

(12) МЕЖДУНАРОДНАЯ ЗАЯВКА, ОПУБЛИКОВАННАЯ В СООТВЕТСТВИИ С
ДОГОВОРом О ПАТЕНТНОЙ КООПЕРАЦИИ (РСТ)

(19) Всемирная Организация
Интеллектуальной Собственности
Международное бюро



(43) Дата международной публикации
15 ноября 2007 (15.11.2007)

PCT

(10) Номер международной публикации
WO 2007/129935 A2

(51) Международная патентная классификация:
A63F 3/06 (2006.01) G06Q 50/00 (2006.01)

(21) Номер международной заявки: PCT/RU2007/000229

(22) Дата международной подачи: 8 мая 2007 (08.05.2007)

(25) Язык подачи: Русский

(26) Язык публикации: Русский

(30) Данные о приоритете:
2006115893 10 мая 2006 (10.05.2006) RU

(71) Заявитель и

(72) Изобретатель: ГЕРТНЕР Дмитрий Александрович
(GERTNER, Dmitry Aleksandrovich) [—/RU]; ул.
Горького, 9, кв. 20, Сыктывкар, 167000, Syktyvkar
(RU).

(81) Указанные государства (если не указано иначе, для
каждого вида национальной охраны): AE, AG, AL,
AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ,
CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC,
EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU,

ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA,
LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN,
MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH,
PL, PT, RO, RS, SC, SD, SE, SG, SK, SL, SM, SV, SY,
TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA,
ZM, ZW.

(84) Указанные государства (если не указано иначе, для
каждого вида региональной охраны): ARIPO (BW, GH,
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), евразийский (AM, AZ, BY, KG, KZ, MD, RU, TJ,
TM), европейский патент (AT, BE, BG, CH, CY, CZ, DE,
DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV,
MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ,
CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN,
TD, TG).

Опубликована:

— с декларацией в соответствии со статьёй 17(2)(a);
без реферата; название изобретения не проверено
международным поисковым органом.

В отношении двубуквенных кодов, кодов языков и других
сокращений см. "Пояснения к кодам и сокращениям",
публикуемые в начале каждого очередного выпуска
Бюллетеня РСТ.

(54) Title: METHOD FOR RUNNING AN ELECTRONIC LOTTERY GAME

(54) Название изобретения: СПОСОБ ОСУЩЕСТВЛЕНИЯ РОЗЫГРЫША ЭЛЕКТРОННОЙ ЛОТЕРЕИ

(57) Abstract:

(57) Реферат:



WO 2007/129935 A2

Способ осуществления розыгрыша электронной лотереи

Описание

Область техники

Изобретение относится к области вычислительной техники, в частности к её использованию для проведения электронной лотереи с применением различных каналов связи, например сети Интернет.

Предшествующий уровень техники

До настоящего времени для проведения розыгрышей лотерей через Интернет в типовом случае использовалась центральная электронная вычислительная машина (сервер), содержащая электронную базу данных с уникальными номерами, присваиваемыми участникам электронной лотереи либо персональным устройствам участников, таких как мобильный телефон. Выигрыш в такой лотерее зависит от случайного выбора определяемого генератором случайных чисел, находящимся на сервере. Так же, например, известен способ проведения Интернет - лотереи (RU 2001125679 A), в котором выигрыш распределяется по номерам, присваиваемым платежным транзакциям за участие в лотерее, кратным заранее оговоренным числам. При проведении электронных лотерей игрок не контролирует ход розыгрыша и вынужден полностью полагаться на честность организаторов лотереи, которые обладают технической возможностью влиять на распределение выигрышей. В связи с этим подобные электронные лотереи не пользуются спросом. Наиболее интересным видом лотерей для игроков являются, в частности, моментальные лотереи с использованием стрейч – карт, покрытых защитным слоем, с несколькими стираемыми полями, под которыми скрыты символы или пиктограммы. В данной лотерее игрок имеет возможность выиграть любой из объявленных призов, если угадает, какие поля необходимо стереть. Известны в частности способы проведения таких лотерей (RU 2233688 C1, RU 2000122770 A). Особенность такого вида лотерей заключается в том, что у организаторов лотереи отсутствует техническая возможность повлиять на результат розыгрыша, причем,

игроки могут в этом легко убедиться. Существует неофициальный термин для такого вида лотерей – лотереи с неуправляемой случайностью. Важен еще и тот момент, что случайный выбор делают сами игроки. Однако, до настоящего времени осуществлять розыгрыши лотерей с неуправляемой случайностью, в которых результат зависит от игрока, эффективно реализованы лишь с использованием бумажных или пластиковых носителей, покрываемых защитным слоем. Кроме того, существует потенциальная возможность визуализировать скрытое под защитным слоем изображение путем сканирования специальным оборудованием, что создает угрозу мошенничества с применением технических средств. Что касается электронных лотерей с неуправляемой случайностью, то из области криптографии известен так называемый «протокол подбрасывания монеты», суть которого заключается в том, что результат розыгрыша лотереи шифруется на стороне, проводящей розыгрыш и полученная криптограмма передается игроку, после чего игрок должен угадать результат розыгрыша, выбрав один вариант из нескольких возможных. Затем игроку передается ключ, с помощью которого игрок может расшифровать криптограмму и сравнить результат со своим выбором, а заодно и убедиться в честности проводимой лотереи. Недостатком данного способа является его сложность, а также и то, что игроку для понимания надежности данной процедуры проверки необходимо хотя бы начальное знание основ криптографии. Кроме того, программная реализация способа проверки по «протоколу подбрасывания монеты» не гарантирует отсутствия лазеек в программе со стороны разработчиков – нельзя исключить такую программную реализацию протокола, при котором существует не один, а несколько различных ключей для расшифровывания криптограммы и получения различных результатов для подтасовки итогов розыгрыша.

