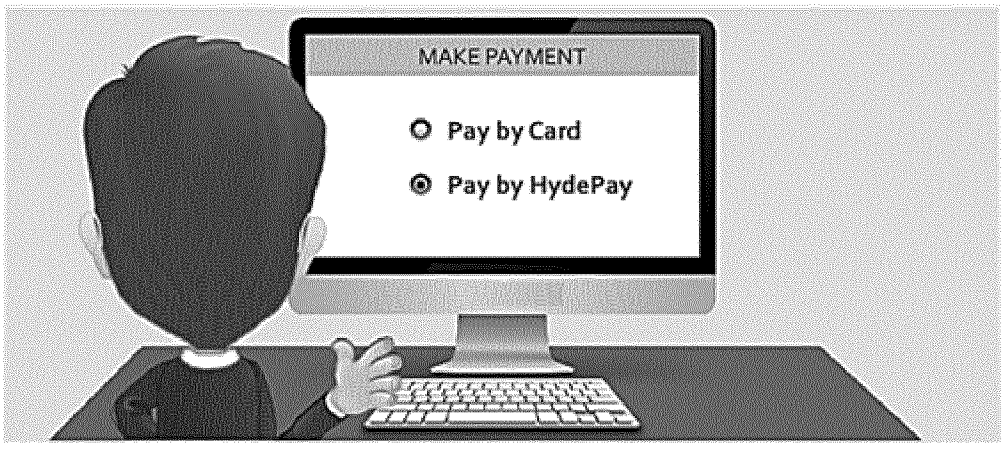


Фиг. 3B



Фиг. 4A

E-COM WEBSITE	ИНТЕРНЕТ-МАГАЗИН
Total Bill: Rs. 1500	Общая сумма счета: Rs.1500

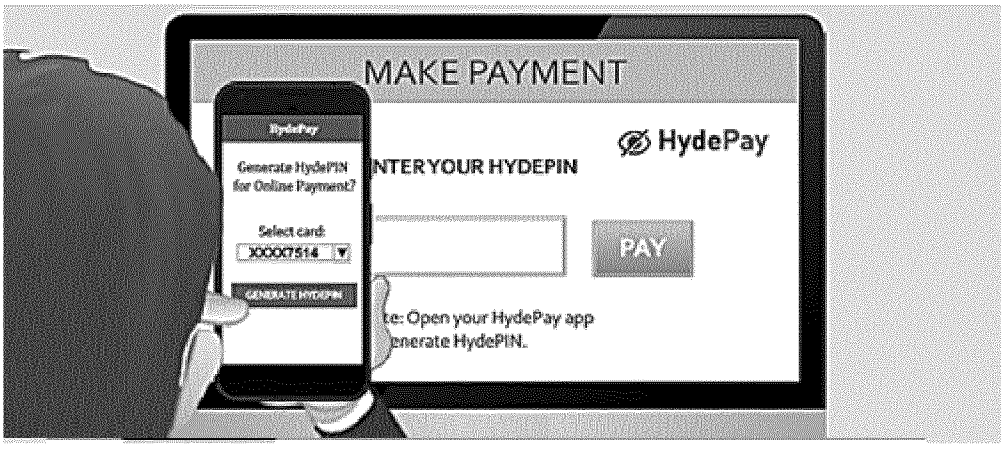


Фиг. 4B

MAKE PAYMENT	ПРОИЗВЕСТИ ОПЛАТУ
Pay by card	Заплатить картой
Pay by HydePay	Заплатить с помощью HydePay

Фиг. 4C

MAKE PAYMENT	ПРОИЗВЕСТИ ОПЛАТУ
HydePay	HydePay
ENTER YOUR HYDEPIN	ВВЕДИТЕ СВОЙ КОД HYDEPIN
PAY	ЗАПЛАТИТЬ
Note: Open your HydePay app to generate HydePIN.	Примечание: Чтобы сгенерировать код HydePIN, запустите приложение HydePay.

