**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

**УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ**

**ГОМЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ П. О. СУХОГО**

Факультет автоматизированных и информационных систем

Кафедра «Информатика»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 5

по дисциплине «ОЗИ»

на тему: «**Патентный поиск**»

Выполнил: студент гр. ИП-32

Суховенко Э.С.

Принял: профессор

Кудин В.П.

Гомель 2022

**Задание:**

1. Выбрать объект промышленной собственности, имеющий непосредственное отношение к вычислительной технике и программированию, а также к защите информации (системы обработки данных в различных отраслях, компьютерные системы, обработка или генерация данных, секретная связь, устройства для секретной или скрытой связи и т.д.)

2.Для выбранного объекта по вышеописанной методике найти 4–5 релевантных патентных документов и предоставить их исчерпывающие описания в отчёте о проведенном поиске.

**Описание патентов:**

# Патент 1:

# Cпособ аутентификации владельца банковского счета при дистанционном банковском обслуживании

# 

Изобретение относится к способу аутентификации владельца банковского счета при дистанционном банковском обслуживании. Техническим результатом является повышение надежности результатов аутентификации владельца банковского счета. Способ аутентификации владельца банковского счета при дистанционном банковском обслуживании с использованием биометрических характеристик лица владельца банковского счета характеризуется тем, что при открытии банковского счета и/или выпуске банковской карты производится фотографическое изображение лица владельца счета, и тем, что оно вносится в электронном виде в базу данных банка и в память банковской карты, и при проведении операции по счету с помощью компьютера, мобильного телефона, банкомата, кассового терминала изображение лица человека, осуществляющего операцию посредством веб-камеры, оптического сканера, установленных на применяемом техническом средстве, передается в базу данных банка, при этом компьютер банка сверяет полученное изображение с изображением, хранящимся в базе данных банка, и в случае тождественности изображений дает разрешение на проведение операции, или в случае несоответствия изображений отказывает в проведении операции, и при наличии инструкции банка-эмитента карты карта блокируется банкоматом.

# Формула изобретения

# Способ аутентификации владельца банковского счета при дистанционном банковском обслуживании с использованием биометрических характеристик лица владельца банковского счета, характеризующийся тем, что при открытии банковского счета и/или выпуске банковской карты производится фотографическое изображение лица владельца счета, и отличающийся тем, что оно вносится в электронном виде в базу данных банка и в память банковской карты, и при проведении операции по счету с помощью компьютера, мобильного телефона, банкомата, кассового терминала изображение лица человека, осуществляющего операцию посредством веб-камеры, оптического сканера, установленных на применяемом техническом средстве, передается в базу данных банка, при этом компьютер банка сверяет полученное изображение с изображением, хранящимся в базе данных банка, и в случае тождественности изображений дает разрешение на проведение операции, или в случае несоответствия изображений отказывает в проведении операции, и при наличии инструкции банка-эмитента карты карта блокируется банкоматом.

## **Описание изобретения к патенту**

Изобретение относится к способам аутентификации владельца банковского счета при осуществлении операций по счету с использованием различных видов дистанционного банковского обслуживания, а именно интернет-банкинга, мобильного банкинга, использовании банкоматов, платежах в торговых точках с помощью банковских карт и т.п. Областью применения настоящего изобретения является предотвращение многочисленных случаев мошеннических действий при осуществлении операций по счету с использованием различных видов дистанционного банковского обслуживания.

Применяемые в настоящее время при дистанционном банковском обслуживании способы аутентификации владельца банковского счета, а именно персональные идентификационные коды, телефонные персональные идентификационные коды, логины, СМС-пароли и т.п., не дают полной гарантии того, что все эти данные переданы в базу данных банка именно владельцем банковского счета, а не похитившим их мошенником.

Наиболее близким аналогом заявленного изобретения является заявка US2005/0224573 А1, опубликованная 13.10.2005, из которой известен способ аутентификации владельца банковского счета при дистанционном банковском обслуживании с использованием биометрических характеристик лица владельца банковского счета. При открытии банковского счета и/или выпуске банковской карты фотографическое изображение лица владельца счета вносится в электронном виде в базу данных банка и печатается на лицевой стороне банковской карты.

Однако указанный аналог имеет ряд существенных отличий по сравнению с заявленным изобретением:

- аналог предусматривает применение описываемого способа аутентификации для проведения операций только при использовании банкоматов, установленных только в офисах банка-владельца банкоматов, и только внутри системы одного банка.

Заявленное изобретение предусматривает применение описываемого способа аутентификации для проведения операций не только при использовании банкоматов без ограничения места их установки и не только внутри системы одного, но и различных банков, но и для проведения операций с использованием иных технических средств - компьютера, мобильного телефона, кассового терминала.

В результате решение, предлагаемое заявленным изобретением, значительно расширяет область применения способа и качественно (через банкоматы различных банков, установленные в любом подходящем для этих целей помещении), и количественно (с применением других технических средств);

- аналог предусматривает, что фотографическое изображение лица владельца счета вносится в базу данных банка и печатается на лицевой стороне банковской карты.

Заявленное изобретение предусматривает, что фотографическое изображение лица владельца счета вносится в базу данных банка и в электронном виде вносится в память банковской карты.

В результате решение, предлагаемое заявленным изобретением, повышает степень безопасности применения способа аутентификации, т.к. теоретически возможно наклеить на карту изображение реального владельца счета;

- аналог предусматривает следующий алгоритм аутентификации: при попытке проведения операции через банкомат изображение лица клиента, полученное камерой банкомата, и считываемые банкоматом с карты номер счета клиента и номер отделения банка, в котором он открыт, передаются на банковский сервер. Сервер по номеру счета и номеру отделения банка находит в базе данных банка хранящуюся там информацию о лице клиента и передает ее в банкомат. Банкомат сравнивает информацию, полученную из базы данных банка, с изображением лица клиента, полученным камерой банкомата, и по результатам сравнения принимает решение о проведении или об отказе в проведении операции.

Заявленное изобретение предусматривает следующий алгоритм аутентификации: при попытке проведения операции через одно из технических средств - банкомат, компьютер, мобильный телефон, кассовый терминал, изображение лица клиента, полученное оптико-электронным устройством видеонаблюдения (веб-камера, оптический сканер), установленным на этом техническом средстве, и введенные для проведения операции персональные данные клиента передаются в базу данных банка, и банковский сервер аутентификации по биометрическим характеристикам лица сравнивает полученные изображение и информацию с изображением и информацией, хранящимися в базе данных банка, и по результатам сравнения принимает решение о проведении или об отказе в проведении операции.