Раскрытие изобретения

Задачей настоящего изобретения является осуществление такого способа розыгрыша электронных лотерей, при котором выбор, а следовательно возможность выигрыша полностью зависит от случайного выбора игрока и при этом у игроков есть технические возможности

контролировать ход лотереи, а организаторы лотереи лишены потенциальной возможности управлять случайным выбором. При этом надежность способа должна быть интуитивно понятной и очевидной практически для любого игрока. Одновременно способ должен обеспечивать защиту от возможных мошеннических действий со стороны недобросовестных игроков. Решение данной задачи должно благотворно повлиять на рынок электронных лотерей, в частности для их применения в розничной торговле в качестве стимулирующих лотерей.

Поскольку у настоящего изобретения нет прямых аналогов, то поэтому прототипы не описаны.

Перед детальным описанием сущности изобретения поясним используемую терминологию. Под электронным носителем информации понимается носитель типа оптический компакт диск. Под персональным приемо-передающим устройством понимается электронная вычислительная машина, снабженная средством выхода в Интернет и находящаяся в распоряжении пользователя (игрока). В частных случаях персональным приемо-передающим устройством является мобильный телефон пользователя. Под компьютерным приложением понимается игровое приложение, выполненное в виде компьютерной программы и рассчитанной на использование в электронных вычислительных машинах пользователей. Под пользователем в настоящем описании понимается игрок в электронную лотерею. Под сервером понимается центральная электронная вычислительная машина, подключенная к общедоступной информационной сети. Сервер включает в себя реляционную СУБД для хранения и поиска данных, в частности для регистрации игроков и для записи информации о ходе розыгрышей.

Краткое описание схем

Фиг. 1 – пошаговая схема с использованием сети Интернет

Фиг. 2 – пошаговая схема с использованием мобильной связи

Фиг. 3 – пошаговая схема с серийным номером

Детальное описание вариантов осуществления изобретения

Указанная задача достигается тем, что розыгрыш электронной лотереи каждый игрок осуществляет на своей электронной вычислительной машине 1 (фиг.1), используя свободно распространяемое компьютерное приложение, которое игрок предварительно получает на съемном носителе информации 2, таком как компакт диск или копирует по сети, например через Интернет (шаг а). Сервер 3 выполняет функцию регистрации игроков (шаг б), генерирует и рассылает игрокам сигналы, содержащие случайные коды 4 для проведения розыгрышей (шаг в). Затем сервер 3 фиксирует сигналы от игроков (шаг г), содержащие варианты выбора, которые делают игроки и от которых зависят результаты розыгрыша, в соответствии с правилами электронной лотереи. Особенность предлагаемого способа заключается в том, что последний ход, от которого зависит результат розыгрыша в электронной лотерее всегда делает игрок, что реализуется следующим образом: игрок сначала получает с сервера код, с помощью которого компьютерное приложение, запущенное на процессоре электронной вычислительной машины, выдаст некоторое значение из нескольких возможных вариантов, и после получения кода игрок в течение ограниченного периода времени выбирает игровую комбинацию и фиксирует свой выбор на сервере при помощи предоставленного интерфейса. Результат розыгрыша игрок видит на своей электронной вычислительной машине, запуская компьютерное приложение и вводя в него полученный код. Для наглядного пояснения ниже приведен частный случай использования описываемого способа. Например, игровое приложение выполнено в виде виртуального аналога рулетки, с изображением кольца, состоящего из 32 секторов с номерами и анимированного шарика, движущегося вокруг кольца. Через какое-то время шарик должен остановиться в одном из секторов. Заранее объявляется правило игры в виртуальную рулетку, исходя из которого, игрок должен заранее выбрать номер сектора, и если шарик остановится на секторе с угаданным номером, то игроку полагается определенный приз. Предлагаемый способ розыгрыша электронной лотереи применительно к виртуальной рулетке будет выглядеть следующим образом. Игрок устанавливает на своей электронной вычислительной машине компьютерное приложение в виде виртуальной рулетки (шаг а). Для

того, чтобы запустить шарик имеется поле для ввода кода. Игрок должен получить код с сервера. Для этого игрок соединяется по Интернету с сервером, используя Web-интерфейс. Заходит на сайт и производит процедуру регистрации (шаг б), и если это необходимо процедуру оплаты. Процедура регистрации может включать в себя заполнение формы с данными игрока, либо регистрацию электронного кошелька игрока. После этого на сервере генерируется случайный код и виде сигнала отправляется игроку (шаг в). Одновременно с этим на сервере отсчитывается заранее определенный промежуток времени T , например 1 минута, в течение которой от игрока ожидают сигнал, который должен содержать номер сектора, выбранный игроком. Код, полученный от сервера выводится на монитор персонального приемо-передающего устройства игрока в виде набора символов. Получив код, игрок вводит значение кода в компьютерное приложение либо используя буфер обмена, либо набрав код на клавиатуре и запускает виртуальную рулетку. И пока шарик крутится, игрок в течение 1 минуты с момента получения кода должен отправить на сервер сигнал, содержащий номер любого из сектора рулетки, на которой, как ожидает игрок, должен остановиться шарик (шаг г). Данный сигнал игрок передаст серверу через Web-интерфейс. Результат электронной лотереи игрок увидит на своем компьютере (шаг д). Естественно, что компьютерное приложение выполнено таким образом, чтобы шарик не успел остановиться раньше 1 минуты, иначе игрок сможет заранее узнать, где остановится шарик. Это достигается за счет использования в компьютерном приложении криптографических и односторонних преобразований с многократным числом повторений, либо за счет использования криптографических преобразований, в которых реализован механизм многократного повтора итераций. Не маловажно и то, что компьютерное приложение игрок может запустить на одной электронной вычислительной машине, а соединение с сервером производить на другой электронной вычислительной машине либо использовать для взаимодействия с сервером мобильный телефон 5 (фиг.2) например, посредством SMS сообщений, если организаторы лотереи предоставят данную техническую возможность. Из данного примера очевидно, что организаторы лотереи не имеют потенциальной технической

