



ПАТЕНТНО ВЕДОМСТВО
на Република България

ПАТЕНТ
ЗА
ИЗОБРЕТЕНИЕ

Рег. № 67746 В1

Заявка № 113519

Дата на заявяване: 07/04/2022

Приоритет:

Срок на действие: 07/04/2042

Публ. за заявката:

Публ. за издаване: 16/06/2025

Наименование: МЕТОД ЗА
УДОСТОВЕРЯВАНЕ

Притежател/и:

ИКТ платформи ООД

ул. "Юрий Гагарин", бл. 154Б, вх. Б,
ет. 3, ап. 16, 1113 София [BG]

Изобретател/и:

Димитър Анастасов Григоров
Светослав Маринов Новков

Olya
Georgieva
Dimitrova

Digitally signed by
Olya Georgieva
Dimitrova
Date: 2025.06.23
08:57:58 +03:00

ОЛЯ ДИМИТРОВА
ПРЕДСЕДАТЕЛ

РЕПУБЛИКА БЪЛГАРИЯ

(19) **BG**



ОПИСАНИЕ КЪМ ПАТЕНТ
ЗА
ИЗОБРЕТЕНИЕ

(11) **67746 B1**

(51) Int. Cl.
G 06 F 21/00 (2013.01)
G 06 F 21/31 (2013.01)
G 06 F 21/45 (2013.01)
(52) CPC
G 06 F 21/00 (2013.01)
G 06 F 21/31 (2013.01)
G 06 F 21/45 (2013.01)

ПАТЕНТНО ВЕДОМСТВО

(21) Заявителски № 113519
(22) Заявено на 07.04.2022
(24) Начало на действие
на регистрацията от: 07.04.2022

Приоритетни данни

(41) Публикувана заявка в
бюлетин № 202310.1 на 16.10.2023
(45) Отпечатано на 16.06.2025
(46) Публикувано в
бюлетин № 202506.1 на 16.06.2025
(56) Информационни източници:
(62) Разделена заявка от рег. №

(73) Притежатели (и):
ИКТ ПЛАТФОРМИ ООД
1113 СОФИЯ, УЛ. "ЮРИЙ ГАГАРИН", БЛ. 154Б,
ВХ. Б, ЕТ. 3, АП. 16

(72) Изобретател(и):
Димитър Анастасов Григоров
Светослав Маринов Новков

(74) Представител по индустриална собственост:
Нейко Христов Нейков
1680 София, ул. "Ворино" 58

(86) № на РСТ заявка:
(87) № и дата на РСТ публикация:

(54) МЕТОД ЗА УДОСТОВЕРЯВАНЕ

(57) Изобретението се отнася до метод за удостоверяване, предназначен за разрешаване на достъп и може да намери приложение за целите на осигуряване на по-високо ниво на сигурност при електронна идентификация и/или комуникация и защита срещу неоторизиран достъп, включително при визуално, видео или друг вид наблюдение на процеса. Методът е приложим и работи успешно в различни физически, виртуални и операционни среди, като защитата се постига чрез комбиниране на тайни елементи с подвеждащи елементи и неявни правила, които освен това могат да бъдат променяни от скрити инструкции. Методът значително ограничава възможностите за използване на стандартни методи за

проследяване на действията на потребителя чрез записване на клавишни комбинации и последователности и/или записване на движения на курсора, или заснемане на показанията на екрана, или визуално наблюдение, тъй като видимите действия не разкриват тайната комбинация. Също така методът не изисква използване на допълнителни устройства или ключове за сигурност от какъвто и да е вид.

29 претенции 19 фигури

BG 67746 B1

BG 67746 B1



(54) МЕТОД ЗА УДОСТОВЕРЯВАНЕ

Област на техниката

Изобретението се отнася до метод за удостоверяване, предназначен за разрешаване на достъп и може да намери приложение за целите на осигуряване на по-високо ниво на сигурност при електронна идентификация и/или комуникация и защита срещу неоторизиран достъп, включително при визуално, видео или друг вид наблюдение на процеса.

Предшестващо състояние на техниката

Понастоящем са известни различни методи за електронно удостоверяване. Удостоверяването обикновено се извършва чрез взаимодействие между потребител и компютърна система. Компютърната система може да установи самоличността на потребителя, като поиска един или повече фактори за удостоверяване от потребителя.

Най-разпространените фактори за удостоверяване са идентификатор, напр. име на потребителя и „фактор въз основа на знание“, напр. парола и/или персонален идентификационен номер (ПИН). Потребителят обикновено се удостоверява, ако комбинацията от фактори за удостоверяване, предоставена от потребителя, съвпада със записи, отнасящи се до самоличността на потребителя [[US 08392975](#)]. Тъй като процесът оторизира вход в система, често се нарича „влизане“. След като потребителя въведе потребителско име и парола, компютърът ги сравнява със тези, които са записани в базата от данни и ако съвпадат, дава достъп на потребителя в системата. Системите за удостоверяване, базирани на „това, което потребителят знае“ са най-атрактивни поради това, че са евтини, лесни за ползване, лесни за разпространение по електронен път и не изискват допълнителен хардуер, за разлика от други фактори за удостоверяване [[US 20040119746](#)].

Основният им недостатък е, че паролата може да бъде открадната, случайно разкрита или забравена. Кражбата може да стане с помощта на шпионски софтуер, записващ клавишните комбинации и/или движенията на курсора (т. нар. Key Listener и Key Logger), в някои случаи с помощта на софтуер, заснемащ показанията на екрана (т. нар. Screen Recorder), чрез видеозапис на сесия за влизане или друг начин за подслушване.

Широко достъпните микро аудио и визуални сензори и други инструменти улесняват скритите наблюдения. Видео- и/или аудио- запис е възможен от значително разстояние и по всяко време на деня, застрашавайки тайните пароли или ПИН кодове, въведени от компютърни или мрежови онлайн потребители на обществени места (банкомати; клиенти в точка на продажба; Интернет терминали предлагани в различни конференции, кафенета, библиотеки; служители, споделящи големи офиси с терминали за настолни компютри във видимия обсега на всички и на други места) [[US 20040123151](#)].

Разкриването на паролата за достъп може да стане дори чрез атака с груба сила, известна като речниковата атака, за последователно изпробване на думи от изчерпателен списък. Речниковите атаки, приложени или към хеширани пароли, прихванати на комуникационни линии, или директно на устройствата за въвеждане на парола, позволяват доста лесен ре-инженеринг на пароли [[US 20040123151](#)].

Типичните потребители избират пароли в рамките на „ниво на комфорт“ на сложност за запаметяване, обикновено в диапазона от 1 до 7 (или 8) буквено-цифрови знака. Често паролата е проста дума или цяло число (като London и 123456). Ето защо разкриването не е особено трудно. Възможни са пробиви в сигурността дори с по-ниско технологични средства за „надзъртане през рамото“, когато натрапник в близост до законния потребител наблюдава въвеждането на парола. Освен това, парола с по-голяма степен на сигурност се въвежда относително по-бавно и се запомня много по-трудно. Затова мерките, въведени за осигуряване на силни, но нерядко безсмислени пароли, често водят до това, че потребителите ги записват и държат близо до компютъра, за да си ги спомнят бързо, като по този начин улесняват натрапника да ги намери и използва и по същество компрометират целта на паролата [US 20040230843].

Ето защо, някои от съвременните методи за удостоверяване използват втори фактор на удостоверяване от категорията „фактор въз основа на притежание“ - допълнително автономно устройство, притежание на потребителя, напр. смартфон, генериращ/получаващ уникален за потребителя, за конкретния момент във времето и устройството идентифициращ динамичен код (т. нар. еднократна парола (one-time password (OTP)). OTP обикновено е кратък код (от 6 до 8 цифри), използва се еднократно, генерира се от хардуерен тоукън, софтуерен тоукън, качен на устройство или от генератор на случайни числа, изпращащ кода до потребителя чрез SMS, e-mail или друг комуникационен канал.

Подобен метод за удостоверяване може да се прилага и върху устройство, което не е собственост на потребителя, както и на обществени места. Въпреки че осигурява повече сигурност, отколкото обикновената парола, еднократната парола има недостатъци: уязвима е за фишинг и атаки от типа Man-in-the-middle (MitM), може да бъде възпроизведена след кражба на ключа, който я генерира; може да бъде прихваната и подслушана, изисква устройство и връзка с него. Освен това използването на еднократна парола изисква труден и отнемаш време процес на интеграция с корекции, понякога големи, в потока и логиката на информационните системи, често е свързана с ръчно копиране на код от едно устройство на друго.

Втори фактор на удостоверяване може да играе и ключ за сигурност (Security Key), който работи с предварително инсталиран драйвер върху общодостъпен физически носител (USB, NFC, Bluetooth). В този случай за потребителя съществува неудобството, че трябва да притежава собствено физическо устройство, да го носи със себе си и периодично да го подновява. Освен това вече има немалко пробиви в сигурността при използването на такъв ключ, които се дължат на неправилно съхранение и опазване. При тези пробиви, след прихващане на ПИН кода или паролата за идентификация на управляващия софтуер на устройството, злонамерените лица осъществяват неправомерен достъп до физическото устройство или до компютърната система, при активно включено устройство, а също и по време на стартиран управляващ софтуер за идентификация, като в последния случай дори може да не е необходимо да разполагат с ПИН кода или паролата за управляващия софтуер.

Освен това, методите, които използват „фактор въз основа на притежание“ обикновено са бавни и тромави, често не се мащабират, сложни са за разбиране, обикновено са трудни и отнемаш време за настройка, податливи са на атаки на социално инженерство срещу потребителя или персонала по поддръжката на доставчика, скъпи са за разполагане и използване и нямат сигурна устойчивост на загуба или кражба.

Затова има и методи, които използват фактор на удостоверяване от категорията „присъщ фактор за удостоверяване на автентичността“ - фактор, който се основава на физически атрибут на физическо лице и от субекта се изисква да докаже, че притежава този физически атрибут (пръстов отпечатък, ирис, лице и др.).

При тези методи съществува риск от погрешно или измамно биометрично удостоверяване. Биометричните данни са много по-скъпи и трудни за внедряване. Съществува също така значителна неохота на обществеността да ползва биометричните методи за удостоверяване поради религиозни и културни проблеми. Друга силна загриженост, ако се използват биометрични данни, е безопасността на частните биометрични данни. Веднъж откраднати, биометричните данни могат да бъдат използвани завинаги, за да се представят за лицето, от което са взети, тъй като няма как да бъдат заменени [US 20040123151]. Биометричните данни обикновено са лесни за кражба или емулиране, те са ненадеждни и приблизителни, могат да насърчат възприеманите или реални опасности от отвлечение и физическа принуда, които поставят потребителите в повишен стрес или опасност, имат сериозни недостатъци за намаляване на поверителността и много щати и държави ограничават или забраняват използването или събирането или обмена на биометрични данни от цялото или част от тяхното население, в някои или всички ситуации [US 20170346851].

Съществуващите техники за сигурност и удостоверяване са изпълнени с пропуски и компромиси. Те страдат от компромиси за използваемост (за сметка на сигурността) или компромиси за сигурност (за сметка на използваемостта). Почти всички съществуващи методи за сигурност включват компромиси, като например възможността да влезете, без да знаете паролата си, като просто поискате нова парола или възможността да влезете, без да използвате биометричен пръстов отпечатък, като вместо това използвате ПИН или парола [US 20170346851].

Съществуват много трудности, които възпрепятстват лесното премахване на такива компромиси: ако подобрената сигурност не продължи да функционира сигурно в случай на загуба, кражба или забрава от страна на потребителите, все още ще са необходими компромиси [US 20170346851]:

- Ако методът е твърде труден за разбиране, много потребители няма да могат да го използват.
- Ако се използва твърде бавно, много потребители няма да искат да го използват.
- Ако зависи от скъпи компоненти, много потребители няма да могат да си позволят да го използват.
- Ако не се мащабира (напр. да може да се използва на стотици различни места, като уеб сайтове или от голям брой различни потребители), ще бъде непрактично за потребителите да го използват или доставчиците да го предлагат.
- Ако изисква физическа връзка, но не побира всеки различен вид конектор или е необходим на машини без конектори, той ще бъде неизползваем при много обстоятелства.
- Ако не може да работи без интернет връзка (например изисква връзка за данни на мобилно устройство, но собственикът на устройството няма оставащ кредит за интернет), той няма да работи достатъчно често, за да бъде надежден.
- Ако понякога „се обърка“ (например биометрични данни, особено пръстови отпечатыци след плуване, лица в тъмното и гласове при заболяване), ще е необходима потенциално отслабваща сигурността алтернатива.

- Ако потребителите се страхуват от него или философски се противопоставят, те ще откажат да го използват (например биометрични данни).

- Ако може да бъде изгубен, забравен или променен и няма сигурно смекчаване на риска за това, той ще се нуждае от алтернатива.

- Ако внедряването (без компромис) налага допълнителни разходи за поддръжка, може да е невъзможно да се внедри икономично.

- Ако е твърде труден за настройка от потребителя или прекалено труден за разгръщане от доставчика, или изисква физическа доставка, или може да бъде обект на ненадеждна доставка, или е с прекомерни разходи, за да бъде икономически разумен за внедряване, или разгръщането разчита на информация, която потребителите не желаят да разкриват (напр. адреси, телефонни номера, рождени дни, лична информация, биометрични данни и т. н.), или съществува някаква друга причина, която не позволява да се постигне пълно покритие на потребителите, тогава ще бъде невъзможно да се избегне компрометиране на метода.