В результате решение, предлагаемое заявленным изобретением, существенно отличается от аналога тем, что аутентификацию владельца счета производит и принимает соответствующее решение о проведении или об отказе в проведении операции не банкомат, а банковский сервер, что, во-первых, значительно удешевляет стоимость применения способа, т.к. установка на каждом банкомате устройств, осуществляющих аутентификацию владельца счета по биометрическим характеристикам лица, технически сложна и весьма дорогостояща; во-вторых, оно снижает риски постороннего вмешательства в работу многочисленных технических средств, расположенных в местах относительно легко доступных, по сравнению с банковским сервером, для злоумышленников;

- аналог предусматривает, в случае отказа банкомата в проведении операции, участие в процессе аутентификации банковского служащего. На управленческий терминал, расположенный в офисе банка, передается полученная информация, и банковский служащий, проведя визуальную проверку лица человека, пытающегося провести операцию, принимает решение о проведении или об отказе в проведении операции.

Заявленное изобретение участия в процессе аутентификации человека (банковского служащего) не предусматривает.

В результате решение, предлагаемое заявленным изобретением, принимая во внимание высокую степень вероятности ошибки (так называемый «человеческий фактор»), а также значительное увеличение временных и материальных затрат на подобный рискованный метод аутентификации, является значительно более безопасным (исключающим «человеческий фактор») и экономичным (отсутствие затрат на дополнительные функции персонала);

- аналог не предусматривает блокировку банкоматом карты в случае отказа банкомата в проведении операции.

Заявленное изобретение в случае отказа банкомата в проведении операции, при наличии инструкции банка-эмитента карты, предусматривает блокировку карты банкоматом.

В результате решение, предлагаемое заявленным изобретением, является значительно более технологически совершенным, так как позволяет при попытке использования злоумышленником похищенной карты «отобрать» её у него при первой же попытке использования и сохранить в базе данных изображение лица злоумышленника, что существенно облегчит работу правоохранительных органов по его розыску.

Техническим результатом применения заявленного изобретения является достижение максимальной степени надежности результатов аутентификации владельца банковского счета и исключение из процесса аутентификации участия банковских служащих.

Технический результат достигается за счет способа аутентификации владельца банковского счета при дистанционном банковском обслуживании с использованием биометрических характеристик лица владельца банковского счета. При открытии банковского счета и/или выпуске банковской карты фотографическое изображение лица владельца счета вносится в электронном виде в базу данных банка и в память банковской карты. Изображение лица человека, осуществляющего операцию по счету с помощью компьютера, мобильного телефона, банкомата, кассового терминала, посредством веб-камеры, оптического сканера, установленных на применяемом техническом средстве, передается в базу данных банка. Компьютер банка сверяет полученное изображение с изображением, хранящимся в базе данных банка, и в случае тождественности изображений дает разрешение на проведение операции или в случае несоответствия изображений отказывает в проведении операции, и при наличии инструкции банка-эмитента карты карта блокируется банкоматом.

Сущность изобретения состоит в том, что все используемые способы аутентификации дополняются способом, которым не смогут воспользоваться мошенники, а именно аутентификацией по биометрическим характеристикам лица владельца банковского счета. Применение изобретения позволит, если не полностью предотвратить, то существенно сократить многочисленные случаи мошеннических действий при осуществлении операций по счету с использованием различных видов дистанционного банковского обслуживания.

При открытии банковского счета (и/или выпуске банковской карты) фотографическое изображение лица владельца счета в электронном виде вносится в базу данных банка и в память банковской карты и становится, наряду с вышеперечисленными способами аутентификации, одним из кодов доступа («ключей») к системе управления банковским счетом.

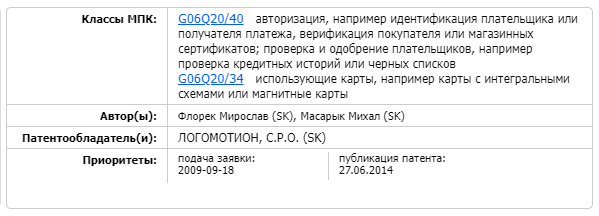
При осуществлении операций по счету в интернет-банкинге, мобильном банкинге, платежах через интернет банковской картой и т.п. оптико-электронное устройство видеонаблюдения (веб-камера, оптический сканер и т.п.), установленное в компьютере, мобильном телефоне или ином техническом средстве, с помощью которого производится попытка осуществить операцию, передает изображение лица человека, осуществляющего операцию, в базу данных банка. Компьютер банка сверяет полученное изображение лица с изображением лица владельца счета, хранящимся в базе данных банка, и в случае тождественности изображений дает разрешение на проведение операции по счету или в случае несоответствия изображений отказывает в проведении операции.

При платежах банковской картой в торговой точке на экране считывающего банковскую карту устройства появляется изображение лица владельца банковского счета, с которого осуществляются платежи по карте, и кассир (оператор и т.п.), сверив его с лицом клиента, предъявившего карту к оплате, в случае их несоответствия отказывает в проведении платежа. Во избежание влияния на проведение вышеописанной операции субъективного фактора (зрение кассира, его настроение и т.п.) возможна установка на кассовом терминале одного из оптико-электронных устройств. В этом случае последовательность действий аналогична указанной в предыдущем абзаце.

При осуществлении операций по счету с помощью банкомата установленные на нем веб-камера или оптический сканер передает изображение лица человека, осуществляющего операцию, в базу данных банка. Компьютер банка сверяет полученное изображение лица с изображением лица владельца счета, хранящимся в базе данных банка, и в случае тождественности изображений дает разрешение на проведение операции или в случае несоответствия изображений отказывает в проведении операции, и при наличии инструкции банка-эмитента карты карта блокируется банкоматом.