возможности влиять на розыгрыш электронной лотереи, т.к. последний и решающий ход остается за игроком. А использование криптографических преобразований с многократным числом итераций и односторонних преобразований защищает призовой фонд электронной лотереи от возможных мошеннических действий со стороны недобросовестных игроков. Данные преобразования осуществляются над кодом, который первоначально генерируется на сервере по случайному закону с помощью программного или аппаратного генератора случайных чисел. Под односторонним преобразованием понимается преобразование кода, которое в вычислительном смысле практически необратимо. Известны многочисленные примеры таких функций и их вычислителей, то есть средства для вычисления таких функций, реализуемых часто с помощью соответствующим образом запрограммированного компьютера (B.Schneier, Applied Cryptography: Protocols, Wiley& Sons, New York, 2nd edition, 1996; A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997). Под криптографическим преобразованием понимается шифрование или дешифрование кода, выполняемое с использованием криптографических алгоритмов, например, «Алгоритма Шифрования Данных», обычно называемого DES. Но сами по себе эти преобразования данных осуществляются процессором за считанные доли секунды. Для того, чтобы преобразования выполнялись не менее 1 минуты, как в приведенном примере, необходимо применить многократные итерации либо в алгоритме одностороннего преобразования, и/или в алгоритме шифрования, либо осуществить многократное повторение преобразований. Например, полученный с сервера в виде сигнала код «K» сначала шифруется, затем полученное значение «S» подается односторонней функции, которая выдает значение «F1», причем, размер в битах кода «K» значения «S» и «F1» должен совпадать. Обе осуществленные с помощью компьютерного приложения и процессора операции преобразования кода примем за одну итерацию. Затем, повторим цикл, присвоив переменной «K» значение «F1». На выходе второй итерации получим новое значение «F2». Полученное конечное значение F_n , где n – число итераций, в приведенном выше примере будет использовано компьютерным приложением для определения номера

сектора виртуальной рулетки, на которой следует остановить шарик. Для этой цели необходимо использовать дополнительное преобразование с применением хеш-функции, которая является частным случаем одностороннего преобразования, отличающееся тем, что результат хеш преобразования H - получается меньшего размера, чем исходное значение. В рассматриваемом примере оптимальный размер кода K , а следовательно и всех преобразуемых значений до $F_n - 56$ бит. Данная длина гарантирует защиту от подбора возможных значений K с использованием современной вычислительной техники и в то же время является удобной для игрока при клавиатурном вводе кода. В то же время результат хеш преобразования H в битах, возведенный в степень двойки должен быть равен числу вариантов в игровом приложении, в нашем примере числом вариантов является количество секторов в виртуальной рулетке. Если их число равно 32, то H должен быть равен 5 битам, т.к. 2 в степени 5 дает 32. Таким образом хеш-функция на входе принимает вектор длиной в 56 бит, а на выходе выдает вектор длиной 5 бит, который игровое приложение использует для определения номера сектора, в котором нужно будет остановить шарик.

Число итераций n подбирается исходя из быстродействия серийно выпускаемых процессоров электронных вычислительных машин, которое влияет на скорость вычисления значений «S» и «H» за одну итерацию и установленного периода времени, в течение которого на сервере ожидают получить сигнал от игрока. Так, если одна итерация на серийном процессоре выполняется за 100 микросекунд, а период времени T равен 60 секундам, то число итераций в компьютерное приложение закладывается более 600 000.

Ниже приведены примеры частных случаев реализации как отдельных операций, так и изобретения в целом.

Компьютерное приложение может быть передано пользователю на мини компакт диске, например при покупке товаров в супермаркете в виде поощрения, причем, на данном мини компакт диске одновременно с компьютерным приложением для электронной лотереи может находиться другая полезная информация, например электронный каталог товаров, продаваемых в этом супермаркете. На web - сервере пользователь,

желающий сыграть в электронную лотерею, заполняет регистрационную форму, в которой, в частности указывает адрес своей электронной почты. После чего, на сервере генерируется код и передается в виде сигнала персональному приемо-передающему устройству игрока и засекается небольшой интервал времени, например 1 минута, в течение которой игрок, с помощью персонального приемо-передающего устройства должен сообщить серверу одну из нескольких возможных комбинаций. О том выиграл игрок или нет, он может узнать сам, запустив на своем компьютере игровое приложение, введя в него полученный с сервера код и сравнив полученный результат с тем, который игрок сообщил серверу. Так как розыгрыш проводится с использованием настоящего изобретения, то количество победителей можно просчитать только с помощью теории вероятности. Доказательством выигрыша являются - заполненная игроком регистрационная форма, сгенерированный код, переданный игроку и вариант комбинации, выбранный игроком. Эта информация хранится в электронной базе данных организаторов лотереи. Для того, чтобы исключить возможность манипулирования результатами розыгрыша электронной лотереи путем искажения информации, хранящейся в базе данных, на сервере предлагается установить дополнительный модуль электронной цифровой подписи. Данный модуль предназначен для автоматического подписания всей критически важной информации, касающейся розыгрыша электронной лотереи. Электронная цифровая подпись, как известно, защищает подписанную информацию от внесения каких либо изменений и, кроме того, придает юридическую значимость подписанным файлам. В нашем случае электронной цифровой подписью нужно подписывать получаемые от пользователей сигналы, содержащие регистрационные данные игроков, коды, сгенерированные на сервере и отправленные игрокам, показания системного времени, а именно – время отправления игроку кода, время получения от игрока встречного сигнала, и сам сигнал, который содержит вариант игрока. Вся эта информация компонуется на сервере в один или несколько файлов, подписывается электронной цифровой подписью и тут же отправляется игроку на его электронный почтовый ящик, который игрок

отметил в регистрационной форме. Полученный игроком файл с цифровой подписью является юридически значимым доказательством при проверке результата розыгрыша и является основанием на выдачу приза в случае выигрыша.