Разпространението на интернет донесе многобройни нови услуги на потребителите, резултатът от които е, че днес всеки потребител на интернет има средно 70 различни онлайн акаунта (напр. имейл, социални, работни, банкови, интереси, форуми, клубове, пазаруване, продажби, търгове, плащания, транспорт, забавления, игри и т. н.). Най-добрата практика за пароли повелява никога да не се използват в повече от един сайт, да са дълги и трудни за отгатване, да съдържат комбинации от големи и малки букви, цифри и други символи и да се променят редовно, да не са записани където и да е и да се ползват само в защитени сайтове след проверка на идентификационните данни на сертификата за сигурност на сайта. Това очевидно е нелепо и всички тези усилия са неефективни така или иначе, с появата на съвременни методи за атака като фишинг, злонамерен софтуер, активен MitM и други, които крадат или заобикалят паролите, които се използват. Повечето потребители не се съобразяват с най-добрите практики, като използват кратки или лесни пароли, използват ги повторно, записват ги и рядко, ако изобщо някога, проверяват най-напред идентификационните данни на сертификата за сигурност на сайта [[US 20170346851](#)].

Затова се разработват алтернативни методи, които преследват по-висока сигурност при по-малко разходи и трудности.

Известни са методи за идентификация на потребител, при които потребителят въвежда за вход в системата графичен код за достъп (напр. [EP 2493228](#), [US 20040230843](#), [US 08392975](#) и др.). Посочените методи са уязвими за шпионски софтуер, заснемащ екрана, както и за по-ниско технологични атаки, от типа на „надзъртане през рамото“, тъй като предложената графична парола е статична (последователността от изображения е една и съща в различни удостоверителни сесии).

Тези недостатъци отчасти се преодоляват от устойчива на измами система за въвеждане на пароли [[US 20160328552](#)], включваща метод за създаване на потребителски код за достъп и метод за удостоверяване с потребителски код за достъп.

Методът за създаване на потребителски код за достъп се състои от следните операции:

- Получаване на избрана кодова последователност, включваща: подреждане на полета за въвеждане, при което всяко поле за въвеждане включва най-малко две различни свойства от група, включваща изображения, буквено-цифрови знаци, символи, цветове, модели, звуци, текстури, топология, местоположение, ориентация или относителна позиция по отношение на потребителския интерфейс, като

кодът за достъп се получава в потребителския интерфейс, при което на всяко свойство се присвоява системна интерпретационна стойност, чрез която свойството се идентифицира от системата, при което свойствата са организирани в групи (набори), всеки набор включва отделно групиране на свойства, които да бъдат идентифицирани като мерна единица от системата, като същевременно се поддържа всяко свойство като индивидуално разпознаваемо и на всеки набор от свойства се присвоява идентификатор на набор, който да се използва при препращане и идентифициране на набора от свойства, при което идентификаторът на набора на всяко свойство се съхранява като образец (шаблон) на свойството с последователността на кода за достъп, която да бъде използвана по-късно заедно с получения избор на системни интерпретационни стойности, присвоени на избраната кодова последователност и системни интерпретационни стойности, различни от тези, присвоени на избраната кодова последователност по време на валидиране на код за достъп след идентифициране на потребител;

- Криптиране на избраните кодови системни интерпретационни стойности; и
- Съхраняване на криптирания код за достъп и образца (шаблона) на свойствата в потребителска база данни.

Методът за удостоверяване с потребителски код за достъп се състои от следните операции:

- Достъпване на база данни с потребителска информация, включваща: най-малко една предварително дефинирана кодова последователност, включваща най-малко два потребителски входни изборни параметъра, най-малко двата потребителски входни изборни параметъра, включващи най-малко две различни променливи свойства на група, включваща: изображения, буквено-цифрови знаци, символи, цветове, модели, звуци, текстури, топология, местоположение, ориентация, относителна позиция по отношение на интерактивен екранен интерфейс, при което на всяко свойство се присвоява системна интерпретационна стойност, чрез която свойството се идентифицира от системата, при което свойствата са организирани в набори от свойства, като всеки набор включва отделно групиране на свойства, които да бъдат идентифицирани като мерна единица от системата, като същевременно поддържа всяко свойство като индивидуално разпознаваемо и на всеки набор от свойства се присвоява идентификатор на набор, който да се използва при препращане и идентифициране на набора от свойства, при което идентификаторите на наборите от свойства са съхранени като образец (шаблон) на свойствата на кода за достъп;

- Генериране на произволно подреждане на входни изборни параметри, включващо свойствата на променливите от предварително дефинираните от потребителя входни изборни параметри, произволното подреждане на входните изборни параметри също включва различни от споменатите променливи свойства, които не са част от предварително дефинираните кодови входни изборни параметри, при което входните изборни параметри, които не са част от предварително дефинирания код за достъп, включват системни интерпретационни стойности, чрез които свойството се идентифицира от системата;

- Визуализиране на произволното подреждане на входните изборни параметри в интерфейса на интерактивния дисплей, при което интерфейсът на интерактивния дисплей визуализира подредба от най-малко два различни виртуални клавиша, поставени на позиции в интерфейса на интерактивния дисплей, и всеки виртуален клавиш визуализира подредба от най-малко два различни входни изборни параметри от произволното подреждане на входните изборни параметри;

- Получаване на селекция от виртуални клавиши от интерфейса на интерактивния дисплей в състоянието, в което са били показани в стъпката на визуализиране, при което системата получава всички системни интерпретационни стойности за всички входни изборни параметри, показани на избраните виртуални клавиши, включително входните изборни параметри на потребителя от предварително дефинирания код за достъп и входните изборни параметри, които не са част от предварително дефинирания код за достъп; и

- Сравняване на системните интерпретационни стойности на цялата получена селекция от виртуални клавиши на интерактивния екранен интерфейс със системните интерпретационни стойности на входните изборни параметри на предварително дефинирания код за достъп и елиминиране на всички неуспешни съвпадения за всяка позиция в кода за достъп, които не принадлежат към набора свойства, посочен в образа (шаблона) на свойството, съхранен за същата позиция в кодовата последователност, оставяйки само една съвпадаща интерпретационна стойност за всяка позиция в кодовата последователност, при което получените стойности след това се криптират и се сравняват със съхранените криптирани интерпретационни стойности.

И двата метода могат да конфигурират:

- Потребителски входни изборни параметри за конкретен потребител, позволявайки на отделните потребители да използват входни изборни параметри, независими или недостъпни за други потребители;
- Потребителски интерфейс за конкретен потребител, позволяващ на отделните потребители да използват потребителски интерфейси, независими или недостъпни за други потребители.
- Потребителски входни изборни параметри и потребителски интерфейс за конкретен потребител, позволявайки на отделните потребители да използват потребителски входни изборни параметри и комбинации на потребителски интерфейс, независими или недостъпни за други потребители.

Въпреки видимите им предимства спрямо разгледаните преди това методи за удостоверяване, методите, описани в [US 20160328552](#), са уязвими при множество наблюдения на процеса на въвеждане на код за достъп. Според самия патент, вероятността за разкриване на код за достъп е обратно пропорционална на броя на използвани набори от свойства, броя на виртуалните клавиши, дефинирани за конфигурацията на интерфейса, броя на уникалните свойства, дефинирани във всеки от наборите от свойства, и дължината на кода за достъп. Това е така, но в случай на подслушване основният влияещ фактор е броят на наблюденията и вероятността за разкриване на кода за достъп на средностатистическия потребител ще бъде доста висока в случай на множество наблюдения.

Техническа същност на изобретението

Предвид на описаното по-горе известно ниво на техниката в разглежданата област, задача на изобретението е да предложи метод за удостоверяване, който се отличава с универсалност, широка приложимост и повишена степен на сигурност (надеждност на достъпа до системата).

Задачата на изобретението се решава с метод за удостоверяване, включващ създаване на потребителски код за достъп и идентифициране с потребителски код за достъп.

Създаването на потребителски код за достъп включва:

1) Получаване на избрана кодова последователност, включваща k елемента ($E_1, E_2, \dots, E_k$) от библиотека с p елемента, разпределени според отличителното им свойство в q набора (напр. цифри, букви, специални символи, цветове, текстури, стрелки, зодиакални знаци, лога, йероглифи, картинки, снимки, други двумерни и тримерни обекти), като кодовата последователност се получава в потребителския интерфейс, при което на всеки елемент E_i ($i \in [1;k]$) се присвоява системна интерпретационна стойност VE_i ($i \in [1;k]$), чрез която елементът се идентифицира, а на всеки набор от свойства се присвоява идентификатор за идентифициране на набора, при което идентификаторът на набора, в който попада елемент E_i се съхранява като образец на свойство PE_i с кода за достъп за валидиране на кода за достъп;

2) Криптиране на последователността от системни интерпретационни стойности ($VE_1, VE_2, \dots, VE_k$) на елементите ($E_1, E_2, \dots, E_k$) от избраната кодова последователност;

3) Съхраняване на криптираната последователност H_s от системни интерпретационни стойности ($VE_1, VE_2, \dots, VE_k$) на елементите ($E_1, E_2, \dots, E_k$) от избраната кодова последователност и образца на свойствата им ($PE_1, PE_2, \dots, PE_k$) в потребителска база данни.

Идентифицирането с потребителски код за достъп включва:

1) Достъпване на база данни с потребителска информация, включваща криптираната последователност H_s от системни интерпретационни стойности ($VE_1, VE_2, \dots, VE_k$) на елементите ($E_1, E_2, \dots, E_k$) от избраната кодова последователност и образца на свойствата ($PE_1, PE_2, \dots, PE_k$);

2) Генериране и визуализиране на случайни комбинации от елементи в полета за избор F_j ($j \in [1;v]$) на екран за вход, един над друг (на отделни слоеве) или един до друг, сред които са и елементите ($E_1, E_2, \dots, E_k$) от избраната кодова последователност;

3) Получаване на селекция от полета за избор и идентифициране на елементите в тях, имащи значение за удостоверяването с помощта на съхранения образец на свойствата;

4) Криптиране на получената последователност от системни интерпретационни стойности на идентифицираните елементи;

5) Сравняване на криптираната последователност H_x със съхранената H_s и предоставяне на достъп, ако има съвпадение ($H_x = H_s$) и отказване на достъп, ако няма съвпадение ($H_x \neq H_s$).

Съгласно изобретението, при получаване на избрана кодова последователност, за всеки елемент E_i от кодовата последователност ($E_1, E_2, \dots, E_k$) се получава правило RE_i , дефинирано от потребителя, при което на всяко правило RE_i се присвоява системна интерпретационна стойност VRE_i , чрез която правилото се идентифицира, като по желание на потребителя (опционално), може да се получат и правила R_u , които не са обвързани с нито един елемент, при което на всяко правило R_u се присвоява системна интерпретационна стойност VR_u , а също така, по желание на потребителя (опционално), може да се получат и условия и начин за подаване на инструкции I_c , чрез които да се изменят елемент(и) и/или правило(а) в хода на удостоверителната сесия, при което на всяка инструкция I_c се присвоява системна интерпретационна стойност VI_c , при което системните интерпретационни стойности на правилата и условията и начина за подаване на инструкциите са съхранени в потребителската база данни, като по време на удостоверителна сесия, на случаен принцип могат да бъдат генерирани и визуализирани на екран за вход инструкции, които да променят за текущата сесия елемент(и) от избраната кодова последователност и/или правило(а), като при

идентифициране на елементите, имащи значение за удостоверяването се съблюдават инструкциите (ако са генерирани и визуализирани такива) и правилата.

Един екран за вход включва полета за избор, всяко от които съдържа два или повече елемента. Те могат да са еднакъв и/или различен брой и вид - двуизмерни, триизмерни, включително движещи се и всеки път да се визуализират на еднакъв или различен фон, или да са с еднакъв или различен цвят и форма. Формата, цвета, осветеността, прозрачността, вида, броя на елементите и полетата могат да се променят, като се запазва принципа на разполагане на повече от един елемент в едно поле за избор.

Елементите могат да бъдат цифри, букви, специални символи, цветове, текстури, стрелки, зодиакални знаци, логотипи, йероглифи, картинки, снимки, други двумерни и тримерни обекти (статични или подвижни). Могат да включват и качени от потребителя обекти, напр. лични снимки или части от тях. Броят им (n) е препоръчително да бъде достатъчно голям ($n \geq 30$).

Потребителят, по своя преценка, избира k от n елементи за тайни, а останалите ($n-k$) елементи се превръщат в примамки. Съгласно едно вариантно изпълнение на метода, във всяко поле за избор се визуализират по t елемента от t различни набора от свойства, където $t \geq 2$, за предпочитане $t = 4$ или 5 .

При всяка удостоверителна сесия, комбинирането (подреждането) на елементите в полетата за избор е различно и потребителят маркира всеки път различни полета с различни комбинации от елементи в тях, намиращи се на различни места по екрана за вход и по непонятен за обикновения наблюдател начин, с което се защитава срещу пробив в сигурността дори при наблюдение на процеса по удостоверяване. Това важи особено за варианта, при който тайните елементи служат само като отправни точки, спрямо които се прилагат правилата и/или инструкциите и не участват директно в процеса на удостоверяване. Така тайната комбинация остава невидима за обикновения наблюдател.

Съгласно едно вариантно изпълнение на метода, правило RE_i , обвързано с елемент E_i може да се зададе чрез логически модел, ползващ избрания елемент като отправна (базисна) точка, чрез формата на избрания елемент (напр. указваща посока), чрез друг елемент в полето на избрания елемент.

Съгласно едно вариантно изпълнение на метода, при избора на елементи потребителят може да зададе най-малко един логически модел, т. е. да определи най-малко една релация за най-малко един елемент, като например отнемстване, прескачане по посока, или др.

Съгласно едно вариантно изпълнение на метода, някои елементи могат да указват посока (да играят ролята на показалец).

Съгласно едно вариантно изпълнение на метода, във всяко поле за избор задължително има елемент, който е стрелка, а потребителят може да зададе за някой от своите тайни елементи правило, изискващо да се следва посоката на тази стрелка.