**Патент 2:**

**Система и способ бесконтактной авторизации платежа**

****

Изобретение относится к средствам бесконтактных электронных платежей. Техническим результатом является повышение безопасности при проведении электронных платежей. Система состоит из платежного терминала, защищенного элемента, устройства мобильной связи с дисплеем и клавиатурой, такого как мобильный телефон. Устройство мобильной связи оснащено съемной картой памяти, на которой расположено не менее двух физически разделенных защищенных элемента. Устройство мобильной связи подключено к платежному терминалу посредством канала беспроводной передачи данных, и как минимум один защищенный элемент на съемной карте памяти содержит блок данных платежной карты. Карта памяти включает НДЧ-элемент. Система также может включать отдельный носитель для ввода ПИН-кода. Носитель питается энергией из принимаемого электромагнитного поля. Блок управления в устройстве мобильной связи используется для активации необходимого защищенного элемента, соответствующего выбранному блоку с данными о платежной карте на карте памяти. Устройство мобильной связи сообщается с платежным терминалом посредством канала беспроводной связи. 2 н. и 8 з.п. ф-лы, 1 ил.

**Формула изобретения**

1. Система бесконтактной авторизации платежа, содержащая устройство мобильной связи с клавиатурой, дисплеем и печатной платой с защищенным элементом виртуального платежного терминала и приложением для осуществления бесконтактных платежей с блоком шифрования, а также имеющее подключенную посредством контактов к печатной плате карту памяти, включающую элемент беспроводного канала связи и, по меньшей мере, два независимых защищенных элемента виртуального платежного терминала, один из которых представляет собой модуль создания одноразового пароля, а остальные - модули, содержащие информацию о платежных картах пользователя, и блок управления для активации на карте памяти защищенного элемента, соответствующего платежной карте, выбранной пользователем, причем устройство мобильной связи выполнено с возможностью подключения виртуального платежного терминала к связанному с сервером обработки платежей стационарному платежному терминалу посредством элемента беспроводного канала связи, размещенного на карте памяти с возможностью приема-передачи одноразового пароля, шифровального ключа и зашифрованного ПИН-кода выбранной платежной карты пользователя.

2. Система по п.1, отличающаяся тем, что она снабжена автономным носителем для бесконтактного ввода ПИН-кода в платежный терминал, включающим модуль хранения ПИН-кода, шифровальный модуль и модуль беспроводного канала связи для подключения этого носителя к платежному терминалу и/или к устройству мобильной связи.

3. Система по п.2, отличающаяся тем, что носитель выполнен с возможностью снабжения электроэнергией из принимаемого им электромагнитного поля.

4. Система по любому из пп.1-3, отличающаяся тем, что клавиатура снабжена специальной кнопкой запуска приложения для осуществления бесконтактных платежей, отмеченной символом валюты.

5. Система по любому из пп.1-3, отличающаяся тем, что виртуальный платежный терминала выполнен с блоком временного хранения данных.

6. Система по любому из пп.1-3, отличающаяся тем, что элемент беспроводного канала связи снабжен преобразователем частот и антенной с возможностью снабжения электроэнергией из принимаемого антенной электромагнитного поля.

7. Система по любому из пп.1-3, отличающаяся тем, что съемная карта памяти выполнена в формате microSD.

8. Способ авторизации платежа при совершении бесконтактной платежной операции, при котором пользователь соответствующими кнопками на клавиатуре средства мобильной связи активизирует виртуальный платежный терминал на печатной плате средства мобильной связи и с помощью блока управления выбирает в меню платежную карту, с которой будет осуществляться платеж, и затем подносит устройство мобильной связи к бесконтактному NFC-элементу беспроводного канала связи на стационарном платежном терминале, который устанавливает связь с элементом беспроводного канала связи, размещенным на карте памяти средства мобильной связи, принимает сведения о выбранной платежной карте и направляет запрос на авторизацию платежа на удаленный сервер обработки платежей для обработки запроса, при которой он проходит проверку на шифровальном модуле на подлинность приложения, с последующим формированием запроса на доступ к базе данных финансового учреждения, причем блок управления активирует соответствующий выбранной платежной карте защищенный элемент на карте памяти и обеспечивает подключение виртуального платежного терминала к связанному с сервером обработки платежей стационарному платежному терминалу посредством элемента беспроводного канала, размещенного на карте памяти с возможностью приема-передачи одноразового пароля, шифровального ключа и зашифрованного ПИН-кода выбранной платежной карты пользователя.

9. Способ по п.8, отличающийся тем, что ПИН-код непосредственно вводится в стационарный платежный терминал с клавиатуры последнего.

10. Способ по п.8, отличающийся тем, что ПИН-код вводится с помощью автономного носителя для бесконтактного ввода ПИН-кода в платежный терминал, при этом стационарный платежный терминал генерирует публичный ключ, отправляет его с помощью бесконтактного канала связи на автономный носитель, где он используется для шифрования ПИН-кода, после чего ПИН-код с помощью бесконтактного канала связи отправляется на стационарный платежный терминал, где зашифрованный ПИН-код дешифруется при помощи закрытого ключа.

**Описание изобретения к патенту**

ОБЛАСТЬ ТЕХНИКИ, К КОТОРОЙ ОТНОСИТСЯ ИЗОБРЕТЕНИЕ

Изобретение относится к области бесконтактных электронных платежных систем, таких как системы для совершения платежей через мобильный телефон либо платежный терминал. Также изобретение включает способ подтверждения платежа при помощи мобильного устройства, беспроводным образом сообщающегося с платежным терминалом.

УРОВЕНЬ ТЕХНИКИ

Известно множество инструментов для совершения платежей - как реально существующих, так и оставшихся на стадии патентных документов. Эти инструменты дают возможность авторизировать платеж через платежный терминал.

Изобретение, приведенное в патенте CN 1450782, описывает взаимодействие между мобильным телефоном и платежным терминалом, однако не имеет отношения к конкретному оборудованию, обеспечивающему безопасность совершаемых платежей. Также существует вариант воплощения изобретения CN 101136123, в соответствии с которым мобильный телефон используется для ввода пароля, однако клавиатура телефона не является приемлемым методом ввода ПИН-кода с точки зрения безопасности.

Решение в соответствии с патентом US 2002/0147658 А1 описывает взаимоотношения между участниками процесса электронного платежа, однако не затрагивает техническую организацию отдельных элементов. Прочие аналогичные изобретения, такие как WO 03/012717 А1 и US2007/0106564 А1, предлагают способ организации элементов, но не затрагивают вопрос конкретного технического воплощения, которое обеспечило бы достаточную безопасность платежей. Изобретение согласно WO 2008/105703 описывает участие мобильного телефона в сообщении с платежным терминалом, однако не предусматривает достаточно безопасного хранения данных о расчетной карточке в мобильном телефоне. Определенные возможности сообщения мобильного телефона и платежного терминала также описаны в таких патентах, как IЕ 980562, US 6450407 В1 и GB 2432031A. Однако в этих патентах не предлагается конфигурация для простого обеспечения безопасности платежей.