Если предоставить пользователю возможность получить код с сервера не сразу после регистрации, а в любое другое время после разрыва соединения, то электронная лотерея приобретает новое свойство – возможность переадресации. Так, при регистрации пользователя на сервере электронных лотерей с применением настоящего изобретения пользователь может внести в регистрационную форму данные другого пользователя, переадресуя тем самым право на розыгрыш лотереи и право на получение выигрыша другому пользователю, данные которого будут сохранены в базе данных сервера. В этом случае электронная лотерея выступает в качестве электронного лотерейного билета, который можно передавать по телекоммуникационным каналам связи в виде набора определенных сигналов. Но для того, чтобы сервер смог узнать, что вновь подключенный пользователь будет разыгрывать электронную лотерею по ранее зарегистрированным данным, сервер должен сгенерировать, сохранить в базе данных и передать пользователю, заполнившему регистрационную форму, идентификационный номер N (фиг. 3, шаг б). А при новом соединении с сервером, пользователь должен передать серверу сигнал, содержащий этот самый идентификационный номер N (шаг г), по которому сервер по своей базе данных определит, что пользователь имеет право на розыгрыш электронной лотереи и по требованию пользователя, выраженному в виде соответствующего сигнала, сгенерирует и передаст пользователю код в соответствии (шагом д). Поскольку в терминологии лотерей существует понятие серийный номер лотерейного билета, то такой идентификационный номер N далее будем называть серийным номером. А так как лотерейным билетом в настоящем изобретении фактически является компьютерное приложение, то серийный номер присвоим компьютерному приложению. Для того, чтобы обеспечить большее функциональное назначение серийного номера, его

можно использовать дополнительно вместе с кодом для получения результата розыгрыша электронной лотереи. Для этого и код и серийный номер передают в виде сигнала на обработку компьютерным приложением с помощью процессора, оказывая влияние на конечный результат преобразования кода. Частная реализация данной процедуры выглядит следующим образом: в компьютерное приложение передается серийный номер N и код K имеющие равный размер в битах и между ними производится операция XOR. Полученный результат присваивается переменной K и обрабатывается далее по вышеописанной схеме со множеством повторений с использованием криптографических и односторонних функций.

Время для розыгрыша электронной лотереи определяет организатор. При отсутствии ограничений во времени проведения розыгрыша – лотерея становится моментальной, иными словами, игрок в произвольно выбранное время производит регистрацию на сервере и получает код для розыгрыша лотереи. С данного момента игрок разыгрывает приз, независимо от участия остальных игроков. В большинстве случаев этот вариант наиболее удобен для игроков. Однако для организаторов лотереи иногда удобнее проводить розыгрыш лотереи в заранее определенный период времени. Например, производители каких-либо товаров решили провести стимулирующую электронную лотерею среди розничных покупателей с использованием настоящего изобретения. Причем, кроме стимулирования продаж электронная лотерея также поможет защитить товар от нелегального тиражирования. В качестве лотерейных билетов можно использовать этикетки, на которые заранее нанесены серийные номера, которые сохранены в электронной базе данных на сервере. Сами номера могут быть защищены стрейч-слоем, либо каждая этикетка может содержать какой-либо элемент, защищенный от копирования. Производители товара объявляют о проведении розыгрыша в определенную дату. Покупатели товара регистрируются на сервере используя серийные номера, полученные с этикеток. Если стоимость товара незначительна или лотерею организует торговое предприятие, то для участия в электронной лотерее может быть

применена накопительная система, при которой покупатель должен собрать не один, а несколько номеров. Если серийный номер, введенный покупателем совпадает с одним из хранящихся в базе данных, то покупатель становится участником электронной лотереи.

В компьютерном приложении может быть реализован розыгрыш в несколько туров. Так если игрок выиграл в электронную лотерею небольшой приз и сообщил об этом серверу в виде определенного сигнала, то на сервере сгенерируют еще один код и отправят его в виде сигнала пользователю для продолжения розыгрыша с возможностью получения более крупного выигрыша.

В целом предлагаемый способ осуществления розыгрыша электронных лотерей может быть использован в качестве базовой технологии при создании различных электронных лотерей, в которых web – интерфейс и компьютерные приложения могут быть реализованы самым различным образом с произвольным дизайном, не меняя при этом сущности настоящего изобретения.

Формула изобретения.

1. Способ осуществления розыгрыша электронной лотереи, характеризуется тем, что передают пользователю на электронном носителе информации или передают по телекоммуникационному каналу связи в персональное приемное устройство пользователя компьютерное приложение, связанное с электронной лотереей, затем между сервером и персональным приемно-передающим устройством пользователя по телекоммуникационному каналу устанавливают сеанс связи и на сервере, с помощью генератора случайных чисел генерируют код, который в виде сигнала по телекоммуникационному каналу связи передают в персональное приемное устройство пользователя, одновременно фиксируют время передачи кода и засекают заранее определенный промежуток времени T , в течение которого на сервере по телекоммуникационному каналу связи ожидают и, в случае получения, сохраняют сигнал от персонального передающего устройства пользователя, включающий в себя произвольно введенный пользователем вариант результата преобразования кода компьютерным приложением из конечного числа возможных вариантов, определяют результат розыгрыша электронной лотереи исходя из заранее объявленного правила в соответствии с упомянутым сохраненным вариантом результата преобразования кода из конечного числа возможных вариантов, и фактическим результатом преобразования кода, который получают с помощью процессора, используя вышеупомянутое компьютерное приложение, которому передают на обработку сигнал, содержащий упомянутый код, причем, компьютерное приложение выполняет обработку сигнала на серийно выпускаемых процессорах за время, превышающее промежуток времени T .