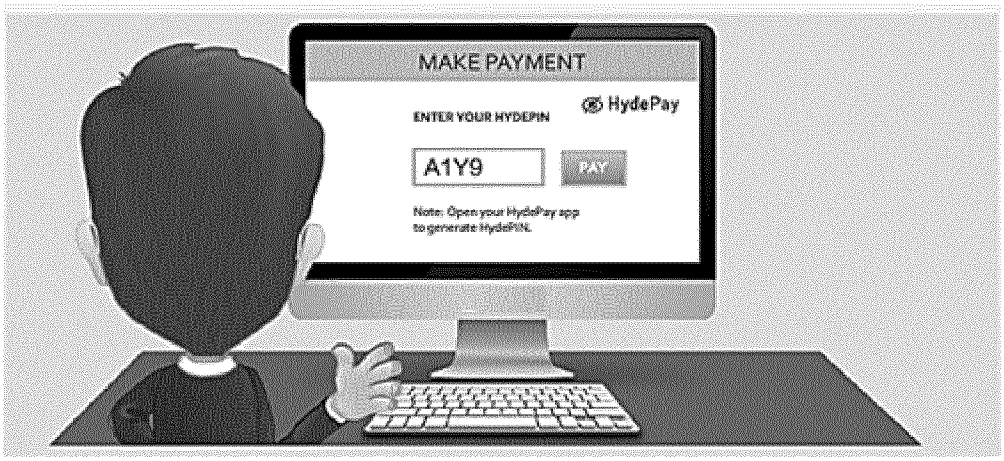


Фиг. 4D

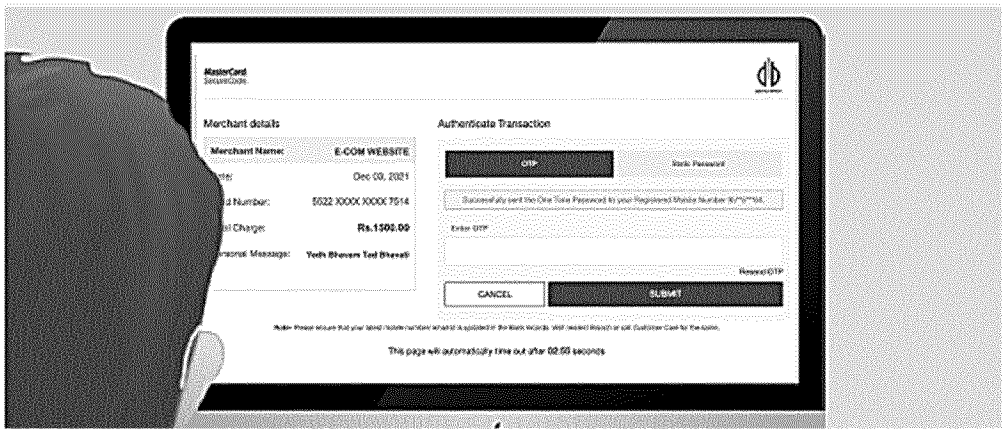
Generate HydePIN for Online Payment?	Сгенерировать код HydePIN для онлайн-платежа?
Select Card:	Выберите карту:
GENERATE HYDEPIN	СГЕНЕРИРОВАТЬ КОД HYDEPIN

Фиг. 4E

Your HydePIN for Online Payment is	Код HydePIN для онлайн-платежа:
For one time use only.	Для одноразового использования.

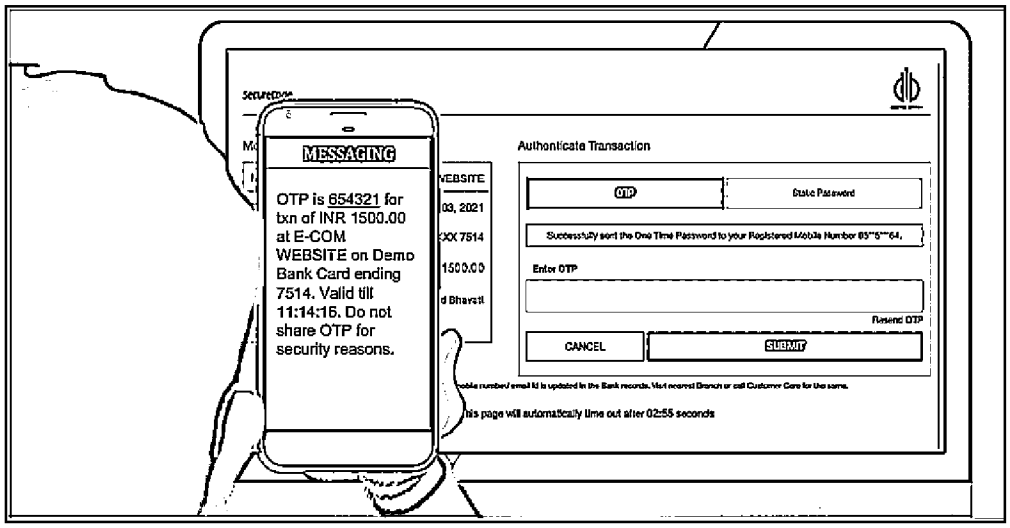


Фиг. 4F



Фиг. 4G

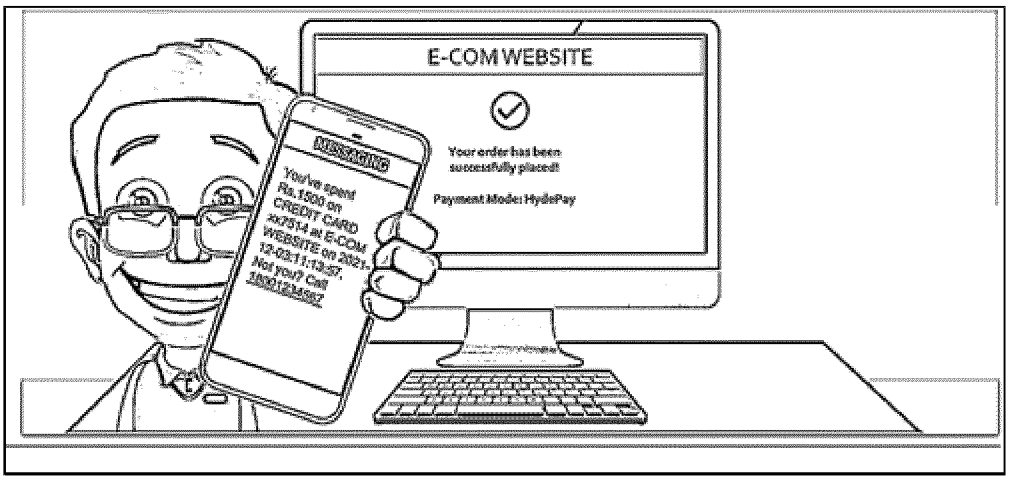
MasterCard	MasterCard
Security Code	Код безопасности
Merchant Details	Сведения о продавце
Authenticate Transaction	Подтвердить транзакцию
Merchant name	Название продавца
E-COM WEBSITE	ИНТЕРНЕТ-МАГАЗИН
Date:	Дата:
Dec 03, 2021	03 Дек. 2021
Card number:	Номер карты:
Total charge:	Общая сумма к оплате:
Rs. 1500.00	Рупий 1500,00
Personal Message:	Персональное сообщение:
Yedh Bhavam Tad Bhavati	Yedh Bhavam Tad Bhavati
OTP	Одноразовый пароль (OTP)
Static Password	Статический пароль
Successfully sent the One Time Password to your Registered Mobile Number 95**5***64	Одноразовый пароль отправлен на зарегистрированный номер мобильного телефона 95**5***64
Enter OTP	Введите одноразовый пароль (OTP)
Resend OTP	Отправить одноразовый пароль (OTP) еще раз
Cancel	Отмена
SUBMIT	ПОДТВЕРДИТЬ
Note: Please ensure that your latest mobile number / email Id is updated in the Bank records. Visit nearest Branch or call Customer Care for the same.	**Примечание**: Убедитесь, что в банковских данных указан актуальный номер мобильного телефона / адрес электронной почты. Чтобы решить этот вопрос, обратитесь в ближайшее отделение или позвоните в службу поддержки клиентов.
This page will automatically timeout after 02:55 seconds	Эта страница автоматически закроется через 2 минуты 55 секунд.