Существующие инструменты не позволяют объединить функции нескольких платежных карт, обеспечив достаточную безопасность. Однако, рассмотрев отзывы пользователей, можно обнаружить, что им необходимо средство для простой и быстрой манипуляции с платежными инструментами. Было бы логично использовать для этого такое распространенное средство, как мобильный телефон.

РАСКРЫТИЕ ИЗОБРЕТЕНИЯ

Описанные неудобства в целом устраняются при использовании системы бесконтактных платежей, состоящей из платежного терминала, подключенного к серверу обработки платежей, и элемента обеспечения безопасности. Также система включает мобильное устройство с дисплеем и клавиатурой, такое как мобильный телефон. Система предусматривает установку в мобильное устройство карты памяти, содержащей, по крайней мере, два отдельных защищенных элемента, связанных с управляющим устройством. Мобильное устройство сообщается с платежным терминалом беспроводным способом, и, по крайней мере, один защищенный элемент на съемной карте памяти содержит данные платежной карты.

Размещение защищенных элементов на сменной карте памяти создает предпосылки для расширения возможностей существующих телефонов с возможностью установки карты памяти. Важной особенностью описываемой конфигурации является аппаратная часть устройств, физическое разделение защищенных элементов; решение, позволяющее безопасно хранить информацию о платежных картах, принадлежащих различным финансовым учреждениям. Защищенные элементы сообщаются с управляющим устройством, активирующим их. Управляющее устройство всегда активирует защищенный элемент с данными о выбранной платежной карте. В данном воплощении съемная карта памяти может нести функции нескольких платежных карт в соответствии с количеством защищенных элементов и даже может хранить личную информацию.

Для упрощения ввода ПИН-кода, соответствующего платежной карте в рамках соответствующего защищенного элемента, логично обеспечить для системы отдельный носитель для ввода ПИН-кода. Носитель включает блок хранения ПИН-кода, блок шифрования ПИН-кода и блок беспроводной связи; все это обеспечивает сообщение носителя с платежным терминалом и/или устройством мобильной связи.

Структура носителя обеспечивает безопасную передачу зашифрованного ПИН-кода на платежный терминал - напрямую либо через устройство мобильной связи. Для обеспечения простоты работы с носителем подразумевается, что он будет пассивным, без собственного долгосрочного источника питания, и электроэнергией будет снабжаться из принимаемого электромагнитного поля.

Предусматривается оснащение карты памяти НДЧ-элементом, обеспечивающим связь устройства мобильной связи с платежным терминалом. В этом случае возможно использование устройства, не оснащенного изначально НДЧ-элементом, однако получающего доступ к нему при установке карты памяти. Для простоты работы с картой памяти предусматривается снабжение карты с НДЧ-элементом антенной для сообщения с платежным терминалом.

Для достижения большей безопасности при вводе ПИН-кода с клавиатуры устройства мобильной связи предусматривается размещение блока единоразового создания пароля в защищенном элементе на карте памяти. Единоразовый пароль генерируется исключительно для текущего платежа.

Для упрощения работы устройство мобильной связи может быть оснащено кнопкой старта приложения бесконтактного платежа. Кнопка выделяется пиктограммой платежа, возможно в виде символа местной валюты. При нажатии кнопки автоматически запускается приложение и/или подтверждаются индивидуальные шаги процесса.

В предпочтительной конфигурации устройства мобильной связи, наряду с размещением на съемной карте памяти защищенных элементов, возможно наличие защищенного элемента, установленного на печатной плате устройства мобильной связи. Этот элемент или совокупность их на печатной плате может содержать виртуальный блок защищенных данных платежного терминала, включающий блок шифрования и, в идеале, блок временного хранения данных. Такая конфигурация позволяет использовать устройство мобильной связи непосредственно в качестве платежного терминала.

Платежный терминал подключается к удаленному серверу обработки данных, который, в свою очередь, подключен, по крайней мере, к одной базе данных определенного финансового учреждения.

Базовой для НДЧ-элемента является частота 13,56 МГц. Для обеспечения лучшего прохождения электромагнитного поля желательно использовать другую частоту. При сохранении существующей аппаратной конфигурации платежных терминалов эта цель может быть достигнута путем размещения преобразователя частот у антенны платежного терминала. Преобразователь питается электроэнергией из электромагнитного поля антенны. Антенна съемной карты памяти настраивается на новую частоту.

Недостатки существующих технологий в большой степени устраняются благодаря методу авторизации платежей, используемому при совершении бесконтактных платежей, выполняемых посредством платежного терминала и устройства мобильной связи, такого как мобильный телефон, что описано в данном изобретении. Предметом изобретения является то, что управляющее устройство в устройстве мобильной связи используется для активации необходимого защищенного элемента, соответствующего выбранной платежной карте, информация о которой хранится на карте памяти. Устройство мобильной связи сообщается с платежным терминалом путем беспроводной связи. Эта часть процесса отменяет необходимость вводить платежную карту в приемник платежного терминала

В случае необходимости ввода ПИН-кода его ввод может быть организован несколькими путями. Пользователь может ввести ПИН-код, используя клавиатуру на платежном терминале. Конфигурация, при которой ПИН-код содержится на отдельном носителе, позволяет удобно и безопасно вводить ПИН-код, лишь поднеся носитель к элементу связи терминала. Для ввода ПИН-кода платежный терминал генерирует публичный ключ и отправляет его на носитель, где ключ используется для шифрования ПИН-кода. Затем ПИН-код отправляется на терминал путем беспроводной передачи данных. Полученный зашифрованный ПИН-код расшифровывается при помощи приватного ключа в платежном терминале и далее обрабатывается таким же образом, как если бы был введен с клавиатуры на терминале.

Также возможно использование процедуры, при которой с помощью соответствующего модуля создается единоразовый пароль, который отправляется на платежный терминал.

При рассмотрении возможности использования устройств мобильной связи без собственной функции НДЧ-сообщения целесообразно использование НДЧ-элемента, установленного в съемную карту памяти.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

Изобретение представлено более подробно на фиг.1, иллюстрирующем систему приложения для совершения бесконтактных платежей с отдельным носителем ПИН-кода. Также система включает три отдельных модуля платежных карт, относящихся к трем различным финансовым учреждениям, содержащихся на съемной карте памяти.

