

(19)



**Евразийское
патентное
ведомство**

(21) **201892372** (13) **A1**

(12) **ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ**

(43) Дата публикации заявки
2020.05.29

(51) Int. Cl. **G06F 21/56** (2006.01)

(22) Дата подачи заявки
2018.11.19

(54) **СПОСОБ И СИСТЕМА ВЫЯВЛЕНИЯ УСТРОЙСТВ, СВЯЗАННЫХ С
МОШЕННИЧЕСКОЙ ФИШИНГОВОЙ АКТИВНОСТЬЮ**

(31) **2018140413**

(72) Изобретатель:

(32) **2018.11.15**

Оболенский Иван Александрович,

(33) **RU**

Анистратенко Александр Артурович

(71) Заявитель:

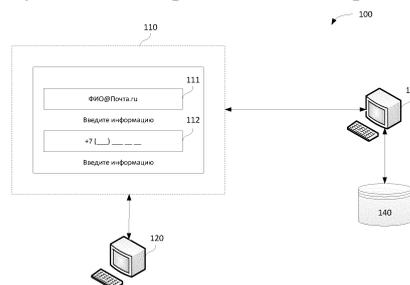
(RU)

**ПУБЛИЧНОЕ АКЦИОНЕРНОЕ
ОБЩЕСТВО "СБЕРБАНК
РОССИИ" (ПАО СБЕРБАНК) (RU)**

(74) Представитель:

Герасин Б.В. (RU)

(57) Заявленное изобретение относится к области вычислительной техники, в частности к способу и системе выявления устройств, связанных с мошеннической фишинговой активностью. Технический результат заключается в повышении защиты информационных продуктов за счет идентификации устройств мошенников, связанных с фишинговыми веб-ресурсами, для их последующего блокирования при попытках доступа к информационным продуктам с помощью данных пользователей. Способ выявления устройств, связанных с мошеннической фишинговой активностью, содержит этапы, на которых с помощью процессора вычислительного устройства: а) определяют веб-сайт подлежащий проверке на предмет фишинговой активности; б) выявляют элементы интерфейса веб-сайта, представляющие по меньшей мере одну форму для ввода данных, причем веб-сайт предназначен для перехвата регистрационных данных пользователя, относящихся к финансовому продукту или услуге; в) определяют по меньшей мере одну область интерфейса для ввода текста в форму ввода данных; д) определяют тип данных, подлежащий вводу в каждую из выявленных форм для ввода данных; е) выполняют обращение к базе данных, содержащей трекингтовую информацию, необходимую для ввода данных по меньшей мере в одну форму данных, выявленную на этапе д); ф) осуществляют автоматическое заполнение каждой из упомянутой формы упомянутыми трекингтовыми данными; г) выполняют регистрацию на веб-сайте с помощью упомянутых трекингтовых данных для доступа к финансовой услуге или продукту; з) осуществляют мониторинг активности использования упомянутых трекингтовых данных по меньшей мере для одного устройства, связанного с мошеннической активностью; и) получают на основании упомянутого мониторинга уникальный аппаратный идентификатор (УАИД) упомянутого устройства, связанного с мошеннической активностью; и) передают УАИД в базу данных для добавления в черный список для последующего блокирования транзакционных операций с помощью соответствующего аппаратного идентификатора.



**201892372
A1**

**201892372
A1**

СПОСОБ И СИСТЕМА ВЫЯВЛЕНИЯ УСТРОЙСТВ, СВЯЗАННЫХ С МОШЕННИЧЕСКОЙ ФИШИНГОВОЙ АКТИВНОСТЬЮ

ОБЛАСТЬ ТЕХНИКИ

[0001] Заявленное техническое решение, в общем, относится к области вычислительной техники, а в частности, к способу и системе выявления устройств, связанных с мошеннической фишинговой активностью.

УРОВЕНЬ ТЕХНИКИ

[0002] По мере стремительного развития ИТ-сервисов, все больше банковских и финансовых услуг осуществляются с помощью онлайн доступа в сети Интернет. При этом остро стоит необходимость в реализации защитных механизмов от мошеннических действий злоумышленников, которые осуществляются с помощью веб-сайтов, направленных на фишинг данных пользователей.

[0003] Фишинг представляет собой вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям с помощью специально создаваемых ресурсов в сети Интернет, которые маскируются под оригинальный бренд, предоставляющий те или иные услуги, и ставят своей целью захват идентификационных данных пользователей при их вводе в формы, размещенные на таковых веб-сайтах.

[0004] Из уровня техники известно решение по мониторингу подозрительной активности пользователя на основании шаблона поведения пользователя при осуществлении финансовых транзакций или доступа к различным финансовым ресурсам (заявка US20130275195, дата приоритета: 17.10.2013). Способ основан на формировании эталонного шаблона пользовательского поведения для одного или нескольких устройств и последующего его использования по идентификационной информации пользователя с помощью сравнения текущих действий пользователя с упомянутым шаблоном.