Фиг. 4H

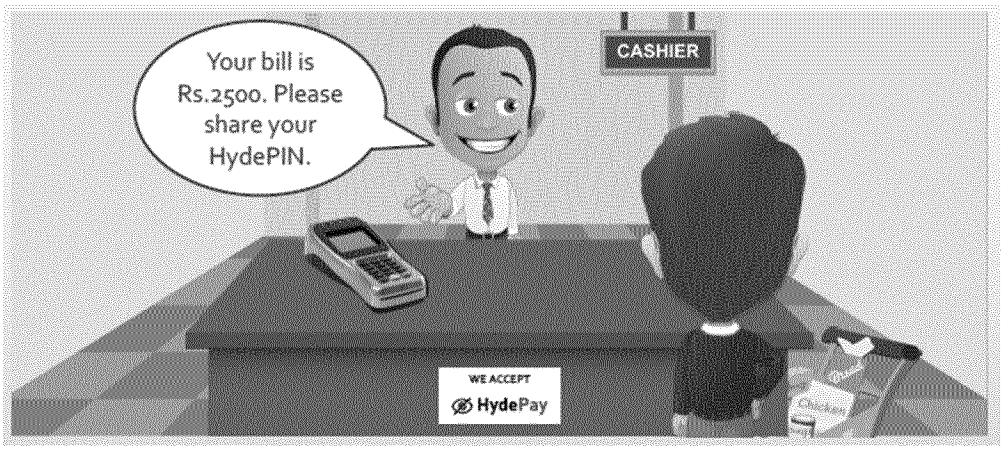
MESSAGING	СООБЩЕНИЕ
OTP is 654321 for txn of INR 1500.00 at E-COM WEBSITE on Issuer Bank Card xx7514. -Issuer Bank	Одноразовй пароль (OTP): 654321 для проведения транзакции на сумму 1500,00 рупий в ИНТЕРНЕТ-МАГАЗИНЕ с использованием карты эмитента xx7514. -Банк-эмитент

Фиг. 4I



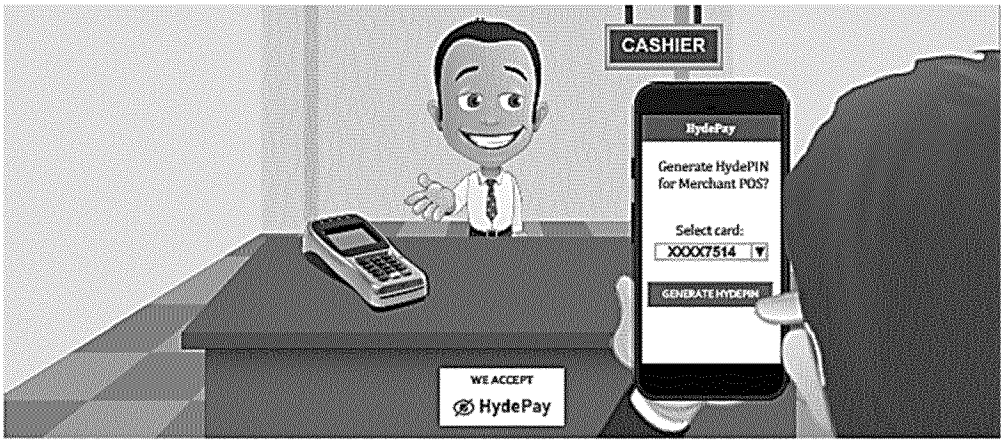
Фиг. 4J

E-COM WEBSITE	ИНТЕРНЕТ-МАГАЗИН
Your order has been successfully placed!	Ваш заказ принят!
Payment Mode: HydePay	Форма оплаты: HydePay
MESSAGING	СООБЩЕНИЕ
You've spent Rs.1500 on CREDIT CARD xx7514 at E-COM WEBSITE on 2021-12-03; 11:13:57. Not you? Call 18001234567	Вы потратили 1500 рупий, которые были списаны с кредитной карты xx7514 в ИНТЕРНЕТ-МАГАЗИНЕ 2021-12-03; 11:13:57. Это были не вы? Позвоните по номеру 18001234567