2. Способ по п. 1 отличающийся тем, что между сервером и персональным приемно-передающим устройством пользователя устанавливают сеанс связи по телекоммуникационному каналу для проведения розыгрыша в произвольно выбранный пользователем момент времени.

3. Способ по п. 1 отличающийся тем, что между сервером и персональным приемно-передающим устройством пользователя устанавли-

вают сеанс связи по телекоммуникационному каналу для проведения розыгрыша в заранее определенный промежуток времени.

4. Способ по п. 1 отличающийся тем, что в персональное приемопередающее устройство пользователя компьютерное приложение копируют с электронного носителя информации типа компакт диск с использованием привода компакт дисков.

5. Способ по п. 1 отличающийся тем, что компьютерному приложению присваивают серийный номер, который используют вместе с кодом для получения результата розыгрыша электронной лотереи и дополнительно передают в виде сигнала на обработку компьютерным приложением с помощью процессора, оказывая влияние на конечный результат преобразования кода.

6. Способ по п. 1 отличающийся тем, что компьютерное приложение выполнено с возможностью обработки сигнала процессором с использованием криптографических преобразований с заранее определенным многократным числом итераций, количество которых подбирают не менее такого числа, при котором компьютерное приложение выполняет обработку сигнала на серийно выпускаемых процессорах за время, превышающее промежуток времени T.

7. Способ по п. 1 отличающийся тем, что компьютерным приложением обрабатывают сигнал при помощи процессора с использованием односторонних преобразований.

8. Способ по п. 1 отличающийся тем, что для формирования кода используют программный генератор случайных чисел.

9. Способ по п. 1 отличающийся тем, что для формирования кода используют аппаратный генератор случайных чисел.

10. Способ по п. 1 отличающийся тем, что передают код пользователю по телекоммуникационному каналу связи в персональное приемопередающее устройство пользователя, являющееся мобильным телефоном.

11. Способ по п. 1 отличающийся тем, что на сервер принимают сигнал, включающий в себя произвольно введенный пользователем вариант результата преобразования кода компьютерным приложением из

конечного числа возможных вариантов, по телекоммуникационному каналу связи с персонального приемо-передающего устройства пользователя, являющегося мобильным телефоном.

12. Способ по п. 1 отличающийся тем, что код, получаемый в виде сигнала в персональное приемо-передающее устройство, выводят на экран монитора в виде набора символов.

13. Способ по п. 1 отличающийся тем, что сигнал для обработки компьютерным приложением при помощи процессора формируют с помощью клавиатуры из набора символов, соответствующего переданному пользователю коду.

14. Способ по п. 1 отличающийся тем, что для обмена данными между персональным приемо-передающим устройством пользователя и сервером используется сеть Интернет, а в качестве сервера используют Web-сервер.

15. Способ по п. 1 отличающийся тем, что сигнал от персонального приемо-передающего устройства пользователя, включающий в себя произвольно введенный пользователем вариант результата преобразования кода из конечного числа возможных вариантов передают на сервер посредством Web-интерфейса.

16. Способ по п. 1 отличающийся тем, что в случае совпадения выбранного пользователем варианта результата преобразования кода из нескольких возможных вариантов с фактическим результатом преобразования кода, пользователю, с его согласия, выраженного в виде соответствующего сигнала, передают новый код для продолжения игры и возможности получения более крупного выигрыша.