ОСУЩЕСТВЛЕНИЕ ИЗОБРЕТЕНИЯ

Пример 1

Система включает устройство мобильной связи 1 в форме мобильного телефона без собственного НДЧ-элемента. В слот 1 мобильного телефона устанавливается карта памяти 3 формата micro SD. Съемная карта памяти со стандартными параметрами включает четыре защищенных элемента 2. Каждый из них является физически отдельным и независимым. На съемной карте памяти 3 также расположен блок управления для переключения защищенного элемента 2 по выбору пользователя. Блок управления отвечает за активацию конкретного защищенного элемента. Один защищенный элемент 2 содержит модуль создания единоразового пароля 12, а остальные три защищенных элемента на карте памяти содержат информацию о платежных картах, в данном примере принадлежащих различным финансовым учреждениям, например VISA, EC/MC и LGM. Съемная карта памяти 3 подключается посредством контактов к печатной плате мобильного телефона 1 и через проводящие пути аппаратной части телефона - к блоку управления 4. Устройство мобильной связи 1 подключается к платежному терминалу 6 посредством беспроводного канала 5 НДЧ-типа. Устройство мобильной связи 1 сообщается с платежным терминалом 6 посредством НДЧ-элемента 7, размещенного на карте памяти 3.

Карта памяти 3 оснащена НДЧ-элементом 7 с НДЧ антенной 8. Система включает отдельный носитель 13 для ввода ПИН-кода. Носитель содержит модуль хранения ПИН-кода, шифровальный модуль и модуль беспроводной связи для подключения носителя 13 к платежному терминалу 6 и/или устройству мобильной связи 1. Носитель 13 выглядит как брелок, безопасно передающий ПИН-код на платежный терминал 6, будучи поднесенным к нему. Носитель 13 получает питание из принимаемого электромагнитного поля и не имеет собственного источника питания.

Устройство мобильной связи 1 оснащено отдельной кнопкой для запуска приложения для осуществления бесконтактных платежей, отмеченной символом валюты евро.

Сервер обработки платежей 10 применяется с той же целью, с какой он применяется при обработке платежей в платежном терминале. Сервер обработки платежей 10 также подключен к базам данных 11 финансовых учреждений, таких как банки, учитывающим совершенные платежи и ассоциирующим их с конкретным клиентом и его счетом. На антенну 8 платежного терминала 6 крепится преобразователь частот. Он получает питание из электромагнитного поля антенны 8. Антенна 8 на съемной карте памяти 3 настроена на преобразованную частоту.

Оплата при помощи устройства мобильной связи 1 в торговой точке с платежным терминалом 6 производится следующим образом. Пользователь выбирает в меню тип карты, с которой будет осуществляться платеж (VISA, ЕС/МС или LGM), и затем подносит устройство мобильной связи 1 к бесконтактному НДЧ-элементу на платежном терминале 6. Платежный терминал 6 определяет выбранный пользователем тип карты (VISA, ЕС/МС или LGM) и направляет запрос на авторизацию платежа на сервер обработки платежей 10. Запрос обрабатывается - сперва проходит проверку на шифровальном модуле на подлинность приложения и затем генерируется запрос на доступ к базе данных 11 финансового учреждения. Там запрос обрабатывается таким же образом, как если бы платеж совершался с платежной карты.

В платежном приложении блок управления 4 активирует соответствующий блоку выбранной платежной карты 9 защищенный элемент 2 на карте памяти 3. Устройство мобильной связи 1 подключается с платежным терминалом 6 посредством беспроводного канала 5. В описанном решении ПИН-код может вводиться с клавиатуры платежного терминала 6. Удобнее будет использовать отдельный носитель 13, передающий информацию о ПИН-коде на терминал 6, будучи поднесенным к нему. Платежный терминал 6 генерирует публичный ключ, отправляет его на носитель 13, где он используется для шифрования ПИН-кода, после чего ПИН-код отправляется на терминал 6. Канал передачи данных между терминалом 6 и носителем 13 является беспроводным. Полученный зашифрованный ПИН-код дешифруется на терминале при помощи закрытого ключа.

Пример 2

Система авторизации бесконтактного платежа, описанная в данном примере, отличается от описанной в примере 1 тем, что устройство мобильной связи 1 снабжено собственными защищенными элементами 2 на печатной плате. Такой защищенный элемент 2 содержит защищенную часть виртуального платежного терминала, содержащую шифровальный блок и, по возможности, блок временного хранения данных. Такая конфигурация позволяет использовать устройство мобильной связи 1 в качестве личного виртуального платежного терминала. Съемная карта памяти 3 является элементом, содержащим блок данных 9 о платежной карте, и расширяет возможности устройства мобильной связи 1 в качестве НДЧ-передатчика.

ПРОМЫШЛЕННАЯ ПРИМЕНИМОСТЬ

Практическое применение изобретения очевидно. В соответствии с изобретением возможно изготовление и использование систем для осуществления бесконтактных платежей, в которых устройство мобильной связи пользователя выступает в качестве инструмента для осуществления платежей.

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ ОБОЗНАЧЕНИЙ:

1 - Устройство мобильной связи

2 - Защищенный элемент

3 - Съемная карта памяти

4 - Блок управления

5 - Канал передачи данных

6 - Платежный терминал

7 - НДЧ-элемент

8 - Антенна

9 - Блок данных о платежной карте

10 - Сервер обработки платежей

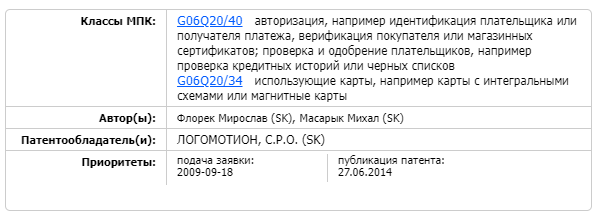
11 - База данных финансового учреждения

12 - Блок создания единоразового пароля

13 - Носитель ПИН-кода

**Патент 3:**

**Cистема электронных платежей и способ авторизации платежа**

****

Изобретение относится к системе электронных платежей. Техническим результатом является повышение надежности проведения платежей за счет защиты от несанкционированного доступа. Система содержит модуль виртуального платежного терминала в персональном мобильном устройстве пользователя, которое содержит модуль управления виртуальным платежным терминалом, сменную карту памяти, на которой есть, по крайней мере, два физически раздельных защищенных элемента. Сменная карта памяти связана с защищенным элементом, содержащим защищенную область виртуального платежного терминала. Устройство мобильной связи и/или отдельный переносной элемент настроены таким образом, чтобы иметь возможность подключиться к удаленному серверу обработки платежей. Сменная карта памяти и отдельный портативный элемент могут быть оснащены модулем связи стандарта NFC. В зависимости от выбора пользователя соответствующий защищенный элемент с данными платежной карты, выбранной модулем выбора платежной карты, активируется на сменной карте памяти. Идентификационные данные платежной карты пользователя добавляются к идентификационным данным получателя платежа вместе с одноразовым паролем, который был создан модулем генерации одноразовых паролей. 2 н. и 8 з.п. ф-лы, 2 ил.