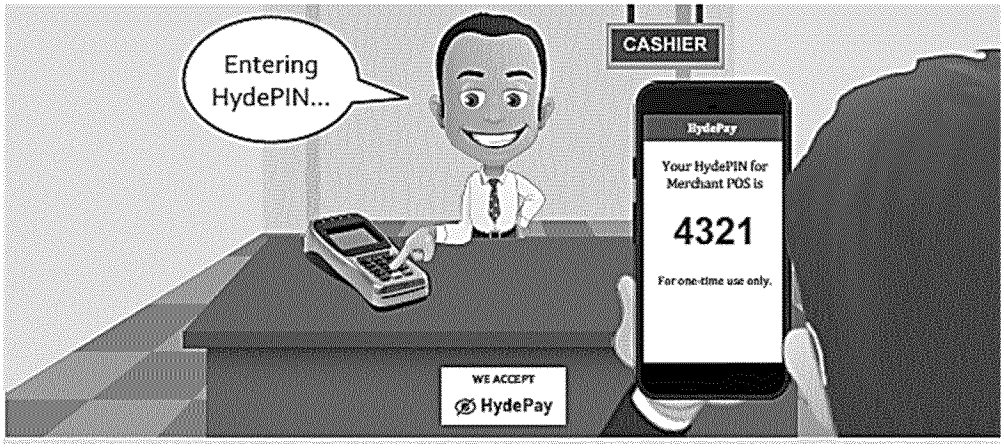
Фиг. 5A

CASHIER	КАССИР
Your bill is Rs.2500. Please share your HydePIN.	Сумма вашего счета: 2500 рупий. Укажите свой код HydePIN.
WE ACCEPT HydePay	МЫ ПРИНИМАЕМ HydePay



Фиг. 5B

Generate HydePIN for Merchant PS?	Сгенерировать код HydePIN для POS-терминала продавца?
Select card:	Выберите карту:
GENERATE HYDEPIN	СГЕНЕРИРОВАТЬ КОД HYDEPIN

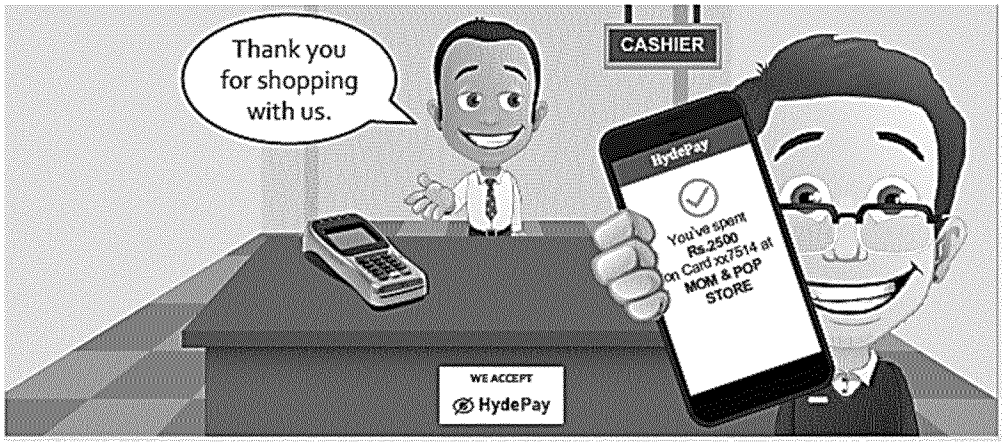


Фиг. 5C

Entering HydePIN...	Ввод кода HydePIN...
Your HydePIN for Merchant POS is	Ваш код HydePIN для POS-терминала продавца:
For one-time use only.	Для одноразового использования.

Фиг. 5D

You’ve received a request for payment of Rs.2500 from MOM & POP STORE	Вы получили запрос на проведение оплаты на сумму 2500 рупий от MOM & POP STORE
AUTHENTICATE	ПОДТВЕРДИТЬ

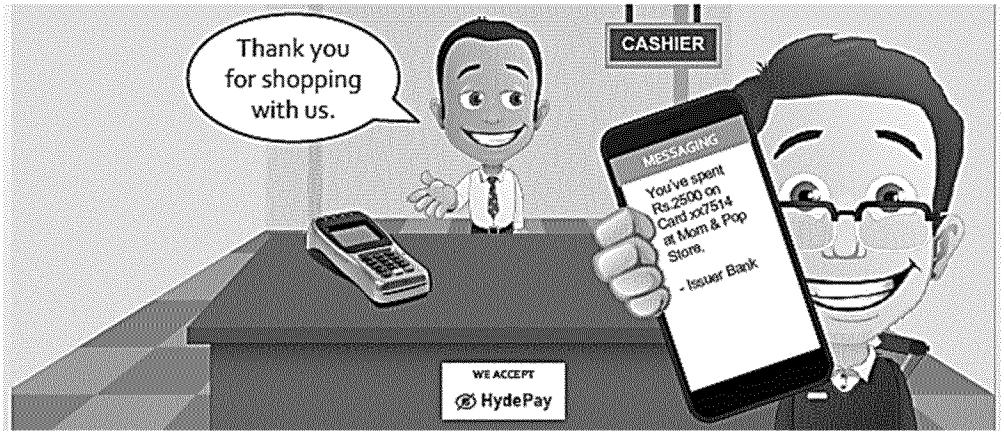


Фиг. 5E

Thank you for shopping with us.	Спасибо, что выбрали наш магазин.
You’ve spent Rs.2500 on Card xx7514 at MOM & POP STORE	Вы потратили 2500 рупий, которые были списаны с карты xx7514 в MOM & POP STORE