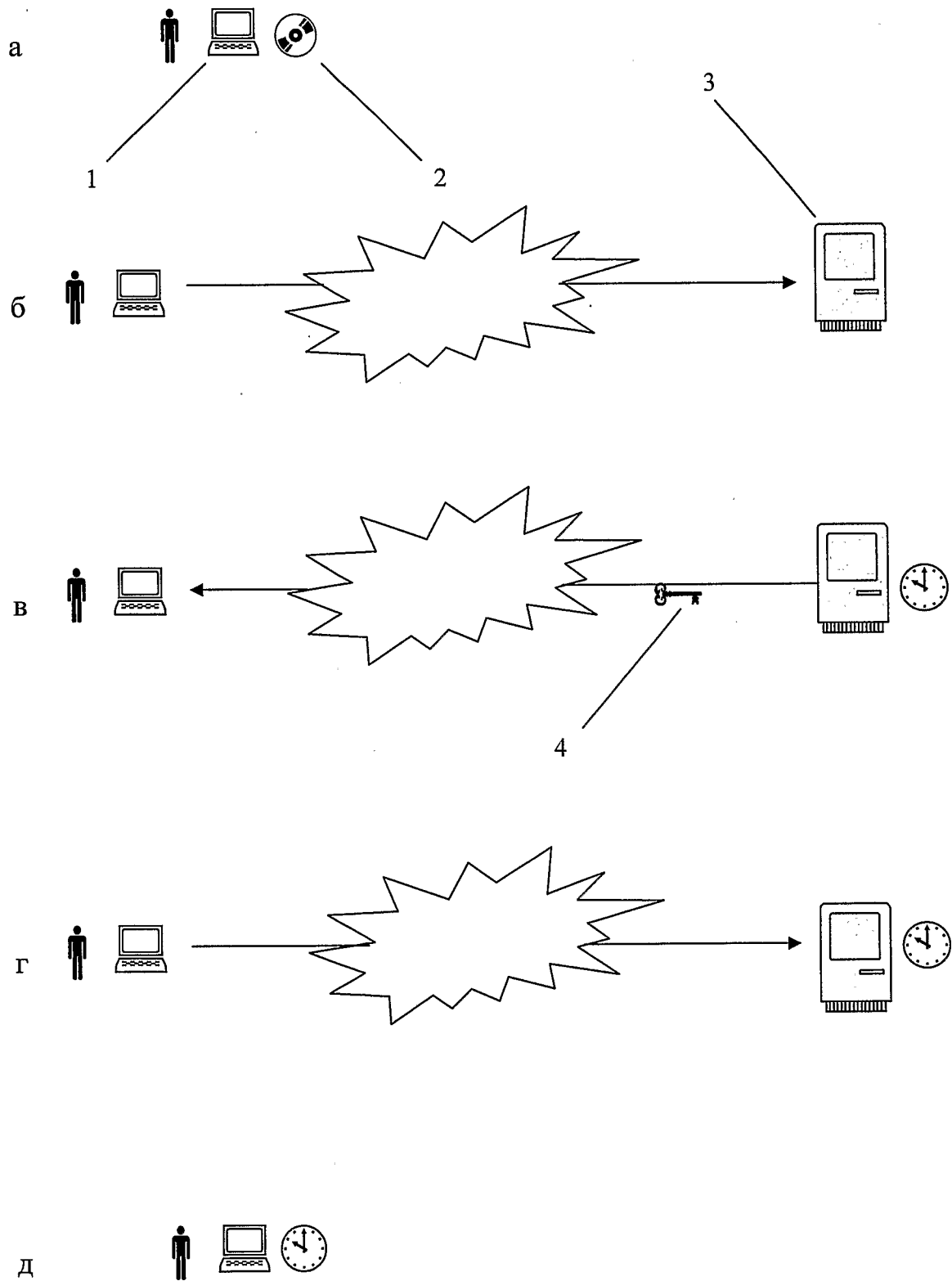
17. Способ по п. 1 отличающийся тем, что указанным пользователем является игрок, указанным компьютерным приложением является игровое приложение, а результатом розыгрыша электронной лотереи является право на получение вещественного приза или денежного приза определенного размера в соответствии заранее объявленными правилами.

18. Способ по п. 1 отличающийся тем, что сервер дополнительно включает в себя модуль электронной цифровой подписи, которой авто-

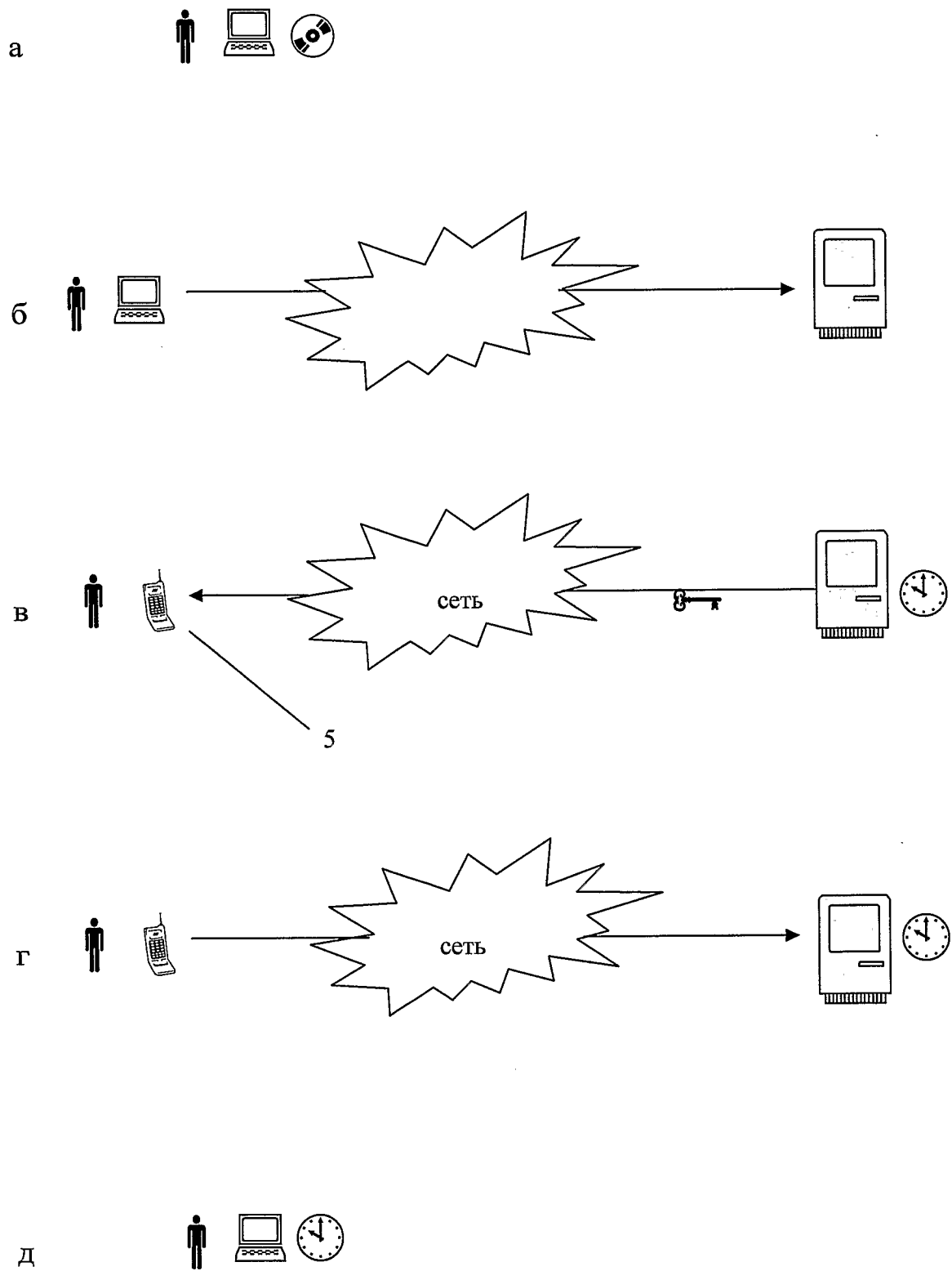
матически подписывают получаемые от пользователей сигналы, сформированные коды и показания системного времени с целью защиты от несанкционированного искажения информации при проверке результатов лотереи.