**Формула изобретения**

1. Система проведения электронных платежей, содержащая устройство мобильной связи, выполненное с дисплеем, печатной аппаратной платой и сменной картой памяти, размещенной в слот устройства мобильной связи, а также с клавиатурой, выполненной с возможностью ввода выбранного пользователем PIN кода и запуска приложения электронного платежа с помощью удаленного сервера обработки платежей, причем печатная аппаратная плата выполнена с виртуальным платежным терминалом, снабженным модулем управления виртуального платежного терминала и связанным с защищенным элементом с защищенной областью виртуального терминала, включающим модуль хранения данных и модуль кодирования для передачи кодированных данных по сети Интернет на сервер обработки платежей, при этом сменная карта памяти связана с модулем управления виртуального платежного терминала и выполнена с независимыми друг от друга защищенными элементами, причем один защищенный элемент карты памяти снабжен модулем создания одноразового пароля, а, по меньшей мере, один другой защищенный элемент карты памяти снабжен модулем активизации одной из платежных карт пользователя, связанным с упомянутым модулем создания одноразового пароля и с модулем управления виртуального платежного терминала

2. Система электронных платежей по п.1, отличающаяся тем, что защищенный элемент с защищенной областью виртуального платежного терминала размещен на печатной плате устройства мобильной связи и связан контактным каналом передачи данных с модулями сменной карты памяти.

3. Система электронных платежей по п.1, отличающаяся тем, что защищенный элемент с защищенной областью виртуального платежного терминала размещен в отдельном переносном приборе и связан бесконтактным каналом передачи данных с модулями сменной карты памяти.

4. Система электронных платежей по п.3, отличающаяся тем, что бесконтактный канал передачи данных выполнен в виде канала NFC, а отдельный переносной прибор выполнен с возможностью подключения через компьютер к серверу обработки платежей.

5. Система электронных платежей по п.4, отличающаяся тем, что сменная карта памяти снабжена модулем связи канала NFC, а отдельный переносной прибор снабжен антенной и модулем связи канала.

6. Система электронных платежей по любому из пп.1-3, отличающаяся тем, что перед сервером обработки платежей помещается модуль пакетной передачи данных, который выполнен с возможностью централизованного соединения с несколькими модулями виртуального платежного терминала.

7. Система электронных платежей по любому из пп.1-5, отличающаяся тем, что устройство мобильной связи оснащено отдельной клавишей для запуска приложения электронного платежа, причем на клавише изображен специальный символ платежа.

8. Способ авторизации платежа, осуществляемый с помощью системы по п.1, при котором пользователь выбирает предмет покупки, а затем с помощью своего мобильного устройства связи, аппаратная плата которого выполнена с виртуальным платежным терминалом и с защищенным элементом с защищенной областью виртуального платежного терминала, выбирает для оплаты платежную карту и передает по сети Интернет запрос в Интернет-магазин на осуществление оплаты, а также сведения о выбранной карте и платеже для обработки на удаленный сервер обработки платежей для идентификации счетов Интернет-магазина и пользователя, и получения уникального номера платежной проводки, передаваемого как пользователю, так и в Интернет-магазин, виртуальный платежный терминал предоставляет номер авторизации, а для выбора платежной карты пользователь активирует соответствующий защищенный элемент с модулем выбора платежной карты на сменной карте памяти мобильного устройства, модулем управления виртуального платежного терминала которого к платежным данным об идентификации получателя платежа и одноразовому паролю, который формируется модулем создания одноразового пароля сменной карты, добавляются номер проводки и данные об идентификации платежной карты пользователя; эти данные подписываются электронной подписью и далее посылаются в кодированном виде через сервер обработки платежей в базу данных финансового учреждения, к которому относится платежная карта, для списания суммы платежа.

9. Способ авторизации платежа по п.8, отличающийся тем, что модуль управления виртуального платежного терминала в устройстве мобильной связи получает от финансового учреждения уникальный номер транзакции, подтверждающий, что оплата была совершена.

10. Способ авторизации платежа по любому из пп.8, 9, отличающийся тем, что защищенный элемент с защищенной областью виртуального платежного терминала размещен в отдельном переносном приборе и связан бесконтактным каналом передачи в виде канала NFC данных с модулями сменной карты памяти.

**Описание изобретения к патенту**

ОБЛАСТЬ ТЕХНИКИ, К КОТОРОЙ ОТНОСИТСЯ ИЗОБРЕТЕНИЕ

Изобретение относится к системе электронных платежей, особенно платежей через устройство мобильной связи, как, например, мобильный телефон. Изобретение также описывает способ реализации и авторизации электронного платежа.

УРОВЕНЬ ТЕХНИКИ

Платежные терминалы широко применяются в процессе электронных платежей с помощью различных платежных карт. Платежные терминалы подключены к платежной системе. Существуют платежные системы, расчеты в которых осуществляются с помощью платежных терминалов, которые обслуживаются организациями - получателями платежа.

Изобретение, приведенное в патенте CN 1450782, описывает взаимодействие между мобильным телефоном и платежным терминалом, которое, однако, не обеспечивает безопасность совершаемых платежей. Также существует вариант воплощения изобретения CN 101136123, в соответствии с которым мобильный телефон используется для ввода пароля, однако сам телефон при этом не выполняет функции платежного терминала.