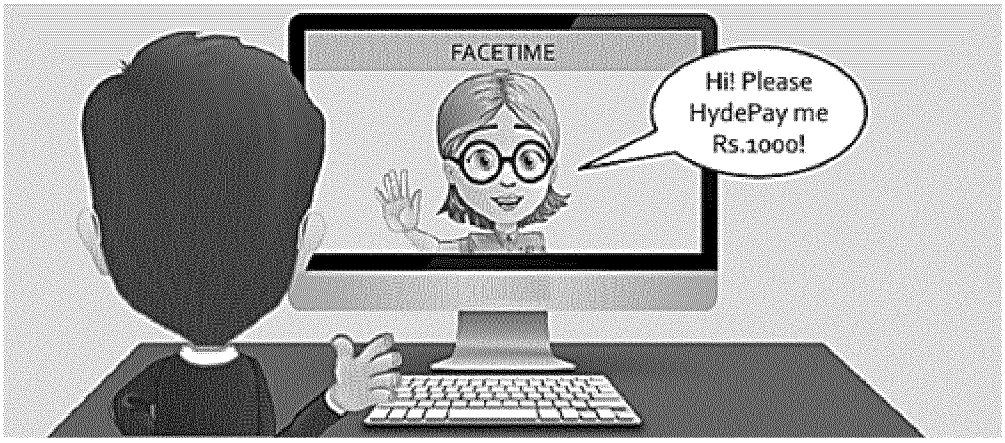
Фиг. 5F

Please enter OTP!	Введите одноразовый пароль (OTP)!



Фиг. 5G

Thank you for shopping with us.	Спасибо, что выбрали наш магазин.
MESSAGING	СООБЩЕНИЕ
You've spent Rs.2500 on Card xx7514 at Mom & Pop Store. - Issuer Bank	Вы потратили 2500 рупий, которые были списаны с карты xx7514 в Mom & Pop Store. -Банк-эмитент

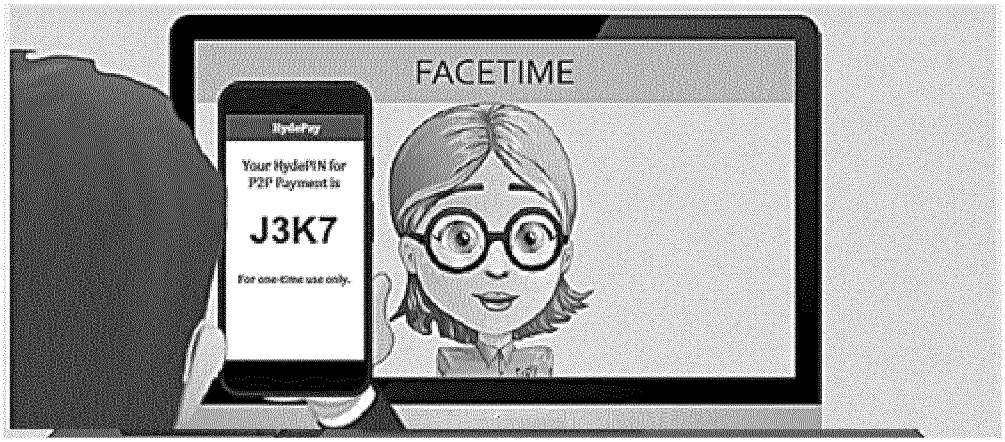


Фиг. 6A

FACETIME	FACETIME
Hi! Please HydePay me Rs.1000!	Привет! Отправь мне 1000 рупий через HydePay!

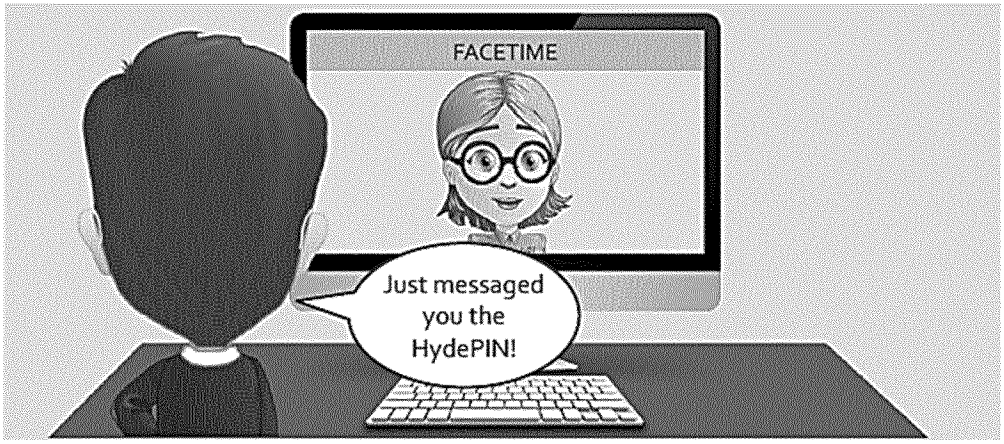
Фиг. 6B

Generate HydePIN for P2P Payment?	Сгенерировать код HydePIN для перевода P2P между пользователями?



Фиг. 6C

Your HydePIN for P2P Payment is For one time use only.	Код HydePIN для перевода P2P между пользователями: Только для одноразового использования.



Фиг. 6D

Just messaged you the HydePIN!	Я отправил тебе код HydePIN!