Съгласно едно вариантно изпълнение на метода, някои елементи, представляващи двумерни или тримерни обекти, може да са подвижни. Например ако даден таен елемент е стрелка, тя може да променя посоката си през интервал от време, като за успешно удостоверяване следва да се маркира полето, към което тя сочи в момента, в който се маркира.

Съгласно едно вариантно изпълнение на метода, отделните тайни елементи могат да бъдат обвързани с различни релации и при удостоверителна сесия потребителят може въобще да не маркира поле, в което се намира таен елемент или пък ако го маркира, то да е по съвсем друг повод. По този начин тайните елементи

могат да останат наистина тайни дори при визуално, видео или друг вид наблюдение на процеса на удостоверяване. Това гарантира наистина тайна комуникация между потребителя и устройство, система или услуга, като мотивът на потребителя за маркиране на дадено поле остава скрит за останалите.

Релации могат да определят разстояние, разположение, изместване, добавяне, отнемане, асоцииране или друга връзка или действие.

В зависимост от конкретното изпълнение на метода, потребителят се ориентира, следва или следи гласови, текстови, видео, асоциативни или други релации и/или комуникации, моделиращи и променящи идентификационния му избор.

Съгласно едно вариантно изпълнение на метода, потребителят може да настрои един или повече логически модели, които да се редуват циклично. Логическите модели могат да бъдат променяни с инструкции, което да нарушава цикличността.

Съгласно едно вариантно изпълнение на метода, правило R_n , необвързано с никой елемент е например правилото за заблуждаващи манипулации, където броят (m) и мястото (p) на тези манипулации са или константи, зададени от потребителя или променливи, определяни динамично и комуникирани по таен начин с потребителя, съгласно условия, дефинирани от потребителя. При един възможен вариант, потребителят задава броя и мястото на заблуждаващите манипулации в тайната комбинация. При друг възможен вариант, в рамките на удостоверителната сесия, потребителят получава инструкции I_c , по непонятен за обикновения наблюдател начин, относно броя заблуждаващи манипулации и евентуално мястото в тайната комбинация, на което трябва да се приложат.

Съгласно едно вариантно изпълнение на метода, правило R_n , необвързано с никой елемент е например правилото за селектирането на полетата по определен начин, за да сработи удостоверяването (напр. чрез натискане на полето само от едната страна или плъзгане в определен посока, или задържане).

Съгласно едно вариантно изпълнение на метода, едновременно с визуализирането на случайно генерирана комбинация от елементи, се визуализира и допълнителна информация, указваща промяна. Допълнителната информация (инструкция I_c) може да се визуализира на отделен ред на екрана, вкл. в полетата за избор, като използва самите елементи като указващи необходимата промяна (алгебрична, геометрична, асоциативна или друга). Може да се визуализира или излъчи и на други устройства или системи, различни от тази, чрез която се прави удостоверяването.

Промяната може да бъде и предварително уговорена под формата на „споделена тайна“, вкл. да представлява обща тайна комбинация, която е обща за повече от един потребител и която допълва или променя личната тайната комбинация на потребителите, според предварителните настройки, като споделената тайна, както и начинът на маркиране са известни само на уговорилите се потребители и не се визуализират и показват никъде.

Използването на подобни инструкции в рамките на процеса на удостоверяване повишава нивото на сигурност, предоставяйки възможност за тайна комуникация между система, устройство и потребител, при това без да изисква допълнителни ресурси или внимание, с което гарантира лесна интеграция и бърза употреба, т. е. добра използваемост.

Съгласно едно вариантно изпълнение на метода, инструкциите може да се появяват постоянно, циклично, периодично или на друг принцип, напр. географски (да се появяват с цел по-голяма сигурност

когато потребителят е извън обичайната си локация (напр. държава) или събитие (напр. да се появяват при смяна на доставчик на услуга или когато в едно поле се срещнат 2 или повече тайни елемента), както е удобно на потребителя и както настрои метода да работи.

Съгласно различни вариантни изпълнения, методът може да конфигурира:

- Потребителски елементи за конкретен потребител, позволявайки на отделните потребители да използват елементи, независими или недостъпни за други потребители;
- Потребителски интерфейс за конкретен потребител, позволяващ на отделните потребители да използват потребителски интерфейси, независими или недостъпни за други потребители.
- Потребителски елементи и потребителски интерфейс за конкретен потребител, позволявайки на отделните потребители да използват потребителски елементи и комбинации на потребителски интерфейс, независими или недостъпни за други потребители.

Удостоверяването може да се използва, за да се предостави достъп до:

- Физическо пространство, напр. офис, къща, апартамент, хотелска стая, магазин, гараж, паркинг и др.;
- Виртуално пространство, напр. уеб акаунт, място за съхранение на данни, електронна папка, виртуален портфейл или сметка и др.;
- Компютърно, мобилно или друго комуникационно или функционално устройство, напр. компютър, мобилен телефон, смарт часовник, терминал за плащане, автомобил, автомат за самообслужване, игрален автомат или конзола и др.;
- Приложения, услуги, данни и др., напр. приложения за електронно (в т. ч. мобилно) банкиране, приложения за комуникация (чат), приложения за споделяне (обмен) на файлове, приложения с виртуална или добавена реалност, удостоверителни услуги, криптирани файлове и др.

Методът за удостоверяване съгласно настоящето изобретение е приложим и работи успешно в различни физически, виртуални и операционни среди, като защитата се постига чрез комбиниране на тайни с подвеждащи елементи и неявни правила, дефинирани от логически модели, елементи, указващи посока, други елементи, начини на маркиране, заблуждаващи манипулации, които могат да бъдат променяни от скрити инструкции.

В сравнение с известното ниво на техниката, където за целите на удостоверяването се използват директно самите тайни елементи, то в предложения метод тази информация е поместена в полета за избор, с които се борави и в които се съдържат повече от един елементи и е възможно тайните елементи само да насочват кои други полета да бъдат маркирани.

Методът значително ограничава възможностите за използване на стандартни методи за проследяване на действията на потребителя чрез записване на клавишни комбинации и последователности и/или записване на движения на курсора (keyloggers), или заснемане на показанията на екрана (screen recorders), или визуално наблюдение, тъй като видимите действия не разкриват тайната комбинация. Също така методът не е уязвим за атака с груба сила (речникова атака) и не изисква използване на допълнителни устройства/ключове за сигурност от какъвто и да е вид.

Методът позволява парола с по-голяма степен на сигурност да се въвежда относително по-бързо и да се запомня много по-лесно. Без риск за сигурността може да се прилага и върху устройство, което не е

собственост на потребителя, както и на обществени места. Не прави компромиси за използваемост (за сметка на сигурността) или компромиси за сигурност (за сметка на използваемостта).

Методът може да се ползва и чрез пренос на идентификационния избор (валидната за дадената сесия последователност от полета) чрез текстово, аудио, видео или др. вид съобщение, като вместо да се назовават/посочват тайните елементи или тайната комбинация, се назовава/посочва местоположението на полетата, които биха осигурили достъп в конкретната сесия.

Различното комбиниране на елементите в полетата за избор при всяка сесия, предпазва потребителя при подслушване, особено когато той не маркира полета, в които се намират неговите тайни елементи, а други полета, указани му по начин и въз основа на принцип/принципи (алгебричен, геометричен, асоциативен или др.), известен/известни само на него.

Методът разрешава за дадена операция или за даден случай прилагане на повече от една тайни комбинации, приложени от два или повече потребителски акаунта, което позволява на повече от един потребител, достъп до обща информация, споделени ресурси и т. н. чрез неговата, неизвестна за другите участници, тайна комбинация.

Методът разрешава за дадена операция или за даден случай прилагане на споделена между двама или повече потребители тайна комбинация, обща за повече от един потребителски акаунта и допълваща или променяща тайните комбинации на потребителите, ползващи тези потребителски акаунти, което осигурява защита дори при споделяне с грешен адресат (получател).

Методът намалява когнитивното натоварване на потребителите, спомага за допускане на по-малко грешки и по-приятно изживяване.

Пояснение на приложените фигури

По-нататък в описанието са представени по-детайлно примерни изпълнения на метода за удостоверяване, които са онагледени с помощта на придружаващите описанието чертежи:

Фигура 1 - примерна библиотека с 36 елементи ($n=36$).

Фигура 2 - примерен екран за вход с 12 полета за избор ($v=12$).

Фигура 2А - примерен правоъгълен екран за вход.

Фигура 2Б - примерен кръгъл екран за вход.

Фигура 3 - примерно поле за избор с 4 елемента ($t=4$).

Фигура 4 - примерна инструкция, изнесена в модули, поместени отстрани на полетата за избор.

Фигура 5 - задаване на примерна тайна комбинация Х.

Фигура 5А - задаване на таен елемент № 1 от примерна тайна комбинация Х с избор на опцията за маркиране на таен елемент № 1.

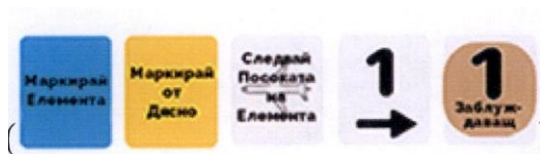
Фигура 5Б - задаване на таен елемент № 2 от примерна тайна комбинация Х с избор на опцията за ползване на логически модел.

Фигура 5В - избор на геометричен логически модел с маркиране отдясно на таен елемент № 2.

Фигура 5Г - задаване на таен елемент № 3 от примерна тайна комбинация Х с избор на опцията за следване на посоката, зададена от таен елемент № 3.

Фигура 5Д - задаване на таен елемент № 4 от примерна тайна комбинация X с избор на опцията за следване посоката на стрелката в полето за избор, в което е таен елемент № 4.

Фигура 5Е - задаване на една заблуждаваща манипулация след последния таен елемент в примерна тайна комбинация X.



Фигура 5Ж - примерна тайна комбинация X

Фигура 6 - примерни удостоверителни сесии при активирана тайна комбинация X.

Фигура 6А - примерна удостоверителна сесия 1 при активирана тайна комбинация X.

Фигура 6Б - примерна удостоверителна сесия 2 при активирана тайна комбинация X.

Фигура 7 - примерна удостоверителна сесия 3 при активирана тайна комбинация X с подробни обяснения.

Фигура 7А - примерна удостоверителна сесия 3 при активирана тайна комбинация X с подробни обяснения за стъпка 1.

Фигура 7Б - примерна удостоверителна сесия 3 при активирана тайна комбинация X с подробни обяснения за стъпка 2.

Фигура 7В - примерна удостоверителна сесия 3 при активирана тайна комбинация X с подробни обяснения за стъпка 3.

Фигура 7Г - примерна удостоверителна сесия 3 при активирана тайна комбинация X с подробни обяснения за стъпка 4.

Фигура 7Д - примерна удостоверителна сесия 3 при активирана тайна комбинация X с подробни обяснения за стъпка 5.

Фигура 8 - примерно ситуиране на повече от един таен елемент в едно поле за избор при активирана тайна комбинация X.

Фигура 9 - примерно маркиране на поле за избор повече от един път при активирана тайна комбинация X.

Фигура 10 - примерен идентификационен избор при активирана тайна комбинация X.

Фигура 11 - примерен идентификационен избор при активирана тайна комбинация X с подробни обяснения.

Фигура 12 - примерна инструкция за промяна на идентификационния избор на база замяна на таен елемент.

Фигура 13 - примерна инструкция за промяна на идентификационния избор на база промяна на броя заблуждаващи манипулации.

Фигура 14 - примерно прилагане на „споделена тайна“ от няколко потребителя.

Фигура 15 - примерно дефиниране на алгебричен логически модел.

Фигура 16 - примерно дефиниране на асоциативен логически модел.

Фигура 17 - примерно дефиниране на персонализиран логически модел.

Фигура 18 - примерна удостоверителна сесия 1 при активирана тайна комбинация Y, илюстрираща как тайните елементи могат да останат тайни дори при визуално, видео или друг вид наблюдение на процеса на удостоверяване.

Фигура 19 - примерна удостоверителна сесия 2 при активирана тайна комбинация Y, илюстрираща как тайните елементи могат да останат тайни дори при повторно визуално, видео или друг вид наблюдение на процеса на удостоверяване.

Примери за изпълнение на изобретението

По-нататък в описанието ще бъде представено едно примерно изпълнение на метода за удостоверяване, като описаната последователност от операции и характеризиращите ги параметри могат да бъдат приложени в различни вариантни изпълнения и модификации, като се използват цифри, букви, специални символи, цветове, текстури, стрелки, зодиакални знаци, логотипи, йероглифи, картинки, снимки, други двумерни и тримерни обекти, или части от тях, чието групиране, подреждане и комбиниране в полета за избор, има еквивалентно действие или функционално предназначение и осигурява описания полезен ефект от използването на метода. В този смисъл примерното изпълнение на метода трябва да се разглежда и тълкува за илюстрация на идеята на предложеното техническо решение, което не ограничава използването и на други вариантни изпълнения. Аспекти на настоящото изобретение са описани във връзка с прилагане на метода съгласно примерните изпълнения на изобретението. Трябва да се разбере, че всеки екран за вход, всяко поле за избор, всички елементи в тях и техните комбинации, могат да се прилагат чрез четене на програмни инструкции от компютър или друго устройство.

Следващото описание е представено, за да даде възможност на всеки специалист в областта да направи и използва изпълненията и е предоставено в контекста на конкретно приложение и неговите изисквания. Общите принципи, дефинирани тук, могат да бъдат приложени към други изпълнения и приложения, без да се отклоняват от духа и обхвата на настоящите изпълнения. По този начин на различните изпълнения трябва да се предостави най-широк обхват в съответствие с принципите и характеристиките, разкрити тук. Въпреки че настоящото изобретение е разкрито чрез позоваване на предпочитаните изпълнения и примери, трябва да се разбере, че тези примери са предназначени в илюстративен, а не в ограничаващ смисъл.