19. Способ по п. 18 отличающийся тем, что подписанные сигналы сохраняют на сервере и одновременно отправляют пользователям.

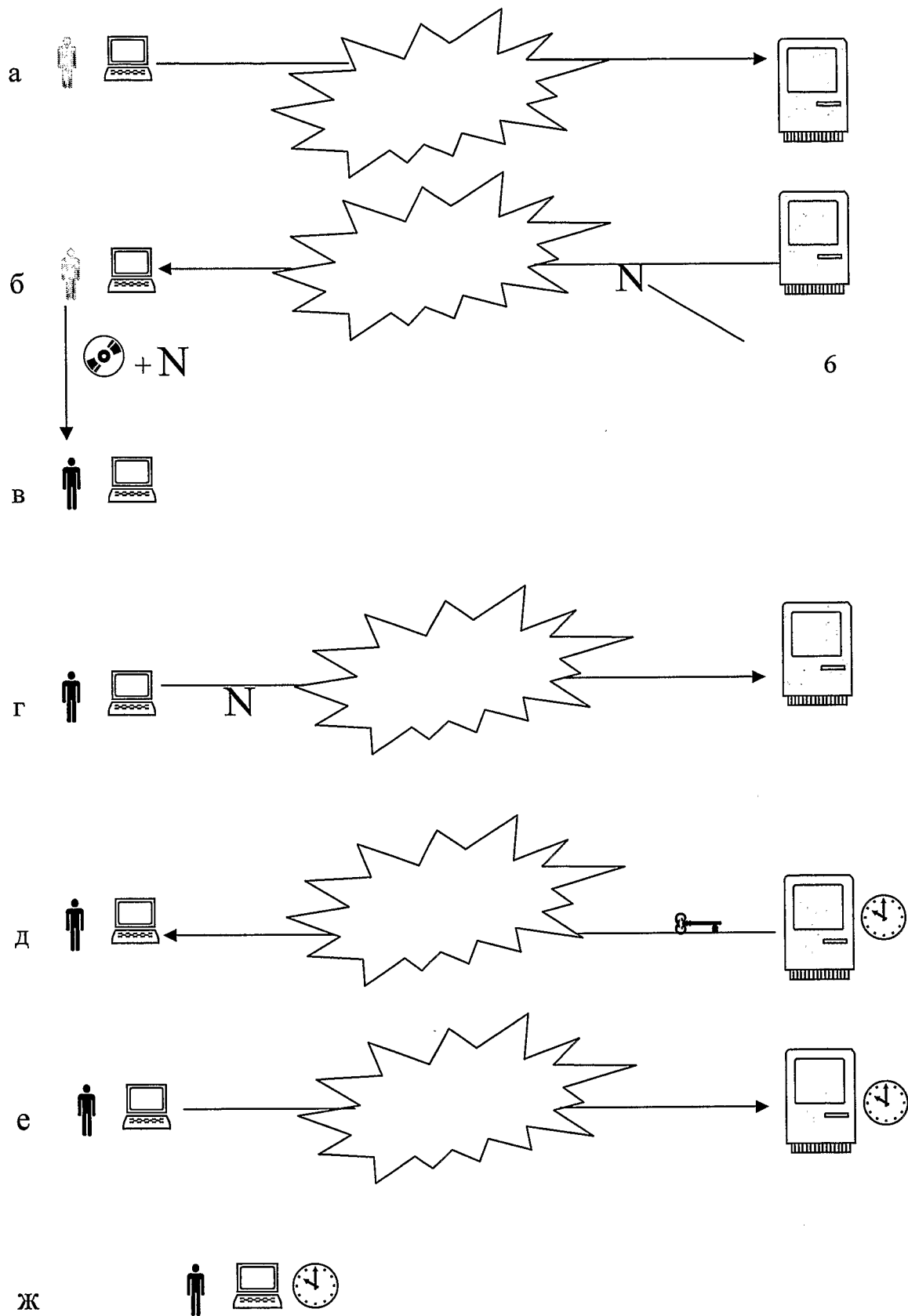
20. Способ по п.п. 1 и 18 отличающийся тем, что определяют результат розыгрыша электронной лотереи в персональном электронном вычислительном устройстве пользователя и в случае выигрыша перепроверяют результат розыгрыша электронной лотереи перед выдачей призов, для чего получают с сервера недостающие данные: сигналы, подписанные электронной цифровой подписью, включающие в себя код, переданный пользователю, вариант результата преобразования кода из конечного числа возможных вариантов выбранный пользователем и показания системного времени отправки кода пользователю и получения от него ответного сигнала.



Фиг.1



Фиг.2



Фиг.3

PATENT COOPERATION TREATY

PCT

DECLARATION OF NON-ESTABLISHMENT OF INTERNATIONAL SEARCH REPORT

(PCT Article 17(2)(a), Rules 13^{ter}.1(c) and (d) and 39)

Applicant's or agent's file reference	IMPORTANT DECLARATION	Date of mailing (<i>day/month/year</i>) 04 October 2007 (04.10.2007)
International application No. PCT/RU 2007/000229	International filing date (<i>day/month/year</i>) 08 May 2007 (08.05.2007)	(Earliest) Priority Date (<i>day/month/year</i>) 10 May 2007 (10.05.2007)
International Patent Classification (IPC) or both national classification and IPC		A63F 3/06 (2006.01) G06Q 50/00 (2006.01)
Applicant GERTNER, Dmitry Aleksandrovich		

This International Searching Authority hereby declares, according to Article 17(2)(a), that **no international search report will be established** on the international application for the reasons indicated below.