Фиг. 6E

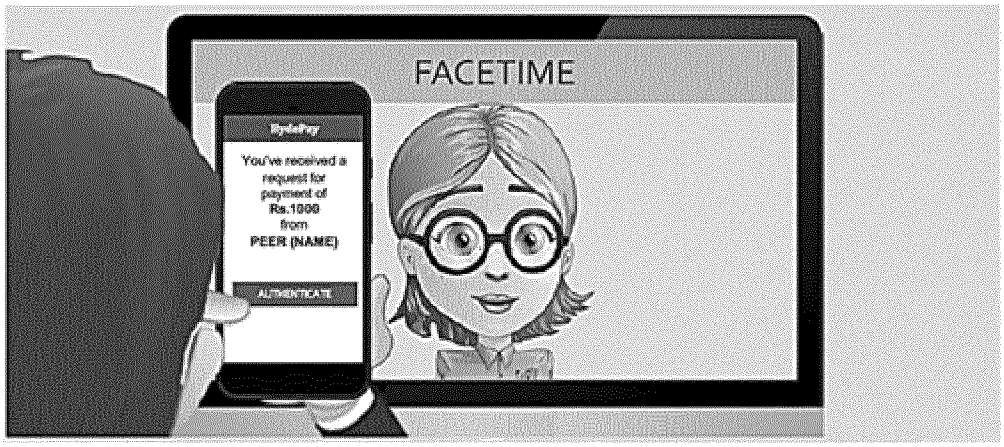
Request Money	Запрос на перевод денег
HydePin:	Код HydePin:
Amount (Rs):	Сумма (Рупий):
REQUEST	ЗАПРОС

Фиг. 6F

You've received a request for payment of Rs.1000 from PEER (NAME)	Вы получили запрос на проведение оплаты на сумму 1000 рупий от ПОЛЬЗОВАТЕЛЯ (ИМЯ)
AUTHENTICATE	ПОДТВЕРДИТЬ

Фиг. 6G

MESSAGING	СООБЩЕНИЕ
OTP is 456789 for txn of INR 1000.00 on HydePay app on Issuer Bank Card xx7514. - Issuer Bank	Одноразовй пароль (OTP): 456789 для проведения транзакции на сумму 1000,00 рупий в приложении HydePay с использованием карты эмитента xx7514. -Банк-эмитент



Фиг. 6H

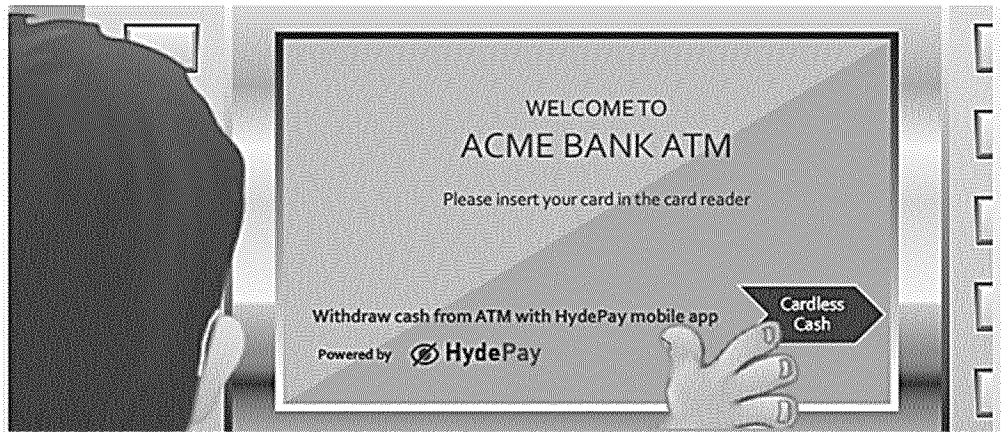
You've received a request for payment of Rs.1000 from PEER (NAME)	Вы получили запрос на проведение оплаты на сумму 1000 рупий от ПОЛЬЗОВАТЕЛЯ (ИМЯ)
AUTHENTICATE	ПОДТВЕРДИТЬ

Фиг. 6I

MasterCard	MasterCard
SecureCode	Код безопасности
Merchant details	Сведения о продавце
Authenticate Transaction	Подтвердить транзакцию
Merchant name	Название продавца
OTP	Одноразовый пароль (OTP)
Static Password	Статический пароль
Successfully sent the One Time Password to your Registered Mobile Number 95**5***64	Одноразовый пароль отправлен на зарегистрированный номер мобильного телефона 95**5***64
Enter OTP	Введите одноразовый пароль (OTP)
Resend OTP	Отправить одноразовый пароль (OTP) еще раз
SUBMIT	ПОДТВЕРДИТЬ
Note: Please ensure that your latest mobile number / email Id is updated in the Bank records. Visit nearest Branch or call Customer Care for the same.	**Примечание**: Убедитесь, что в банковских данных указан актуальный номер мобильного телефона / адрес электронной почты. Чтобы решить этот вопрос, обратитесь в ближайшее отделение или позвоните в службу поддержки клиентов.