Терминологията, използвана по-нататък в описанието е за целите на поясняване на описанието на конкретните изпълнения и не е предназначена да ограничава изобретението. Термините, използвани тук, обикновено имат своите обичайни значения в областта. В случай на противоречие, настоящият документ, включително всички определения, дадени тук, ще имат предимство. Едно и също нещо може да бъде изразено по повече от един начин. Алтернативен език и синоними могат да се използват за всеки термин(и), обсъждан(и) тук, и не трябва да се придава специално значение на това дали даден термин е разработен или обсъждан тук. Съображение на един или повече синоними не изключва използването на други синоними. Формите за единствено число са предназначени да включват множество форми, освен ако контекстът ясно не посочва друго. Термините „включва“ и/или „включващ“, когато се използват в това описание, задават наличието на посочените характеристики, цели числа, стъпки, операции, елементи и/или компоненти, но не изключват присъствието или добавяне на една или повече други функции, цели числа, стъпки, операции, елементи, компоненти и/или групи от тях.

Терминът „работна система“ означава компютърна система, компютърно устройство, мобилно комуникационно устройство, система за разплащания, система за контрол на достъпа до сгради, офиси, помещения или друга система или устройство, изискващи удостоверяване при влизане.

Терминът „елемент“ означава обект, който системата предлага за ползване в процеса на удостоверяване на потребител в дадена работна система. Елементите могат да представляват цифри, букви, специални символи, цветове, текстури, стрелки, зодиакални знаци, лога, йероглифи, картинки, снимки, други двумерни и тримерни обекти (напр. изобразените във фиг. 1). Методът допуска избраните елементи да са еднакви или различни по вид, да се отличават по големина, цвят, растер, посока и т. н. Основната им цел е да дадат възможност на потребителя да си избере лесно разпознаваеми и запомнящи се тайни елементи.

Терминът „таен елемент“ означава елемент, избран от потребителя при създаването на код за достъп за нуждите на удостоверяването. В различни ситуации, като заместители на този термин могат да бъдат използвани „избран елемент“ и „елемент от тайната комбинация“. Тайните елементи се избират от библиотеката с елементи (фиг. 1), както е показано на фигура 5. При откриване на удостоверителна сесия, потребителят следва да маркира полетата за избор, определени от тайните елементи и правилата. Ако потребителят предварително е избрал да работи не с един, а с набор от тайни елементи, то може да се окаже че в дадена сесия ще се наложи да маркира дадено поле за избор повече от един път (фиг. 9).

Терминът „елемент, имащ значение за удостоверяването“ означава елемент, рефериран от актуалните инструкции и правила като потенциален таен елемент.

Терминът „екран за вход“ (фиг. 2) обозначава работната зона на екрана, в която са поместени полетата за избор (фиг. 3). Той може да съдържа и инструкции към потребителя (фиг. 4). В него се поместват и всички останали функционални области и части, необходими на системата, като например:

-  бутон за опресняване
-  бутон за изчистване
-  бутон за връщане
-  бутон за вход и брояч на маркиранията.

Може да бъде с различна форма напр. правоъгълна (фиг. 2А), кръгла (фиг. 2Б), многоъгълна.

Терминът „поле за избор“ (фиг. 3) обозначава част от екрана за вход (фиг. 2), в която е поместена една група от елементи. В различни ситуации, като заместители на този термин могат да бъдат използвани „поле за въвеждане“, „виртуален клавиш“, „плочка“. Полето може да е определено с ясни граници, местоположение и очертания, но може и да не е ясно очертано и конкретно локализирано. Основна негова функция е да групира на едно място тайни и подвеждащи елементи. В дадена сесия, потребителят следва да маркира полетата за избор, определени от тайните елементи и правилата (фиг. 5), или съобразно инструкциите (фиг. 4).

Във всяко поле за избор елементите следва да са повече от един ($t \geq 2$). По този начин причината (поводът), поради която потребителят маркира дадено поле за избор остава неясен за другите, които наблюдават или записват действията му в рамките на удостоверителната сесия. В резултат - ако трето лице използва шпионски софтуер или наблюдава удостоверителната сесия, то няма да може да разбере защо потребителят го маркира.

Полетата за избор в екрана за вход може да имат постоянна форма, местоположение, големина и очертания или параметри, които са зададени за дадена удостоверителна сесия. Съгласно едно предпочитано изпълнение на метода, размерът и формата на екрана за вход и полетата за избор са съобразени с конкретното потребителско устройство. Съгласно някои вариантни изпълнения, отделните потребители могат да използват потребителски елементи и/или комбинации на потребителски интерфейс, независими или недостъпни за други потребители.

Основното предназначение на полето за избор е да даде възможност на потребителя да открие в него свой таен елемент или да разпознае инструкциите му. Така той се ориентира дали да маркира полето, в което се намира тайният елемент или да извърши друго действие - да маркира друго поле, въз основа на предварително дефинираните правила или получените инструкции.

Терминът „свойство“ обозначава отличителна характеристика на елемента. Групата от елементи, отличаващи се със свойството PE_i се нарича набор (множество) от клас PE_i , напр. изобразените на фигура 1 елементи „оранжев“, „лилав“, „зелен“, „червен“, „розов“, „син“ и т. н. са множество от клас „Цветове“; елементите „куче“, „коктейл“, „роза“, „земя“, „монета“, „детелина“ и т. н. са множество от клас „Картинки“; елементите 1, 2, 3, 4, 5, 6 и т. н. са множество от клас „Числа“.

Терминът „правило“ означава принцип на действие, дефиниран от логически модел, от формата на елемента (напр. елемент, който чрез формата си указва посока), от друг елемент в полето на изборния елемент, от заблуждаваща манипулация, от начин на маркиране (напр. натискане само от едната страна на полето или плъзгане в определен посока, или задържане за известно време).

Терминът „тайна комбинация“ означава последователността от тайни елементи и правила (фиг. 5Ж).

При вариантни изпълнения на метода, елементите в полето за избор може да визуализират на слоеве или един до друг (фиг. 3).

Терминът „удостоверителна сесия“ (фиг. 6, 7, 18, 19) обхваща съвкупността от действия, които се извършват от потребителя, в рамките на предварително определен период от време, за удостоверяване или вход в дадена услуга, устройство или система, или по отношение на дадена информация. След всеки неуспешен опит за удостоверяване, удостоверителната сесия се закрива и потребителят трябва да открие нова сесия, в чието времетраене да въведе валидния за съответната сесия идентификационен избор.

Терминът „инструкция“ означава указание, изискващо определени действия спрямо таен елемент или правило, в рамките на дадена удостоверителна сесия. Инструкцията определя реда и начина на промяна на таен елемент или правило, без да е разбираема за околните.

Инструкциите може да са поместени в специално обособени зони, например по периферията на екрана за вход (фиг. 4), както и в полетата за избор. Възможно е и друго вариантно изпълнение, при което самите елементи или част от тях да служат като инструкции за действие в рамките на дадена удостоверителна сесия. Условието и начина за подаване на инструкциите са зададени предварително в настройките на системата или устройството, ако съответната система и устройство позволяват такива инструкции да бъдат изпълнени (фиг. 12 и 13).

Инструкциите се дават от системата и може да са видими в полетата за избор или в отделен модул (фиг. 4), устройство или система. Чрез тях потребителят се информира за необходимите действия в рамките на дадена удостоверителна сесия.

Инструкциите може да са замаскирани, като за целта се използват самите елементи. Действията на потребителя в зависимост от конкретните инструкции могат да са базирани на различни принципи (алгебричен, геометричен, асоциативен, или др.), които предварително са настроени от потребителя.

Терминът „модул за инструкции“ се отнася до мястото в екрана за вход, в което потребителят получава указанията на системата. В него освен указания може да се появява и заблуждаваща информация.

Терминът „споделена тайна“ означава тайната комбинация предварително уговорена между няколко потребителя. Споделената тайна допълва или променя тайните комбинации на потребителите, като не се визуализира и показва никъде, оставайки известна само на тях. В дадена удостоверителна сесия, спрямо дадена операция, за да се постигне успешно удостоверяване, всеки потребител трябва да приложи собствената си тайна комбинация плюс споделената тайна (фиг. 14). Това може да стане на една стъпка като се ползва комбинация от собствената тайна комбинация и споделената тайна, или на няколко стъпки, като първо се направи идентификационен избор базиран на едната тайна комбинация, а после идентификационен избор базиран на другата тайна комбинация, която е споделената тайна комбинация.

Терминът „логически модел“ определя логическа връзка (релация), зададена на алгебричен, геометричен, асоциативен или персонализиран принцип, използвайки операции като събиране (+), изваждане (-), умножение (x), деление ($\div$), изместване (Δx), конюнкция ($\wedge$), дизюнкция ($\vee$), отрицание ($\neg$), изключваща дизюнкция ($\underline{\vee}$), импликация ($\Rightarrow$), двойна импликация ($\Leftrightarrow$). Например, ако логическият модел е определил изместване с едно поле вдясно, то следва да се маркират полето, вдясно от това, в което е тайният елемент.

Терминът „заблуждаващи манипулации“ се отнася до нищо не значещите, камуфлажни, фалшиви манипулации, например кликания върху екрана за вход, които се извършват от потребителя за заблуда на злонамерени наблюдатели. Техният брой в дадена удостоверителна сесия може да е предварително фиксиран или да се указва от системата чрез елементите или чрез допълнителни модули и полета в екрана за вход.

Терминът „начин на маркиране“ най-общо казано означава модел на селектиране на полетата за избор. Залага се предварително от потребителя в системата и ако не бъде спазен, независимо че бъдат спазени всички други условия, удостоверяването няма да бъде успешно. Примери за начин на маркиране са плъзгане, частично маркиране, странично маркиране, задържане при маркиране. Моделът може да се активира от системата при определени условия, за което да се информира потребителя чрез тайни инструкции в специално обособени зони на екрана за вход или чрез самите елементи, полета за избор, тяхната форма, местоположение, отстояние и т. н., както и чрез допълнителни визуални или аудио средства в екрана за вход или извън него, вкл. в други устройства или системи.

Идентификационен избор (фиг. 10, 11) е действието на потребителя, в екрана за вход, в дадена удостоверителна сесия, което е базирано на тайната комбинация и отчита активните инструкции и правила. Идентификационният избор е съчетание и съвкупност от:

- 1) Идентифициране на полетата, в които се намират тайните елементи;
- 2) Спазване на активните инструкции, ако има такива;
- 3) Спазване на активните правила.

Всички те могат да доведат до специфични манипулации по полетата за избор, по екрана за вход, по части от него, както и до пропускане или повторяемост на дадено действие. Например в една удостоверителна сесия е възможно дадено поле за избор да се маркира повече от един път, защото в него може да има повече от един таен елемент (фиг. 8) и по тази причина потребителят да маркира два или повече пъти въпросното поле за избор, или защото дадено поле е посочено за маркиране от инструкциите в дадена удостоверителна сесия или пък от дадено правило (фиг. 9).

Валидният идентификационен избор осигурява достъп.

Идентификационният избор може да бъде съобщен чрез назоваване/посочване на местоположението на полетата, които биха осигурили достъп в конкретната сесия. Например при удостоверителната сесия, показана на фигура 6А, назоваването/посочването ще бъде от вида: натисни поле 9, после натисни поле 0, после натисни поле 5, после натисни поле 4, накрая натисни поле *. При следваща сесия тайните елементи ще бъдат разположени по различен начин и идентификационният избор няма да е същият. При показаната на фигура 6Б сесия, назоваването/посочването ще бъде от вида: натисни поле 8, после натисни поле 6, после натисни поле *, после натисни поле 2, накрая натисни поле 9.

Методът за удостоверяване включва провеждане на операции в последователност както следва:

При създаване на потребителски код за достъп:

1) Получаване на избрана кодова последователност, например включваща 4 елемента (E_1, E_2, E_3, E_4) от библиотека с 36 елемента, разпределени според отличителното им свойство в 3 набора (цветове, картинки, цифри), като кодовата последователност се получава в потребителския интерфейс (напр. както е показано на фиг. 5), при което на всеки елемент E_i ($i \in [1;4]$) се присвоява системна интерпретационна стойност VE_i ($i \in [1;4]$), чрез която елементът се идентифицира (за $E_1 = \text{син}$, $VE_1 = \text{Blue}$; за $E_2 = \text{оранжево}$, $VE_2 = \text{Orange}$; за $E_3 = \text{самолет}$, $VE_3 = \text{Airplane}$; за $E_4 = 1$, $VE_4 = \text{One}$), а на всеки набор от свойства се присвоява идентификатор за идентифициране на набора, при което идентификаторът на набора, в който попада елемент E_i от кодовата последователност се съхранява като образец на свойство PE_i с кода за достъп за валидиране на кода за достъп ($PE_1 = \text{color}$; $PE_2 = \text{color}$; $PE_3 = \text{picture}$; $PE_4 = \text{digit}$), като за всеки елемент E_i от кодовата последователност (E_1, E_2, E_3, E_4) се получава правило RE_i , при което на всяко правило RE_i ($i \in [1;4]$) се присвоява системна интерпретационна стойност VRE_i ($i \in [1;4]$), чрез която правилото се идентифицира (за $PE_1 = \text{маркирайте елемента}$ (фиг. 5А), $VRE_1 = \text{MarkTheElement}$; за $PE_2 = \text{следвайте геометричен логически модел}$ (фиг. 5Б) с изместване 1 поле вдясно (фиг. 5В), $VRE_2 = \text{RightRelation}$; за $PE_3 = \text{следвайте посоката на елемента}$ (фиг. 5Г), $VRE_3 = \text{FollowTheElement}$; за $PE_4 = \text{следвайте посоката на стрелката, в долната част на полето, в което попадне елементът}$ (фиг. 5Д), $VRE_4 = \text{FollowTheArrow}$), като по желание на потребителя може да се получат и правила R_u , които не са обвързани с нито един елемент, напр. заблуждаващи манипулации, където броят (m) и мястото (p) на тези манипулации са константи, зададени от потребителя (напр. $m = 1$ и $p = 4+1 = 5$), т. е. $R_1 = 1$ заблуждаваща манипулация след последния таен елемент (фиг. 5Е), $VR_1 = \text{IfFalseClickAfter}$.