1. ☒ The subject matter of the international application relates to:
 - a. ☐ scientific theories
 - b. ☐ mathematical theories
 - c. ☐ plant varieties
 - d. ☐ animal varieties
 - e. ☐ essentially biological processes for the production of plants and animals, other than microbiological processes and the products of such processes
 - f. ☐ schemes, rules or methods of doing business
 - g. ☐ schemes, rules or methods of performing purely mental acts
 - h. ☒ schemes, rules or methods of playing games
 - i. ☐ methods for treatment of the human body by surgery or therapy
 - j. ☐ methods for treatment of the animal body by surgery or therapy
 - k. ☐ diagnostic methods practised on the human or animal body
 - l. ☐ mere presentations of information
 - m. ☐ computer programs for which this International Searching Authority is not equipped to search prior art
2. ☐ The failure of the following parts of the international application to comply with prescribed requirements prevents a meaningful search from being carried out:

☐ the description
 ☐ the claims
 ☐ the drawings
3. ☐ A meaningful search could not be carried out without the sequence listing; the applicant did not, within the prescribed time limit:

☐ furnish a sequence listing on paper complying with the standard provided for in Annex C of the Administrative Instructions, and such listing was not available to the International Searching Authority in a form and manner acceptable to it.
☐ furnish a sequence listing in electronic form complying with the standard provided for in Annex C of the Administrative Instructions, and such listing was not available to the International Searching Authority in a form and manner acceptable to it.
☐ pay the required late furnishing fee for the furnishing of a sequence listing in response to an invitation under Rule 13^{ter}.1(a) or (b).
4. ☐ A meaningful search could not be carried out without the tables related to the sequence listings; the applicant did not, within the prescribed time limit, furnish such tables in electronic form complying with the technical requirements provided for in Annex C-bis of the Administrative Instructions, and such tables were not available to the International Searching Authority in a form and manner acceptable to it.
5. Further comments:

Name and mailing address of the ISA/	Authorized officer
Facsimile No.	Telephone No.

ДОГОВОР О ПАТЕНТНОЙ КООПЕРАЦИИ РСТ

декларация о невозможности подготовки отчета о международном поиске (РСТ статья 17(2)(а), Правила 13ter.1 (c) и (d) and 39)

№ дела заявителя:	ВАЖНОЕ УВЕДОМЛЕНИЕ	Дата отправки: 04 октября 2007 (04.10.2007)
Международная заявка: PCT/RU 2007/000229	Дата международной подачи: 08 мая 2007 (08.05.2007)	Самая ранняя дата приоритета: 10 мая 2006 (10.05.2006)
Международная патентная классификация (МПК) или национальная классификация и МПК A63F 3/06 (2006.01)i G06Q 50/00 (2006.01)i		
Заявитель: ГЕРТНЕР Дмитрий Александрович		

Международный поисковый орган уведомляет, что в соответствии со Статьей 17(2)(а) отчет о международном поиске не будет подготовлен по следующим причинам.

1. ☒ Объект международной заявки относится к следующему:

- а. ☐ научные теории
- б. ☐ математические теории
- в. ☐ сорта растений
- г. ☐ породы животных
- д. ☐ чисто биологические способы выращивания растений и животных, за исключением микробиологических способов и продуктов, полученных такими способами
- е. ☐ схемы, правила и методы организации производства
- ж. ☐ схемы, правила и методы выполнения чисто умственных расчетов
- з. ☒ схемы, правила и методы выполнения игр
- и. ☐ оперативные или терапевтические методы лечения людей
- к. ☐ оперативные или терапевтические методы лечения животных
- л. ☐ способы диагностики заболеваний людей или животных
- м. ☐ простое изложение информации
- н. ☐ вычислительные программы в той мере, в какой Международный поисковый орган не оснащен для проведения поиска по определению уровня техники в отношении таких программ

2. ☐ Часть международной заявки, которая не удовлетворяет установленным требованиям настолько, что проведение полноценного поиска невозможно:

- ☐ описание ☐ формула изобретения ☐ рисунки

3. ☐ Полноценный поиск не мог быть проведен без перечня последовательностей; заявитель в установленный срок:

- ☐ не представил перечень последовательностей на бумаге, соответствующий стандарту, предусмотренному в приложении С Административной инструкции, и такой перечень не был доступен Международному поисковому органу в форме и способом, приемлемым для него.
- ☐ не представил перечень последовательностей в электронной форме, соответствующий стандарту, предусмотренному в приложении С Административной инструкции, и такой перечень не был доступен Международному поисковому органу в форме и способом, приемлемым для него.
- ☐ не оплатил требуемую пошлину за позднее представление для представления перечня последовательностей в ответ на предложение согласно Правилу 13ter.1(a) или (b).

4. ☐ Полноценный поиск не мог быть проведен без таблиц, относящихся к перечню последовательностей; заявитель не представил в установленный срок такие таблицы в электронной форме, соответствующей техническим требованиям, предусмотренным приложением C-bis Административной инструкции, и такие таблицы не были доступны Международному поисковому органу в форме и способом, приемлемым для него.

5. Дополнительные пояснения: см. дополнительный лист

Наименование и адрес Международного поискового органа: Федеральный институт промышленной собственности, Россия, 123995, Москва, Г-59, ГСП - 5, Бережковская наб., 30-1 факс: 243-3337	Уполномоченное лицо: А.Никитин Телефон № (095) 240-25-91
---	---