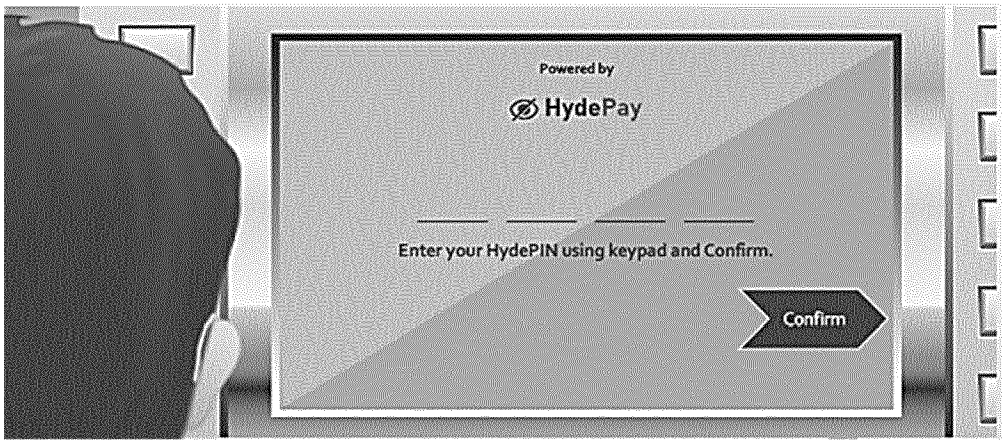
Фиг. 6J

You’ve sent Rs.1000 using Card xx7514 to PEER (NAME)	Вы отправили 1000 Рупий с использованием карты xx7514 ПОЛЬЗОВАТЕЛЮ (ИМЯ)
You’ve received Rs.1000 from CUSTOMER (NAME)	Вы получили 1000 Рупий от КЛИЕНТА (ИМЯ)



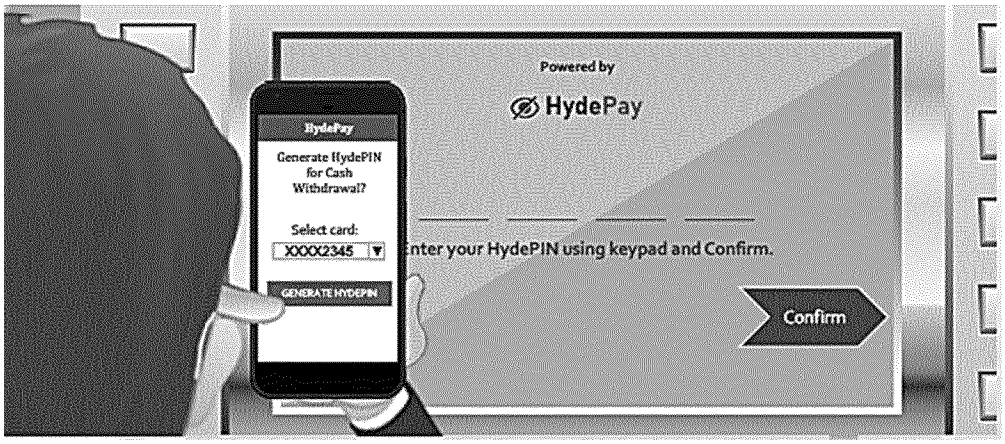
Фиг. 7A

WELCOME TO ACME BANK ATM	ДОБРО ПОЖАЛОВАТЬ В БАНКОМАТ ACME BANK
Please insert your card in the card reader	Вставьте свою карту в устройство для считывания карт
Withdraw cash from ATM with HydePay mobile app	Используйте мобильное приложение HydePay для снятия наличных с банкомата
Cardless Cash	Снятие наличных без карты
Powered by HydePay	Поддерживается HydePay



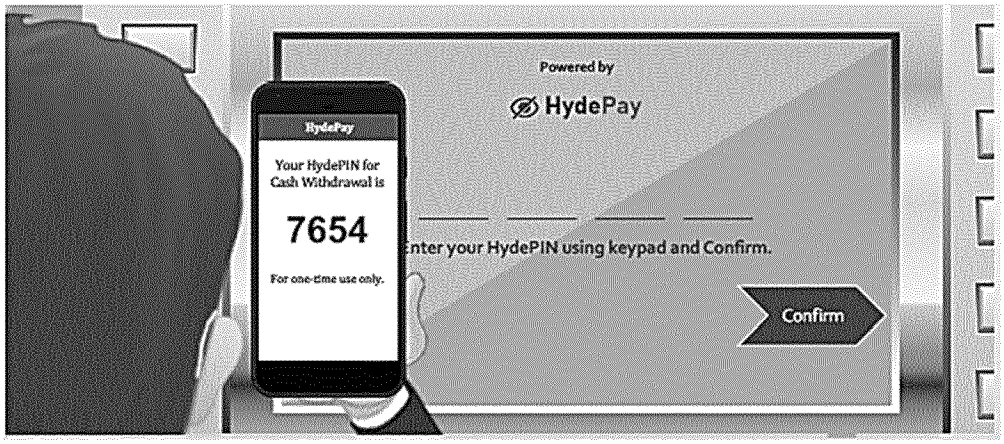
Фиг. 7B

Powered by HydePay	Поддерживается HydePay
Enter your HydePIN using keypad and Confirm.	Введите код HydePIN с помощью клавиатуры и нажмите кнопку Подтвердить.
Confirm	Подтвердить



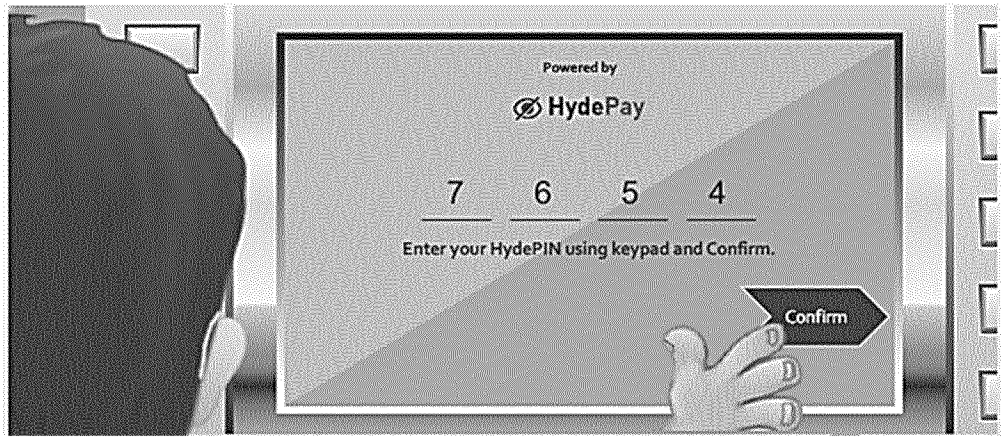
Фиг. 7C

Generate HydePIN for Cash Withdrawal?	Сгенерировать код HydePIN для снятия наличных?
Select card:	Выберите карту:
GENERATE HYDEPIN	СГЕНЕРИРОВАТЬ КОД HYDEPIN