При друг вариант броят (m) и мястото (p) са променливи, определяни динамично и комуникирани по таен начин е потребителя, съгласно условия, дефинирани от потребителя (напр. както е показано на фиг. 12 и 13).

Също така, по желание на потребителя, може да се получат и условия и начин за подаване на инструкции I_c , чрез които да се изменят елемент(и) и/или правило(а) в хода на удостоверителната сесия (напр. I_1 със същия цвят като цвета на елемента, както е показано на фиг. 12, $VI_1 = \text{SameColor}$, I_2 със червен цвят в елипсовидно бежово поле, както е показано на фиг. 13, $VI_2 = \text{RedBeigeEllipse}$).

2) Криптиране на последователността от системни интерпретационни стойности (VE_1, VE_2, VE_3, VE_4) на елементите (E_1, E_2, E_3, E_4) от избраната кодова последователност (напр. SHA256 хеширане на $\text{BlUeOrAnGeAiRpLaNeArRoWOnEnUmBeR}$);

3) Съхраняване на криптираната последователност

H_s (6ceee8700221bf8c4a20858489422f7bbbd9768737f03c9e709e8bc874852699) от системни интерпретационни стойности (VE_1, VE_2, VE_3, VE_4) на елементите (E_1, E_2, E_3, E_4) от избраната кодова последователност и образа на свойствата им (PE_1, PE_2, PE_3, PE_4) т. е. (Цвят, Цвят, Картинка, Цифра), както и системните интерпретационни стойности на правилата ($VRE_1, VRE_2, VRE_3, VRE_4, VR_1$), т. е. (MarkTheElement, RightRelation, FollowTheElement, FollowTheArrow, 1FalseclickAfter) в потребителска база данни.

Ако са получени условия и начин за подаване на инструкциите (VI_1, VI_2), т. е. (SameColor , RedBeigeEllipse), те също се съхраняват.

При идентифициране с потребителски код за достъп:

достъпване на база данни с потребителска информация, включваща криптираната последователност H_s от системни интерпретационни стойности (VE_1, VE_2, VE_3, VE_4) на елементите (E_1, E_2, E_3, E_4) от избраната кодова последователност и образа на свойствата (PE_1, PE_2, PE_3, PE_4), както и системните интерпретационни стойности на правила ($VRE_1, VRE_2, VRE_3, VRE_4, VR_1$).

Ако са съхранени условия и начин за подаване на инструкциите (VI_1, VI_2), то се осигурява достъп и до тях.

2) Генериране и визуализиране на случайни комбинации от елементи в полета за избор F_j ($j \in [1;12]$) на екран за вход (напр. както е показано на фиг. 7), сред които са и елементите (E_1, E_2, E_3, E_4) от избраната кодова последователност.

Ако са съхранени условия и начин за подаване на инструкции, се генерират и визуализират и случайни комбинации от инструкции (напр. както е показано на фиг. 12 и 13), които да променят елемент(и) от избраната кодова последователност (напр. както е показано на фиг. 12, I_1 изменя за дадената удостоверителна сесия първият елемент (E_1) от „син“ на „б“ и/или да променят правило (а) (напр. както е показано на фиг. 13, I_2 изменя за дадената удостоверителна сесия правило R_1 от „1 заблуждаваща манипулация след последния таен елемент“ на „3 заблуждаващи манипулации след последния таен елемент“).

3) Получаване на селекция от полета за избор (напр. както е показано на фиг. 7: първо поле 0 (защото е със син фон) (фиг. 7А), после поле 3 (защото е отдясно на полето с оранжев фон) (фиг. 7Б), после поле 0 (защото към него сочи самолетът) (фиг. 7В), после поле 4 (защото към него сочи стрелката в поле 1) (фиг. 7Г) и накрая произволно поле (в случая поле 5) (фиг. 7Д) и идентифициране на елементите в тях, имащи значение за удостоверяването (в случая: син, оранжев, самолет, 1) чрез съблюдаване на инструкциите и правилата и с помощта на образа на свойствата, съхранен в базата данни с потребителска информация.

В примера на фигура 12 е показана инструкцията със син цвят за промяна на тайния елемент „син“. Съгласно тази инструкция, в началото, вместо да се селектира поле 0, където е синият фон, се селектира поле 6, тъй като това е числото, зададено от инструкцията със същия син цвят.

В примера на фигура 13 е показана инструкцията със червен цвят за промяна на броя заблуждаващи манипулации. Съгласно тази инструкция, накрая, вместо да се селектира 1 произволно поле, се селектират 3 произволни полета.

4) Криптиране на получената последователност от системни интерпретационни стойности (BIUeOrAnGeAiRpLaNeArRoWOnEnUmBeR) на идентифицираните елементи (син, оранжев, самолет, 1);

5) Сравняване на криптираната последователност

H_x (6ceee8700221bf8c4a20858489422f7bbbd9768737f03c9e709e8bc874852699) със съхранената H_s (6ceee8700221bf8c4a20858489422f7bbbd9768737f03c9e709e8bc874852699) и предоставяне на достъп, тъй като има съвпадение ($H_x=H_s$).

Съгласно едно примерно изпълнение, при заключване (кодиране) на електронно съобщение или файл, методът допуска потребителят да се верифицира и по същество да заключи информацията със своя лична тайна комбинация, а потребителят, който получава информацията, да се верифицира и по същество да отключи подадената към него информация с идентификационен избор базиран на неговата собствена тайна комбинация, която е различна и неизвестна за подателя на информацията и за всички останали.

Съгласно друго вариантно изпълнение, освен собствените си тайни комбинации, потребителите могат да ползват и обща споделена тайна комбинация (напр. елемент „червен“ с правило „маркирай елемента“ и елемент „6“ с правило „маркирай елемента“, както е показано на фиг. 14). По този начин се намалява риска от разкриване на чувствителна информация с грешен адресант. В този случай, ако дадено съобщение се изпрати случайно към грешен адресант (получател), той няма да е способен да го отключи с идентификационен избор, базиран само на личната си тайна комбинация тъй като няма да знае „споделената тайна“.

Възможни са вариантни изпълнения, при които правила се дефинират чрез алгебричен, геометричен, асоциативен или персонализиран логически модел.

Фигура 15 представя алгебричен логически модел, при който за елемент „оранжев“ се дефинира правило за събиране на номера на полето за избор, в което се намира елемента с числото 4 и маркиране на поле(та) за избор с номер(а), отразяващи резултата от събирането. В конкретния пример, на екрана за вход елемент „оранжев“ се намира в поле за избор с номер 9, събирането на 9 с 4 дава 13, поради което се извършва маркиране на 2 полета за избор - първо поле за избор с номер 1 и след това поле за избор с номер 3.

Фигура 5B представя геометричен логически модел, при който, за елемент „оранжев“ се дефинира изместване ($\Delta x = +1$), т. е. изместване едно поле вдясно. При този вариант, по време на удостоверяване, вместо да се маркира полето за избор с оранжев фон, се маркира полето за избор, което е отдясно. В примера на екрана за вход, представен на фигура 7B, елемент „оранжев“ се намира в поле за избор с номер 2, поради което се извършва маркиране на поле за избор с номер 3 (намиращо се отдясно).

Фигура 16 представя асоциативен логически модел, при който, за елемент „детелина“ се дефинира правило за 4 заблуждаващи манипулации в случай, че в полето за избор, в което попадне елемента са намира

и цифрата 4, като се разчита на по-лесното запомняне поради асоцииране на „четирилистна детелина“ и 4 с 4 заблуждаващи манипулации.

Фигура 17 представя персонализиран логически модел, при който, за елемент „оранжев“ се дефинира правило за следване на посоката на елемент „показалец“, ако двата елемента попаднат в едно и също поле за избор; за 4 заблуждаващи манипулации в случай, че елемент „оранжев“ и елемент „детелина“ или елемент „4“ попаднат в едно и също поле за избор и за маркиране на полето за избор, в което попадне елемент „оранжев“ във всички останали случаи. В първия изобразен случай, елемент „оранжев“ е в едно и също поле за избор с елемент „показалец“ (поле за избор #), затова вместо да се маркира полето за избор, в което се намира тайния елемент, се маркира полето за избор, към което сочи тайния елемент, т. е. следва се посоката на показалеца и се маркира поле за избор с номер 9. Във втория изобразен случай, елемент „оранжев“ е в едно и също поле за избор с елемент „4“, затова се извършват 4 заблуждаващи манипулации. В третия изобразен случай, елемент „оранжев“ не е заедно нито с елемент „показалец“, нито с елемент „детелина“, нито с елемент „4“, затова се маркира полето за избор, в което е попаднал елемент „оранжев“ (поле за избор с номер 1).

Фигура 5Д представя логическия модел, при който, за елемент „1“ се дефинира правило за следване на посоката на стрелката. В примера на екрана за вход, представен на фигура 7Г, елемент „1“ е заедно със стрелка, сочеща надолу, поради което се маркира поле за избор с номер 4, намиращо се отдолу.

Методът позволява и вариантното изпълнение, в което, при забравена тайна комбинация, задава на потребителя предварително формулирани от него насочващи въпроси, за да му помогне да си спомни тайната комбинация. Това става по таен за околните начин, напр. чрез слушалки, на които само потребителят чува въпросите. При неуспех на потребителя да си спомни тайната комбинация, му се дава възможност да си въведе нова тайна комбинация, която обаче, за да стане активна, трябва да бъде потвърдена от друг потребител, с който даденият потребител е имал „споделена тайна“, чрез въвеждането на „споделената тайна“ от другия потребител, в рамките на определен период от време след заявката за промяна.

За разлика от методите, при които потребителят задава постоянен ПИН, при разглеждания метод на удостоверяване мястото и/или броя на манипулациите се мени, което увеличава многократно сигурността.

При успешно изпълнение на метода, системата разрешава достъп на потребителя. При неуспешно изпълнение, на екрана се визуализира съобщение за грешка, потребителската сесия се закрива, при което потребителя може да стартира нова сесия, в която елементите се смесват наново. След определен брой неуспешни опити е възможно достъпът на потребителя да бъде частично или изцяло блокиран.

В примерните изпълнения, представени на фигурите, всички описани признаци (операции) са изобразени и/или генерирани на случаен принцип, за дадена удостоверителна сесия и са били валидни за определен период от време, след изтичане на който вече не са актуални, съответно удостоверяването на потребител чрез преповтарянето им е невъзможно.

Патентни претенции

1. Метод за удостоверяване, включващ създаване на потребителски код за достъп чрез получаване на избрана кодова последователност, включваща k елемента ($E_1, E_2, \dots, E_k$) от библиотека с n елемента, разпределени според отличителното им свойство в q набора (напр. цифри, букви, специални символи, цветове, текстури, стрелки, зодиакални знаци, логотипи, йероглифи, картинки, снимки, други двумерни и тримерни обекти), като кодовата последователност се получава в потребителския интерфейс, при което на всеки елемент E_i ($i \in [1;k]$) се присвоява системна интерпретационна стойност VE_i ($i \in [1;k]$), чрез която елементът се идентифицира, а на всеки набор от свойства се присвоява идентификатор за идентифициране на набора, при което идентификаторът на набора, в който попада елемент E_i се съхранява като образец на свойство PE_i с кода за достъп за валидиране на кода за достъп; криптиране на последователността от системни интерпретационни стойности ($VE_1, VE_2, \dots, VE_k$) на елементите ($E_1, E_2, \dots, E_k$) от избраната кодова последователност; съхраняване на криптираната последователност H_s от системни интерпретационни стойности ($VE_1, VE_2, \dots, VE_k$) на елементите ($E_1, E_2, \dots, E_k$) от избраната кодова последователност и образеца на свойствата им ($PE_1, PE_2, \dots, PE_k$) в потребителска база данни, а също така включващ идентифициране с потребителски код за достъп чрез достъпване на база данни с потребителска информация, включваща криптираната последователност H_s от системни интерпретационни стойности ($VE_1, VE_2, \dots, VE_k$) на елементите ($E_1, E_2, \dots, E_k$) от избраната кодова последователност и образеца на свойствата ($PE_1, PE_2, \dots, PE_k$); генериране и визуализиране на случайни комбинации от елементи в полета за избор F_j ($j \in [1;v]$) на екран за вход, един над друг (на отделни слоеве) или един до друг, сред които са и елементите ($E_1, E_2, \dots, E_k$) от избраната кодова последователност; получаване на селекция от полета за избор и идентифициране на елементите в тях, имащи значение за удостоверяването с помощта на съхранения образец на свойствата; криптиране на получената последователност от системни интерпретационни стойности на идентифицираните елементи; сравняване на криптираната последователност H_x със съхранената H_s и предоставяне на достъп, ако има съвпадение ($H_x = H_s$) и отказване на достъп, ако няма съвпадение ($H_x \neq H_s$), характеризиращ се с това, че при получаване на избрана кодова последователност, за всеки елемент E_i от кодовата последователност ($E_1, E_2, \dots, E_k$) се получава **правило RE_i** , дефинирано от потребителя, при което на всяко **правило RE_i** се присвоява системна интерпретационна стойност **VRE_i** , чрез която **правило** се идентифицира, като по желание на потребителя (опционално), може да се получат и **правила R_n** , които не са обвързани с нито един елемент, при което на всяко **правило R_n** се присвоява системна интерпретационна стойност **VR_n** , а също така, по желание на потребителя (опционално), може да се получат и условия и начин за подаване на **инструкции I_c** , чрез които да се изменят **елемент(и)** и/или **правило(а)** в хода на удостоверителната сесия, при което на всяка **инструкция I_c** се присвоява системна интерпретационна стойност **VI_c** , при което системните интерпретационни стойности на **правилата** и условията и начина за подаване на **инструкциите** са съхранени в потребителската база данни, като по време на удостоверителна сесия, на случаен принцип могат да бъдат генерирани и визуализирани на екран за вход **инструкции**, които да променят за текущата сесия **елемент(и)** от избраната кодова последователност и/или **правило(а)**, като при идентифициране на елементите, имащи значение за удостоверяването се съблюдават **инструкциите** (ако са генерирани и визуализирани такива) и **правилата**.