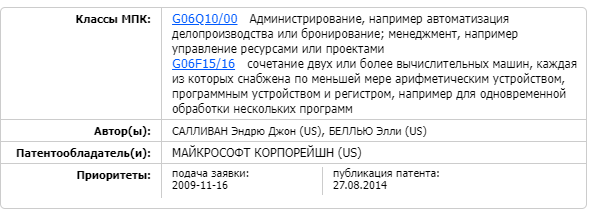
Решение в соответствии с патентом US 2002/0147658 А1 описывает взаимоотношения между участниками процесса электронного платежа, однако не затрагивает техническую организацию отдельных элементов. Прочие аналогичные изобретения, такие как WO 03/012717 А1 и US 2007/0106564 А1, предлагают способ организации элементов, но не затрагивают вопрос конкретного технического воплощения, которое обеспечило бы достаточную безопасность платежей. Изобретение согласно WO 2008/105703 описывает участие мобильного телефона в обмене информацией с платежным терминалом, однако не предусматривает достаточно безопасного хранения данных о платежной карте в мобильном телефоне. Определенные возможности связи между мобильным телефоном и платежным терминалом описаны в таких патентах, как IE 980562, US 6450407 В1 и GB 2432031A. Однако и в этих решениях не предлагается удобная система для обеспечения безопасности платежей.

РАСКРЫТИЕ ИЗОБРЕТЕНИЯ

Упомянутых недостатков можно избежать, используя систему оплаты электронных платежей, которая состоит из защищенного элемента, сервера обработки платежей, мобильного устройства связи с дисплеем и клавиатурой, такого как мобильный телефон, как описано в этом изобретении. Использование мобильного телефона предполагает, что мобильное устройство связи оснащено модулем виртуального платежного терминала. Функциями платежного терминала оборудуется устройство, находящееся в полном распоряжении пользователя, а не получателя платежа, как в существующих решениях. Защищенный элемент с модулем кодирования и модулем хранения данных может быть размещен внутри устройства мобильной связи, как, например, мобильный телефон, или он может быть выполнен в виде отдельного переносному модуля в форме клавиши USB. Клавиша USB соединяется с персональным компьютером через соединитель USB. Устройство мобильной связи также содержит сменную карту памяти, например, распространенного формата microSD. На сменной карте памяти содержатся, по меньшей мере, два физически раздельных защищенных элемента, и сменная карта памяти подключается к модулю управления виртуальным терминалом. Размещение защищенных элементов на сменной карте памяти создает предварительное условие, которое предоставляет возможности расширить возможности существующих телефонов со слотом для вставки карты памяти. Важной характеристикой системы, описанной здесь, есть аппаратное, физическое разделение защищенных элементов; решение, которое дает возможность хранения данных о платежных картах, которые принадлежат различным финансовым учреждениям, в надежном, безопасном месте. В упомянутом решении сменная карта памяти может содержать в себе различные функции платежной карты, и согласно количеству защищенных элементов она может даже содержать безопасную область, в которой могут храниться персональные данные или тому подобное. Защищенные элементы на сменной карте памяти соединяются с модулем управления, который переводит защищенный элемент в активный режим. Модуль управления всегда активирует защищенный элемент с выбранными данными платежной карты. Устройство, на котором размещен защищенный элемент с модулем кодирования и модулем хранения данных, настроено таким образом, чтобы быть способным соединиться с сервером обработки платежей. С точки зрения обработки платежей система и связанные с ней элементы организованы таким же образом, как если бы платежи производились через терминалы, принадлежащие финансовым учреждениям. Модуль кодирования и модуль хранения данных формируют защищенную часть виртуального терминала, расположенного в защищенном элементе. В пределах системы описанных электронных платежей эти модули могут быть размещены на печатной плате технического обеспечения устройства мобильной связи или в отдельном переносном элементе, который приспособлен для подсоединения к персональному компьютеру. В первом случае канал передачи между сменной картой памяти и управляющим модулем виртуального терминала - контактный и создается проводящими путями технического обеспечения устройства мобильной связи. Во втором случае канал передачи между отдельным переносным элементом и сменной картой памяти бесконтактный (беспроводной). Эта основная конфигурация предоставляет возможность создания платежного терминала непосредственно в устройстве мобильной связи каждого пользователя, как, например, в мобильном телефоне. Пользуясь системой, описанной выше, пользователь сможет произвести оплату бесконтактным способом, пользуясь своим телефоном или телефоном, который связывается с его персональным компьютером. С тех пор как это решение вызовет увеличение числа платежных терминалов и с тех пор как платежные терминалы не будут управляться только финансовыми организациями, но в основном, каждым пользователем мобильного телефона, было бы разумно, если бы связь между виртуальным терминалом и сервером обработки платежей прошла сначала через модуль пакетной передачи данных, а затем, на выходе - на сервер обработки платежей. Индивидуальные платежи от большого ряда индивидуальных виртуальных терминалов будут вводами для модуля пакетной передачи данных. Предполагается, что один виртуальный терминал будет иметь небольшое количество платежей. На выходе модуля пакетной передачи данных будет краткая информация о полученных платежах в пакетном режиме.

**Патент 4:**

**Визуализация подписок rss на календаре**

****

Изобретение относится к визуализации каналов исчерпывающей сводки сайта (RSS). Техническим результатом является повышение быстродействия доступа пользователя к содержимому электронного календаря. Способ визуализации каналов исчерпывающей сводки сайта (RSS) включает в себя прием канала RSS с помощью клиента RSS, причем канал RSS содержит элемент данных, ассоциированный с событием и соответственной датой события. Элемент данных содержит пиктограмму, являющуюся визуальным представлением события, ассоциированного с элементом данных. Далее, согласно способу, отображают принятый элемент данных на поверхности электронного календаря. Поверхность электронного календаря содержит боковое окно, в котором отображается структура каталога доступных компоновок календаря, и в боковом окне дополнительно отображается структура каталога доступных каналов RSS. Принятый элемент данных отображается в местоположении на электронном календаре, представляющем упомянутую дату события, при этом при отображении элемента данных отображают, по меньшей мере, пиктограмму, содержащуюся в принятом элементе данных. 3 н. и 15 з.п. ф-лы, 5 ил.

**Формула изобретения**

1. Способ визуализации каналов исчерпывающей сводки сайта (RSS), содержащий этапы, на которых:  
принимают канал RSS с помощью клиента RSS, причем канал RSS содержит элемент данных, ассоциированный с событием и соответственной датой события, при этом элемент данных содержит пиктограмму, являющуюся визуальным представлением события, ассоциированного с элементом данных; и отображают принятый элемент данных на поверхности электронного календаря, при этом поверхность электронного календаря содержит боковое окно, в котором отображается структура каталога доступных компоновок календаря, и в боковом окне дополнительно отображается структура каталога доступных каналов RSS, причем принятый элемент данных отображается в местоположении на электронном календаре, представляющем упомянутую дату события, при этом при отображении элемента данных отображают, по меньшей мере, пиктограмму, содержащуюся в принятом элементе данных, причем принятый элемент данных отображается отличающимся образом от множества визуализируемых введенных пользователем напоминаний в электронном календаре.