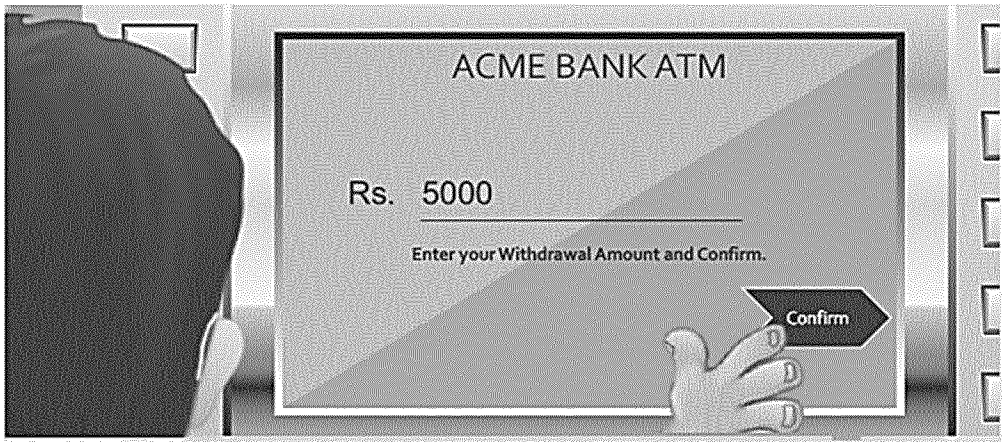


Фиг. 7D

Your HydePIN for Cash Withdrawal is	Код HydePIN для снятия наличных:

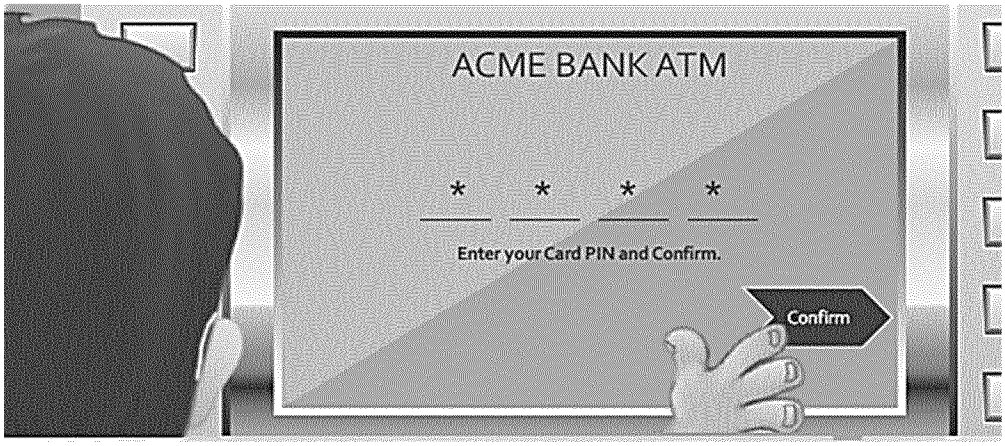


Фиг. 7E



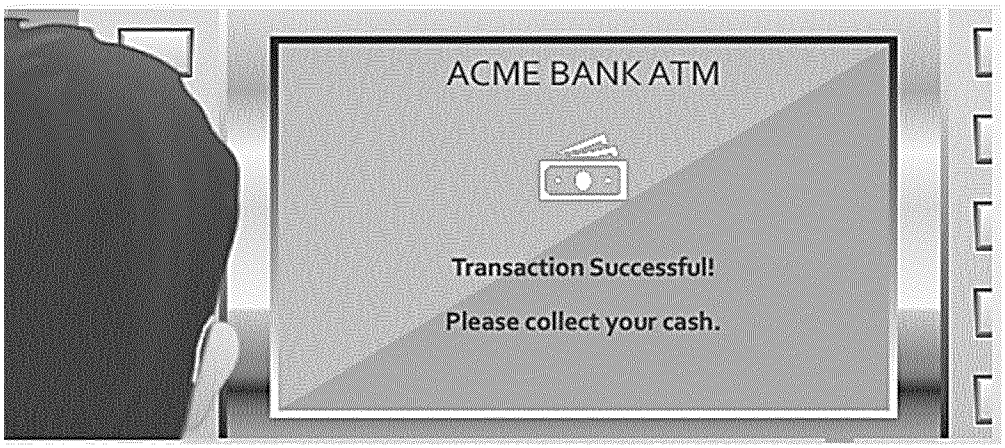
Фиг. 7F

ACME BANK ATM	БАНКОМАТ ACME BANK
Rs. 5000	Рупий 5000
Enter your withdrawal Amount and Confirm	Введите сумму для снятия и нажмите кнопку Подтвердить



Фиг. 7G

Enter your Card PIN and Confirm	Введите PIN-код карты и нажмите кнопку Подтвердить



Фиг. 7H

Transaction Successful!	Транзакция проведена!
Please collect your cash.	Получите деньги.