2. Метод съгласно претенция 1, характеризиращ се с това, че най-малко едно **правило** се задава чрез **логически модел**, който ползва като отправна точка даден таен елемент.
3. Метод съгласно претенция 1, характеризиращ се с това, че най-малко едно **правило** се задава чрез **таен елемент тип показалец** (елемент, който чрез формата си указва посока).
4. Метод съгласно претенция 1, характеризиращ се с това, че във всяко поле за избор задължително има елемент, който е стрелка, а потребителят задава за най-малко един от своите тайни елементи **правило**, **изискващо да се следва посоката на тази стрелка**.
5. Метод съгласно претенция 1, характеризиращ се с това, че най-малко едно правило се задава чрез **m заблуждаващи манипулации**, където **m** е константа, определена от потребителя.
6. Метод съгласно претенция 1, характеризиращ се с това, че най-малко едно **правило** се задава чрез **m заблуждаващи манипулации**, където **m** е променлива, определена от системата на случаен принцип и комуникирана по таен начин с потребителя.
7. Метод съгласно претенция 1, характеризиращ се с това, че най-малко едно правило се задава чрез **начин на маркиране** (напр. плъзгане, частично маркиране, странично маркиране, задържане).
8. Метод съгласно претенция 1, характеризиращ се с това, че **инструкциите** се подават от тайните елементи.
9. Метод съгласно претенция 1, характеризиращ се с това, че **инструкциите** се подават от някой от останалите елементи в полето за избор, в което се намира даден таен елемент.
10. Метод съгласно претенция 1, характеризиращ се с това, че **инструкциите** се подават от елементи, извън полетата за избор.
11. Метод съгласно претенция 1, характеризиращ се с това, че **инструкциите** се подават чрез текстови, аудио и/или видео съобщения.
12. Метод съгласно претенция 1, характеризиращ се с това, че по **t** елемента от **t различни набора от свойства** се визуализират във всяко поле за избор.
13. Метод съгласно претенция 1, характеризиращ се с това, че **полетата за избор (F_i)** се генерират и визуализират автоматично, като техният брой, размер и форма се адаптират към техническите параметри на екрана за вход на устройството, използвано за удостоверяване.
14. Метод съгласно претенция 2, характеризиращ се с това, че **логическият модел** определя логическа връзка (релация), зададена на алгебричен, геометричен, асоциативен или персонализиран принцип, използвайки операции като събиране (+), изваждане (-), умножение (x), деление ($\div$), изместване (Δx), конюнкция ($\wedge$), дизюнкция ($\vee$), отрицание ($\neg$), изключваща дизюнкция ($\underline{\vee}$), импликация ($\Rightarrow$), двойна импликация ($\Leftrightarrow$).
15. Метод съгласно претенция 2, характеризиращ се с това, че за **всички елементи** от кодовата последователност се задава **общовалидно правило** чрез един общ **логически модел**.
16. Метод съгласно претенция 2, характеризиращ се с това, че **логическият модел** задава релации за полетата за избор, в които се намират тайните елементи.
17. Метод съгласно претенция 2, характеризиращ се с това, че **логическият модел** задава релации за полета за избор, в които не се намират тайни елементи.

18. Метод съгласно претенция 2, характеризиращ се с това, че **логическият модел** може да се променя циклично, случайно, периодично, на географски или събитийен принцип.

19. Метод съгласно претенция 6, характеризиращ се с това, че броят на необходимите **заблуждаващи манипулации** (m) се указва от някой от останалите елементи в полето за избор, в което се намира даден таен елемент.

20. Метод съгласно претенция 6, характеризиращ се с това, че мястото (p) за прилагане на **заблуждаващи манипулации** се указва от някой от останалите елементи в полето за избор, в което се намира даден таен елемент.

21. Метод съгласно претенция 1 ÷ 20, характеризиращ се с това, че при криптиране на съобщения или файлове, **ключът за криптиране се генерира чрез криптографско преобразуване на съхранената криптирана последователност (H_s) на приемащото устройство (акаунт)**, като по този начин само съответното приемащо устройство (акаунт) може да декриптира изпратено до него съобщение или файл.

22. Метод съгласно претенция 21, характеризиращ се с това, че при криптиране на съобщения или файлове, **ключът за криптиране се генерира чрез криптографско преобразуване на комбинация от съхранената криптирана последователност (H_s) на приемащото устройство (акаунт) и предварително съхранено споделено криптографско съдържание**, достъпно както за изпращащото устройство (акаунт), така и за приемащото устройство (акаунт).

23. Метод съгласно претенция 1 ÷ 22, характеризиращ се с това, че при забравена тайна комбинация, в работната система се излъчва (възпроизвежда) поредица от предварително записани текстови, аудио и/или видео съобщения, съдържащи **кодирана информация за тайната комбинация**.

24. Метод съгласно претенция 23, характеризиращ се с това, че излъчването става по предварително зададен **защитен комуникационен канал**.

25. Метод съгласно претенция 23, характеризиращ се с това, че при забравена кодова последователност допуска нулиране (избор на нова), като **активирането на новата кодова последователност се извършва след допълнително удостоверяване, включващо идентификационния избор на второ, предварително определено устройство (акаунт)**, в рамките на определен период от време след заявката за промяна.

26. Метод съгласно претенция 3, характеризиращ се с това, че елементите тип показалец **автоматично променят посоката си** на екрана за вход през предварително дефинирани времеви интервали по време на удостоверителната сесия, като текущата им посока автоматично се отчита при формиране на идентификационния избор.

27. Метод съгласно претенции 1 ÷ 26, характеризиращ се с това, че при създаването на кодова последователност, всяко устройство (акаунт) добавя **персонализирани елементи към библиотеката**, като добавените елементи се съхраняват в потребителската база данни и са достъпни единствено при последващо удостоверяване от същото устройство (акаунт).

28. Метод съгласно претенции 1 ÷ 26, характеризиращ се с това, че при създаването на кодова последователност, **интерфейсът на екрана за вход се конфигурира индивидуално за всяко устройство (акаунт)** с уникални характеристики като оформление, визуални теми или подредба на полетата, като конфигурацията за дадено устройство (акаунт) се съхранява в потребителската база данни и се прилага при всяка следваща удостоверителна сесия на това устройство (акаунт).

29. Метод съгласно претенции 1 ÷2 6, характеризиращ се с това, че при създаването на кодова последователност, всяко устройство (акаунт) **едновременно дефинира персонализирани елементи за библиотеката и индивидуални характеристики за интерфейса на екрана за вход**, като комбинацията за дадено устройство (акаунт) се съхранява и е достъпна единствено за това устройство (акаунт).

Приложение: 19 фигури



Фиг. 1

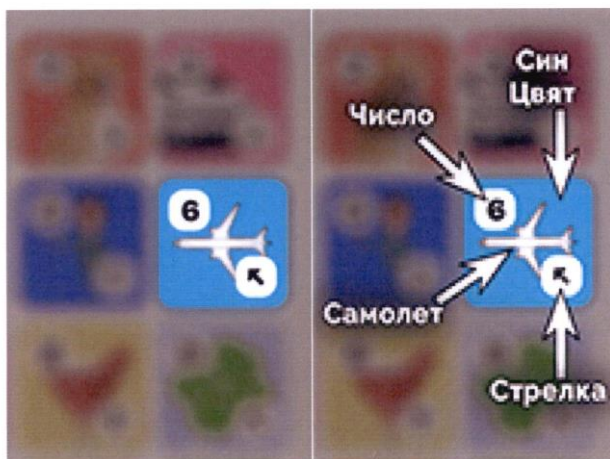


Фиг. 2А



v

Фиг. 2Б



Фиг. 3



Фиг. 4



Заблуждаващи
манипулации

Позиция:

Преди ▾

Брой:

0 ▾



Потвърди



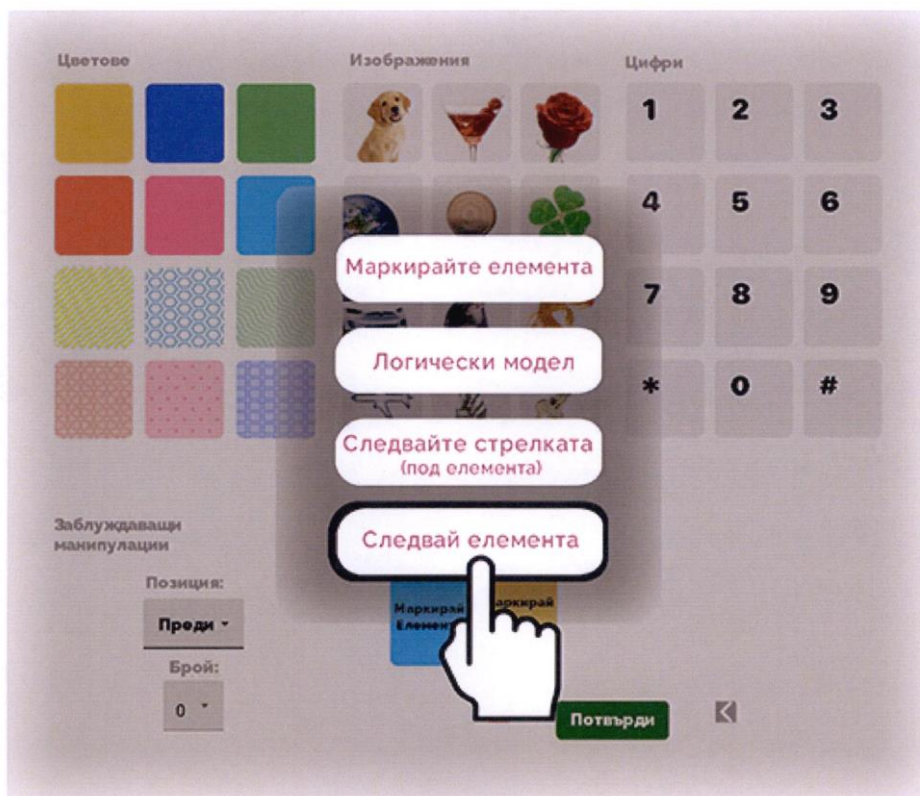
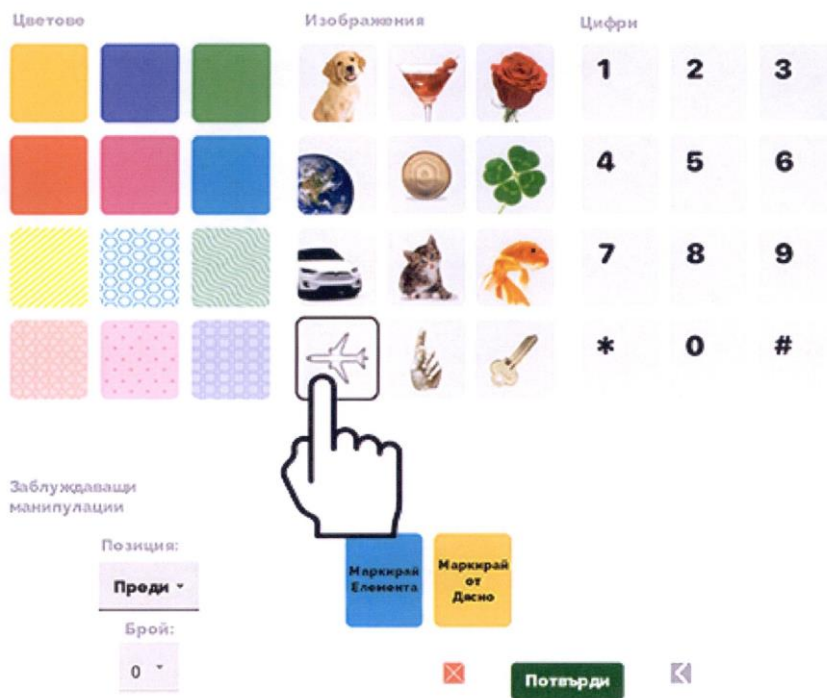
Фиг. 5А



Фиг. 5Б



Фиг. 5В



Фиг. 5Г



Фиг. 5Д



Заблуждаващи
манипулации

Позиция:

Преди -

Преди

След



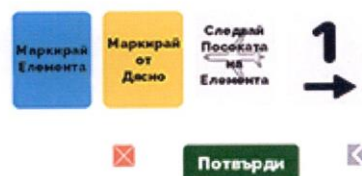
Заблуждаващи
манипулации

Позиция:

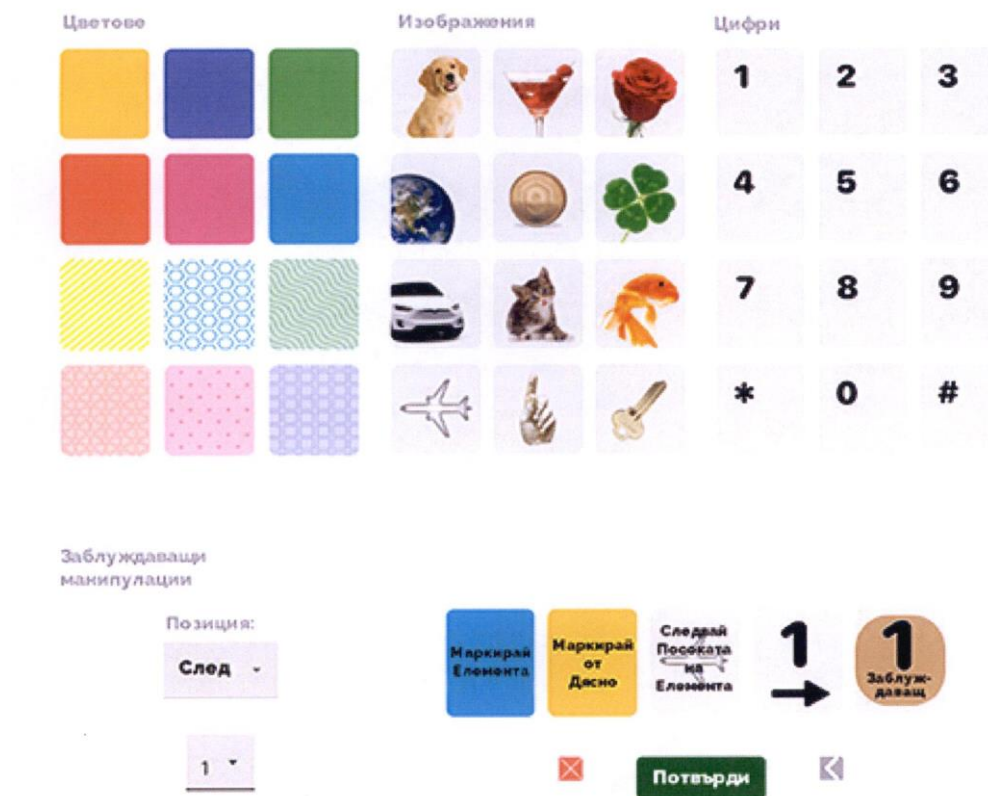
Преди -

Преди

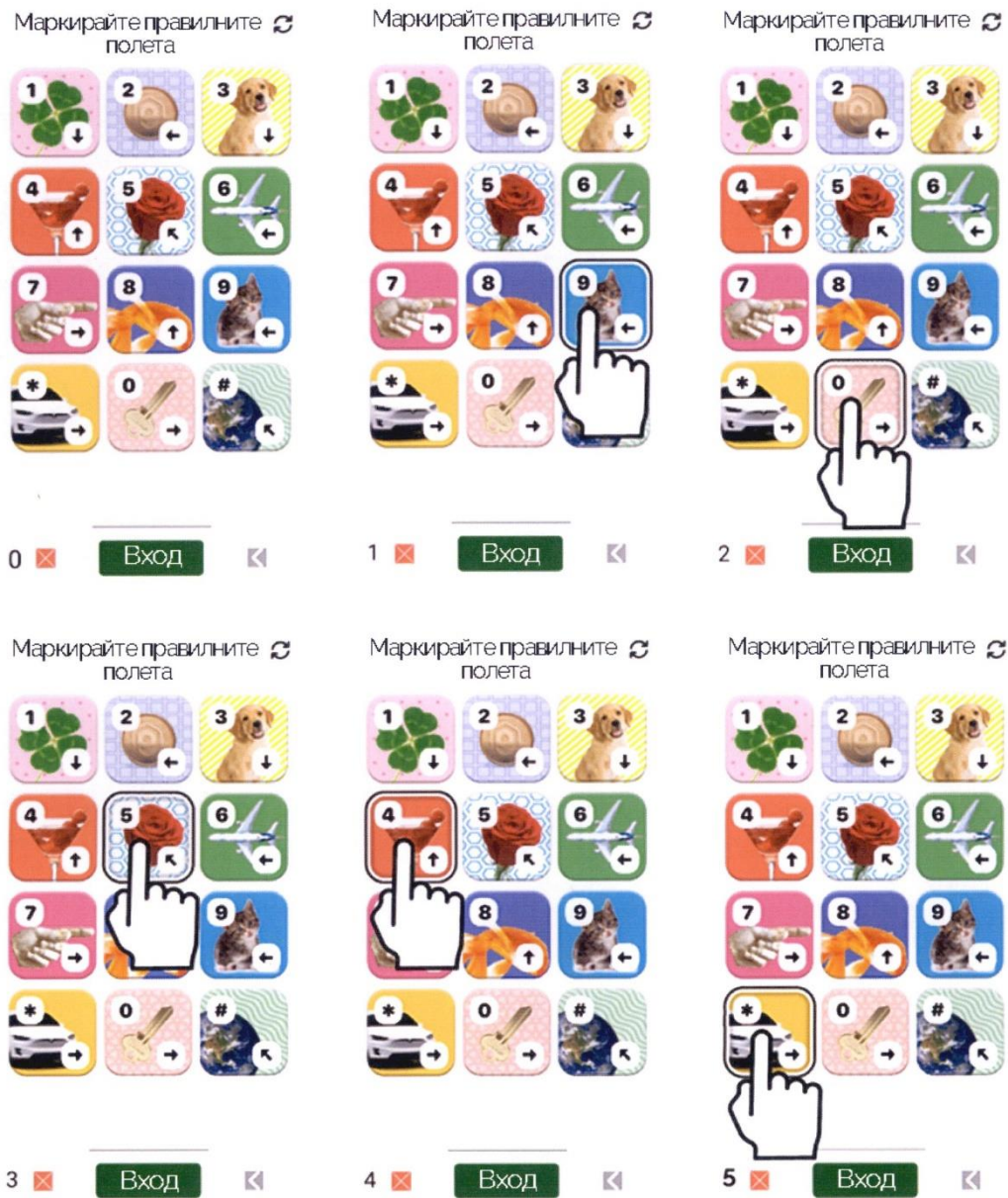
След



Фиг. 5Е



Фиг. 5Ж



Фиг. 6А

Маркирайте правилните полета



0 ☒ Вход

Маркирайте правилните полета



1 ☒ Вход

Маркирайте правилните полета



2 ☒ Вход

Маркирайте правилните полета



3 ☒ Вход

Маркирайте правилните полета



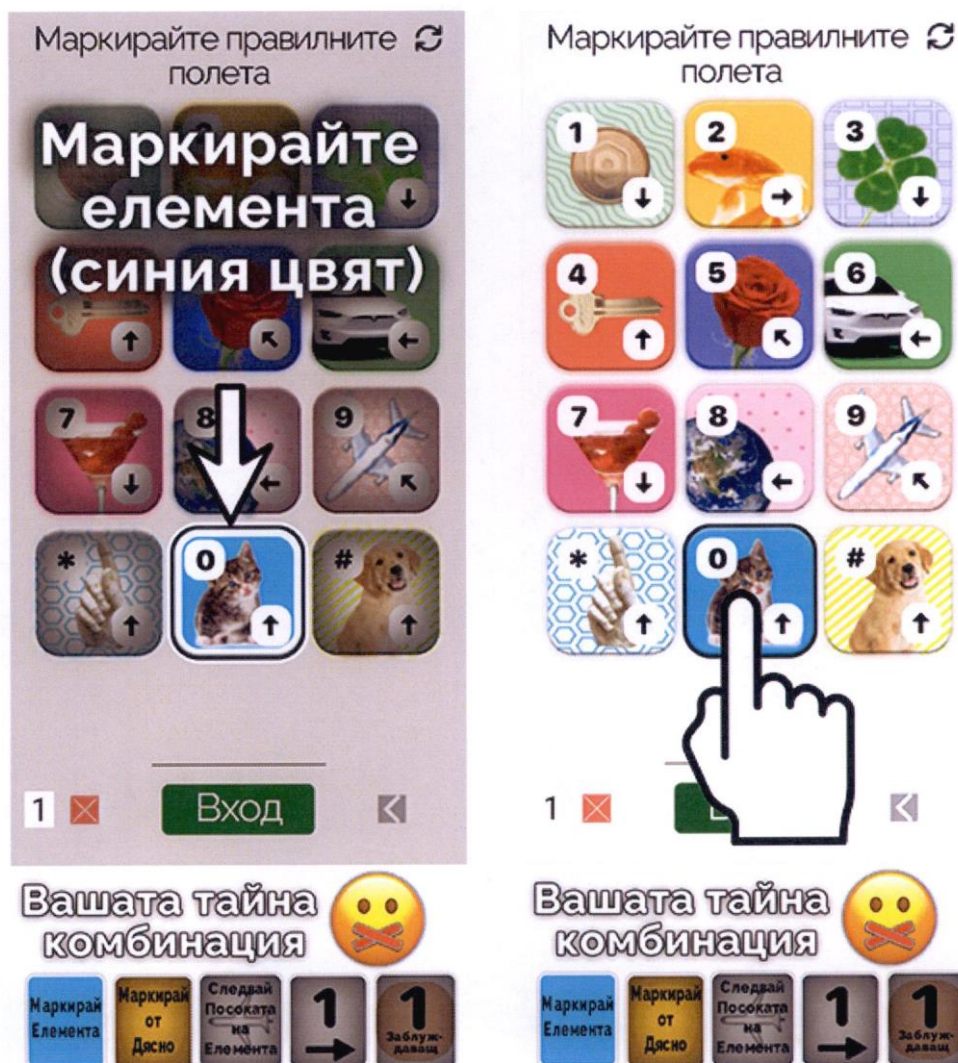
4 ☒ Вход

Маркирайте правилните полета

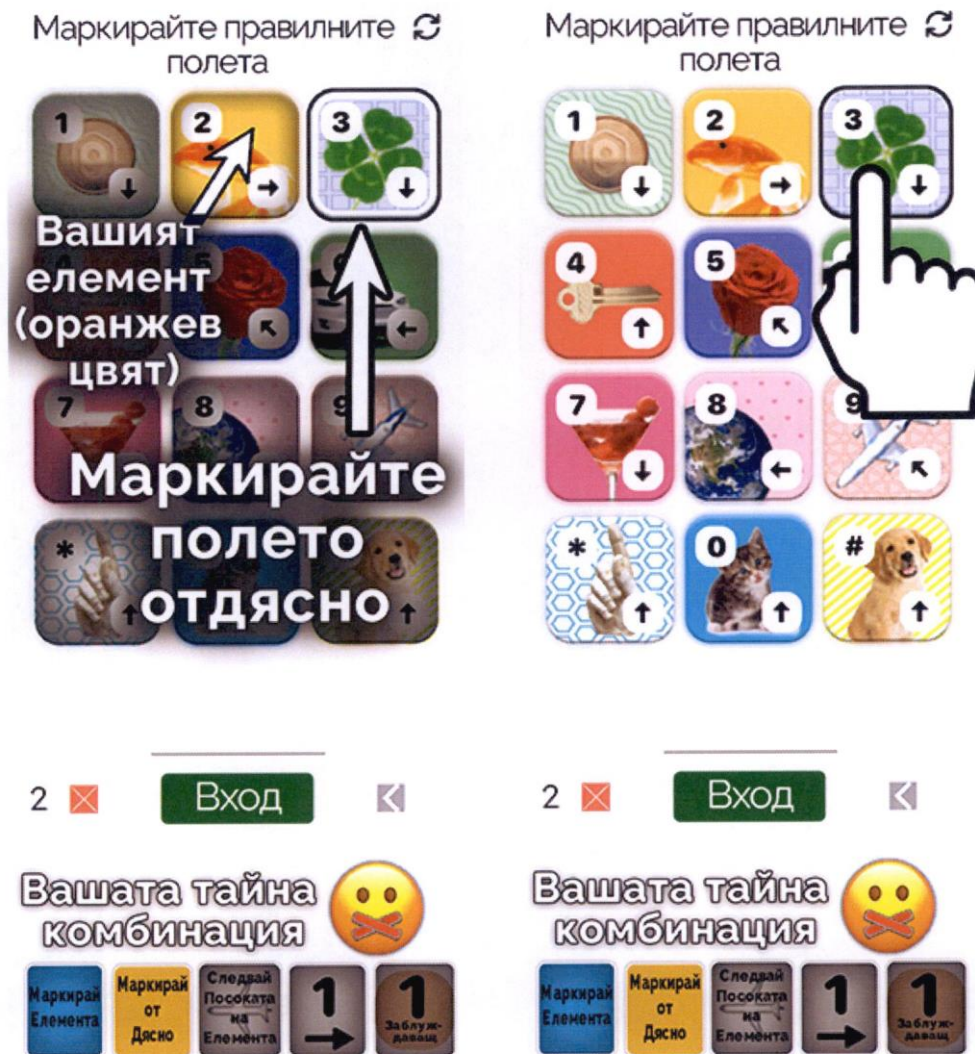


5 ☒ Вход

Фиг. 6Б



Фиг. 7А



Фиг. 7Б



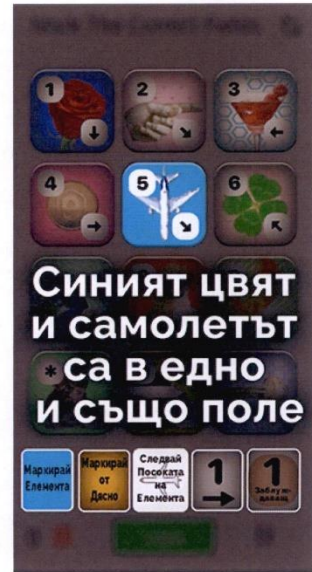
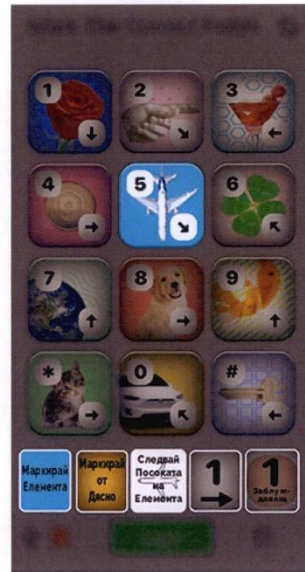
Фиг. 7В