2. Способ по п.1, в котором, при приеме канала RSS с помощью клиента RSS, канал RSS принимают так, что клиент RSS также обрабатывает данные, относящиеся к функциональным возможностям планирования электронного календаря.

3. Способ по п.1, в котором, при приеме канала RSS с помощью клиента RSS, канал RSS принимают так, что упомянутая дата события выводится из принятого элемента данных.

4. Способ по п.1, дополнительно содержащий этапы, на которых:  
загружают новое содержимое из канала RSS; и  
обновляют отображаемый элемент данных загруженным новым содержимым.

5. Способ по п.1, в котором принятый элемент данных содержит дату и время события в предварительно форматированном поле данных в элементе данных.

6. Способ по п.1, в котором при отображении пиктограммы пиктограмму отображают в местоположении на электронном календаре, предварительно определенном пользователем.

7. Машиночитаемый носитель, который хранит набор команд, которым при его исполнении выполняется способ обработки каналов исчерпывающей сводки сайта (RSS), при этом способ, выполняемый набором команд, содержит: прием канала RSS с помощью клиента RSS, причем канал RSS содержит элемент данных, ассоциированный с событием и соответственной датой события, при этом элемент данных содержит пиктограмму, являющуюся визуальным представлением события, ассоциированного с элементом данных; получение даты события из принятого элемента данных; и отображение принятого элемента данных на поверхности электронного календаря, при этом поверхность электронного календаря содержит боковое окно, в котором отображается структура каталога доступных компоновок календаря, и в боковом окне дополнительно отображается структура каталога доступных каналов RSS, причем элемент данных отображается в местоположении на электронном календаре, представляющем упомянутую дату события, при этом при отображении элемента данных отображается, по меньшей мере, пиктограмма, содержащаяся в принятом элементе данных, при этом принятый элемент данных отображается отличающимся образом от множества визуализируемых введенных пользователем напоминаний в электронном календаре.

8. Машиночитаемый носитель по п.7, при этом клиент RSS также обрабатывает данные, относящиеся к функциональным возможностям планирования электронного календаря.

9. Машиночитаемый носитель по п.7, при этом пиктограмма, содержащаяся в элементе данных, представляет информацию о погоде.

10. Машиночитаемый носитель по п.7, в котором способ дополнительно содержит:  
загрузку нового содержимого из канала RSS; и обновление отображаемого элемента данных загруженным новым содержимым.

11. Машиночитаемый носитель по п.7, в котором принятый элемент данных содержит дату и время события в предварительно форматированном поле данных в элементе данных.

12. Машиночитаемый носитель по п.7, при этом пиктограмма отображает событие и время.

13. Машиночитаемый носитель по п.12, при этом пиктограмма отображается в местоположении на электронном календаре, предварительно определенном пользователем.

14. Система для обработки каналов исчерпывающей сводки сайта (RSS), содержащая:  
запоминающее устройство; процессорный блок, подключенный к запоминающему устройству, при этом процессорный блок выполнен с возможностью: принимать канал RSS с помощью клиента RSS, причем канал RSS содержит элемент данных, ассоциированный с событием и соответственной датой события, при этом элемент данных содержит пиктограмму, являющуюся визуальным представлением события, ассоциированного с элементом данных; и  
отображать принятый элемент данных на поверхности электронного календаря, при этом поверхность электронного календаря содержит боковое окно, в котором отображается структура каталога доступных компоновок календаря, и в боковом окне дополнительно отображается структура каталога доступных каналов RSS, причем принятый элемент данных отображается в местоположении на электронном календаре, представляющем упомянутую дату события, при этом при отображении элемента данных отображается, по меньшей мере, пиктограмма, содержащаяся в принятом элементе данных, причем принятый элемент данных отображается отличающимся образом от множества визуализируемых введенных пользователем напоминаний в электронном календаре.

15. Система по п.14, в которой клиент RSS также обрабатывает данные, относящиеся к функциональным возможностям планирования электронного календаря.

16. Система по п.14, в которой дата и время события выводятся из принятого элемента данных.

17. Система по п.14, в которой процессорный блок дополнительно выполнен с возможностью: загружать новое содержимое из канала RSS; и обновлять отображаемый элемент данных загруженным новым содержимым.

18. Система по п.14, в которой пиктограмма отображается в местоположении на электронном календаре, предварительно определенном пользователем.

**Описание изобретения к патенту**

Уровень техники

Каналы обогащенной сводки сайта ("RSS") можно принимать по сети, чтобы предоставить информацию, относящуюся к любому количеству тем. Часто канал RSS может содержать данные, которые относятся к конкретной дате, или иногда к конкретному времени в дате. Эти данные в настоящее время визуализируются в устройстве чтения RSS. Устройство чтения RSS в современных системах отображает данные в виде элементов, отсортированных на основе времени, когда элементы публиковались в канале RSS. Однако этот способ отображения элементов RSS не использует ценную информацию о дате события, содержащуюся в этих данных.

Сущность изобретения

Данная сущность изобретения предоставляется, чтобы представить набор идей в упрощенном виде, которые дополнительно описываются ниже в подробном описании. Данная сущность изобретения не предназначена для определения ключевых признаков или существенных признаков заявленного предмета изобретения, и также не предназначена для использования в ограничении объема заявленного предмета изобретения.

Может предоставляться визуализация подписок RSS на календаре. Сначала канал RSS может быть принят клиентом RSS. Канал RSS может содержать элемент данных, ассоциированный с датой события. Компьютер-получатель, исполняющий программу электронного календаря, может отобразить принятый элемент данных на поверхности электронного календаря. Элемент данных может отображаться в местоположении на электронном календаре, представляющем дату события. Периодически новое содержимое может загружаться из канала RSS и использоваться для обновления отображенных элементов данных. Клиент RSS также может обрабатывать данные, относящиеся к функциональным возможностям планирования электронного календаря. Принятый элемент данных может содержать дату события в предварительно форматированном поле данных в элементе данных. В качестве альтернативы, дата события может выводиться из другой информации в принятом элементе данных.

## **Вывод**: в ходе выполнения данной лабораторной работы я изучил структуру патентов, изучил схему строения паттерна.