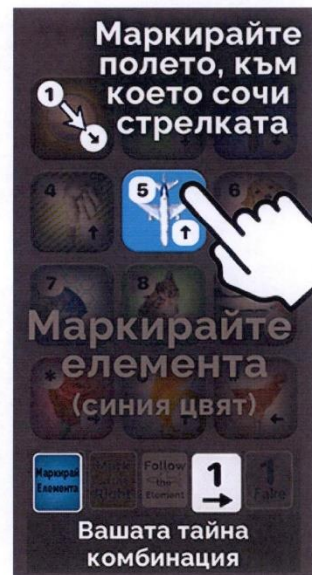
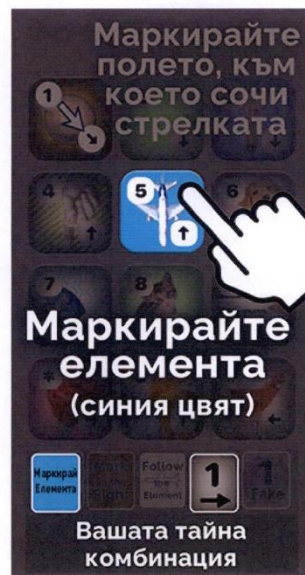
Фиг. 7Г



Фиг. 7Д



Фиг. 8



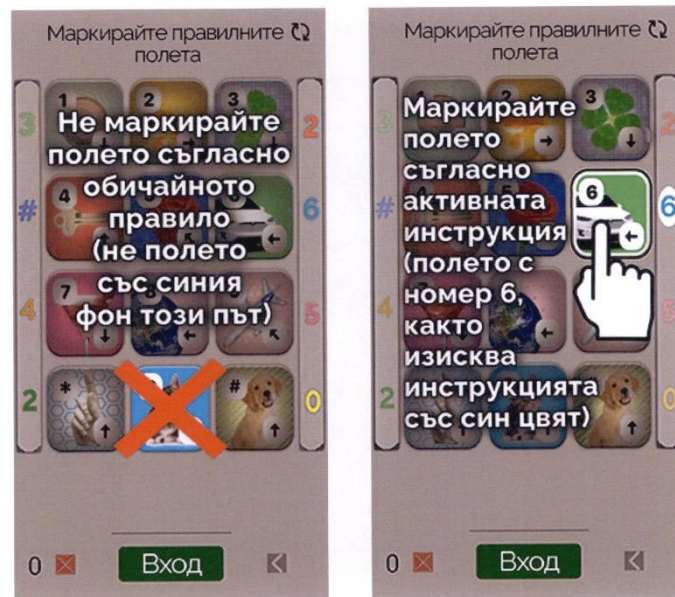
Фиг. 9



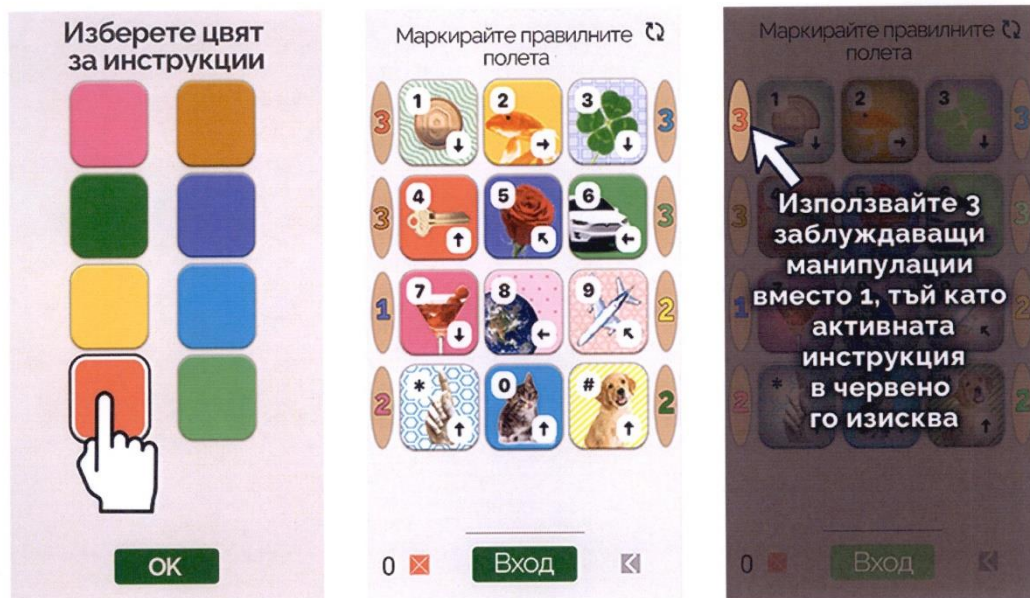
Фиг. 10



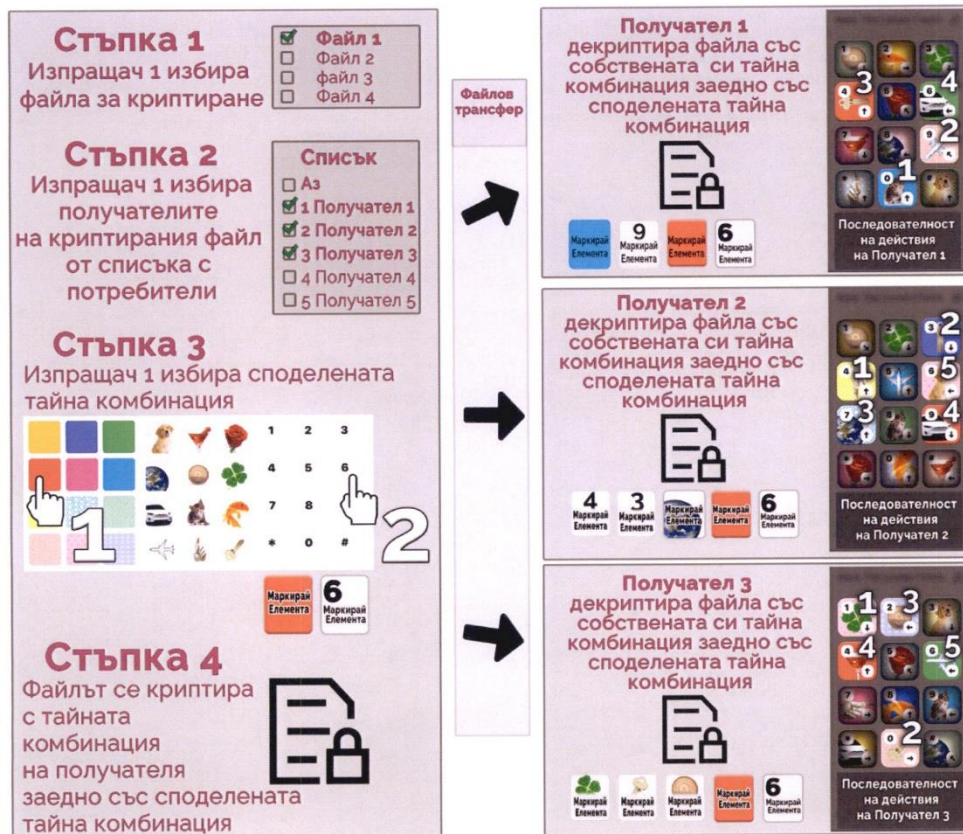
Фиг. 11



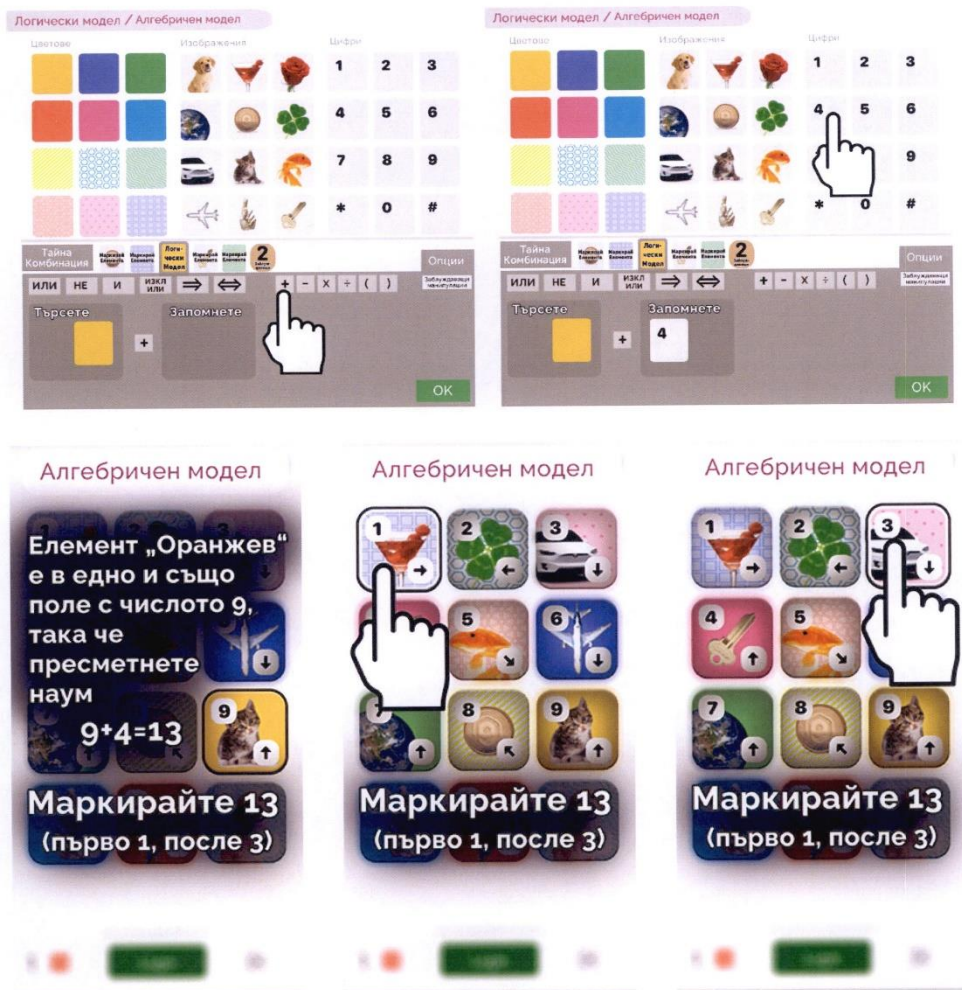
Фиг. 12



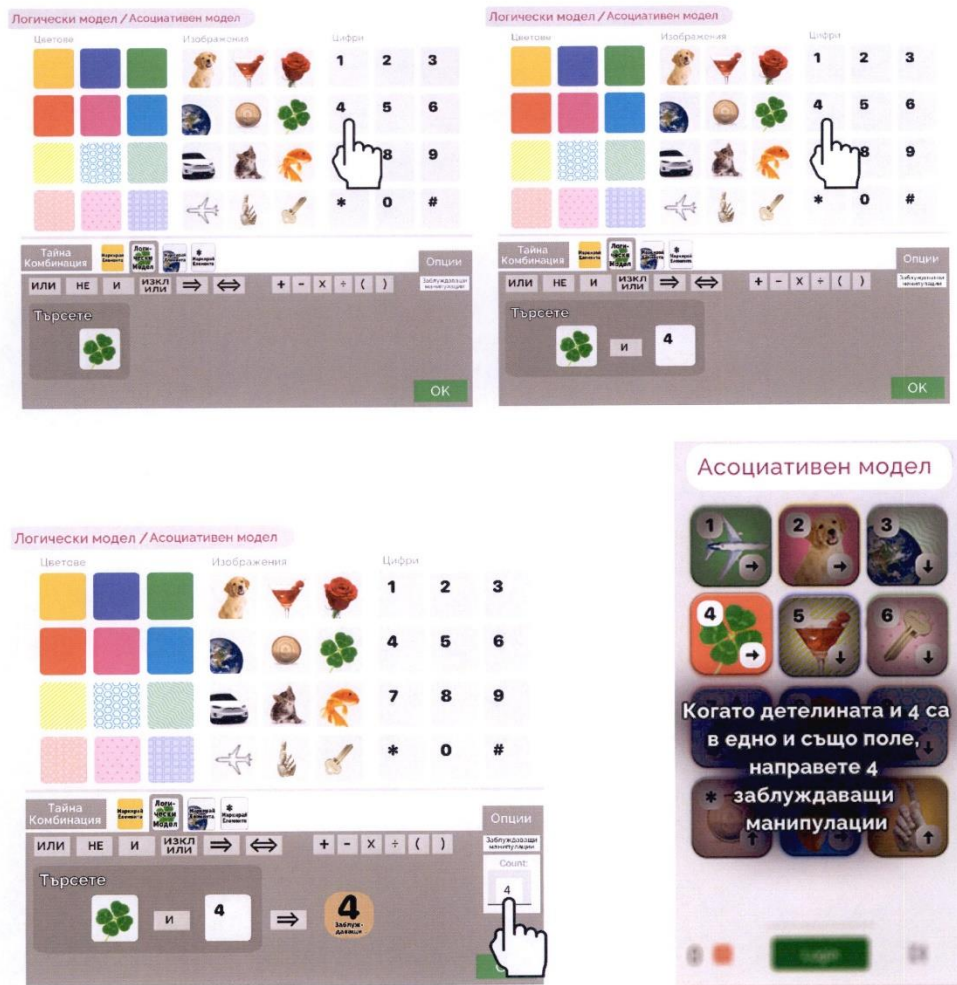
Фиг. 13



Фиг. 14



Фиг. 15



Фиг. 16



Фиг. 17



Фиг. 18



Фиг. 19