[0005] Аналогом заявленного технического решения является способ «бэйтинга» мошеннических схем в сети Интернет, реализуемых с помощью веб-сайтов (заявка US20140041024, дата приоритета: 06.02.2014). Суть способа заключается в автоматизированном анализе полей ввода информации на веб-ресурсах и применении принципа подстановки данных, имитирующих ввод информации, идентифицирующей пользователя.

[0006] Недостатком известных решений является принцип выявления данных, идентифицирующих непосредственно фишинговый веб-ресурс или программное приложение для их последующего добавления в черный список и блокирования обработки запросов через упомянутые ресурсы. При этом само устройство или группа устройств, с помощью которых осуществляется перехват и последующее использование данных пользователей, не выявляются, и смена веб-сайтов позволяет далее применять аппаратные средства мошенников для перехвата пользовательских данных.

РАСКРЫТИЕ ИЗОБРЕТЕНИЯ

[0007] Заявленное решение обеспечивает решение технической проблемы или технической задачи, заключающейся в необходимости идентификации непосредственно аппаратных средств злоумышленников, которые связаны с фишинговыми веб-ресурсами.

[0008] Технический результат, достигаемый при решении указанной технической проблемы, заключается в повышении защиты информационных продуктов за счет идентификации устройств мошенников, связанных с фишинговыми веб-ресурсами, для их последующего блокирования при попытках доступа к информационным продуктам с помощью данных пользователей.

[0009] Заявленный технический результат достигается за счет осуществления способа выявления устройств, связанных с мошеннической фишинговой активностью, содержащий этапы, на которых с помощью процессора вычислительного устройства выполняют:

- a) определение веб-сайта, подлежащего проверке на предмет фишинговой активности;
- b) выявляют элементы интерфейса веб-сайта, представляющую по меньшей мере одну форму для ввода данных, причем веб-сайт предназначен для перехвата регистрационных данных пользователя, относящихся к финансовому продукту или услуге;
- c) определяют по меньшей мере одну область интерфейса для ввода текста в форму ввода данных;
- d) определяют тип данных, подлежащий вводу в каждую из выявленных форм для ввода данных;
- e) выполняют обращение к базе данных, содержащей трекингтовую информацию, необходимую для ввода данных по меньшей мере одну форму данных, выявленную на этапе d);
- f) осуществляют автоматическое заполнение каждой из упомянутой формы упомянутыми трекингтовыми данными;

- g) выполняют регистрацию на веб-сайте с помощью упомянутых трекинговых данных для доступа к финансовой услуге или продукту;
- h) осуществляют мониторинг активности использования упомянутых трекинговых данных для по меньшей мере одного устройства, связанного с мошеннической активностью;
- i) получают на основании упомянутого мониторинга уникальный аппаратный идентификатор (УАИД) упомянутого устройства, связанного с мошеннической активностью;
- j) передают УАИД в базу данных для добавления в черный список для последующего блокирования транзакционных операций с помощью соответствующего аппаратного идентификатора.

[0010] В частном варианте выполнения способа, элементы, представляющие форму для ввода данных, выбираются из группы: кнопка графического интерфейса, область ввода текста, рамка, ссылка на переход с сайта.

[0011] В частном варианте выполнения способа, этап f) начинается после полной загрузки страницы веб-сайта и дополнительно установленного временного промежутка.

[0012] В частном варианте выполнения способа, для каждой области текста проверяется наличие элементов автозаполнения.

[0013] В частном варианте выполнения способа, для элементов автозаполнения определяется количество пунктов вариантов автозаполнения.

[0014] В частном варианте выполнения способа, выполняется случайный выбор пунктов вариантов автозаполнения.

[0015] В частном варианте выполнения способа, для каждой области текста проверяется наличие шаблона текста для ввода.

[0016] В частном варианте выполнения способа, шаблон проверяется на наличие ключевых слов.

[0017] В частном варианте выполнения способа, по выявленным ключевым словам выполняется обращение в базу данных трекинговой информации для получения данных, соответствующих шаблону для заполнения.

[0018] В частном варианте выполнения способа, проверка выполняется по DOM-дереву и/или с помощью локатора близлежащих элементов, содержащих текст, длиной не менее 3х символов.

[0019] В частном варианте выполнения способа, в случае если шаблон содержит ключевые слова, указывающие на подтверждение регистрации с помощью SMS-сообщения, то выполняется шаг его отправки на номер телефона, связанный с трекинговыми данными.

[0020] В частном варианте выполнения способа, определяют поступление SMS-сообщения с на указанный номер телефона, связанный с трекинговыми данными.

[0021] В частном варианте выполнения способа, определение выполняется с помощью программного модуля, определяющего поступление SMS-сообщения и его передачу в базу данных.

[0022] В частном варианте выполнения способа, информация, переданная в базу данных, проверяется модулем анализа на наличие информации для авторизации в полученном SMS-сообщении.

[0023] Заявленное решение реализуется также за счет системы выявления устройств, связанных с мошеннической фишинговой активностью, которая содержит:

по меньшей мере один процессор;

по меньшей мере одну память, связанную с процессором, содержащую машиночитаемые инструкции, которые при их выполнении по меньшей мере одним процессором осуществляют вышеуказанный способ.

ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0024] Признаки и преимущества настоящего технического решения станут очевидными из приводимого ниже подробного описания и прилагаемых чертежей, на которых:

[0025] Фиг. 1 иллюстрирует общий вид заявленного решения.

[0026] Фиг. 2 иллюстрирует блок-схему выполнения заявленного способа.

[0027] Фиг. 3 иллюстрирует пример решения с формой на веб-сайте с выбором вариантов для заполнения.

[0028] Фиг. 4 иллюстрирует общий вид вычислительного устройства.

ОСУЩЕСТВЛЕНИЕ ИЗОБРЕТЕНИЯ

[0029] В контексте настоящего описания, если четко не указано иное, «сервер» подразумевает под собой компьютерную программу, работающую на соответствующем оборудовании, которая способна получать запросы (например, от клиентских устройств) по сети и выполнять эти запросы или инициировать выполнение этих запросов. Оборудование может представлять собой один физический компьютер или одну физическую компьютерную систему, но ни то, ни другое не является обязательным для данной технологии. В контексте настоящей технологии использование выражения «сервер» не означает, что каждая задача (например, полученные инструкции или запросы) или какая-

либо конкретная задача будет получена, выполнена или инициирована к выполнению одним и тем же сервером (то есть одним и тем же программным обеспечением и/или аппаратным обеспечением); это означает, что любое количество элементов программного обеспечения или аппаратных устройств может быть вовлечено в прием/передачу, выполнение или инициирование выполнения любого запроса или последствия любого запроса, связанного с клиентским устройством, и все это программное и аппаратное обеспечение может являться одним сервером или несколькими серверами, оба варианта включены в выражение «по меньшей мере один сервер».

[0030] В контексте настоящего описания, если четко не указано иное, «клиентское устройство пользователя» или «мобильное устройство связи пользователя» подразумевает под собой аппаратное устройство, способное работать с программным обеспечением, подходящим к решению соответствующей задачи. Таким образом, примерами клиентских устройств (среди прочего) могут служить персональные компьютеры (настольные компьютеры, ноутбуки, нетбуки и т.п.), смартфоны, планшеты, а также сетевое оборудование, такое как маршрутизаторы, коммутаторы и шлюзы. Следует иметь в виду, что устройство, ведущее себя как устройство пользователя в настоящем контексте, может вести себя как сервер по отношению к другим клиентским устройствам. Использование выражения «клиентское устройство» не исключает возможности использования множества клиентских устройств для получения/отправки, выполнения или инициирования выполнения любой задачи или запроса, или же последствий любой задачи или запроса, или же этапов любого вышеописанного метода.

[0031] В контексте настоящего описания, если четко не указано иное, термин «база данных» подразумевает под собой любой структурированный набор данных, не зависящий от конкретной структуры, программного обеспечения по управлению базой данных, аппаратного обеспечения компьютера, на котором данные хранятся, используются или иным образом оказываются доступны для использования. База данных может находиться на том же оборудовании, которое выполняет процесс, который сохраняет или использует информацию, хранящуюся в базе данных, или же она может находиться на отдельном оборудовании, например, выделенном сервере или множестве серверов.

[0032] В контексте настоящего описания, если четко не указано иное, термин «информация» включает в себя любую информацию, которая может храниться в базе данных. Таким образом, информация включает в себя, среди прочего, аудиовизуальные произведения (изображения, видео, звукозаписи, презентации и т.д.), данные (данные о местоположении, цифровые данные и т.д.), текст (мнения, комментарии, вопросы, сообщения и т.д.), документы, таблицы и т.д.

[0033] На Фиг. 1 представлен общий вид представленного технического решения (100). Система взаимодействия элементов решения включает в себя веб-сайт (110), анализируемый на предмет фишинга, связанное с веб-сайтом (110) одно или более устройств мошенников (120), сервер (130), осуществляющий анализ веб-сайта (110) и необходимые действия по идентификации устройств (120) мошенников, и связанную с сервером (130) базу данных (140), содержащую данные, применяемые для подстановки на веб-сайте (110) для отслеживания фишинговой активности и связанных с ней устройств (120).

[0034] В качестве устройства мошенников (120) могут применяться различные средства, например, компьютеры, сервера, смартфоны, планшеты и т.п. Основная специфика устройства (120) в данном случае заключается в непосредственном доступе с помощью перехваченных данных пользователя к финансовым и/или банковским услугам, или регистрации пользователя на подставных веб-ресурсах для последующего трекинга и перехвата поступающей информации от пользователя.

[0035] Реализация заявленного решения осуществляется с помощью программно-аппаратного комплекса, воплощенного с помощью сервера (130) и соответствующего программного приложения, обеспечивающего анализ веб-сайтов (110) и выявления подозрительной активности, направленной на совершение мошеннических действий.

[0036] Как правило, веб-ресурс (110), применяемый для фишинга данных пользователя, содержит одну или несколько форм (111, 112) для ввода идентифицирующей пользователя информации, например, номера телефона, адреса электронной почты, ФИО пользователя, идентификатора пользователя и т.п.

[0037] Алгоритм работы аналитического модуля сервера (130) осуществляет анализ форм (111, 112) веб-сайта (110) на предмет необходимой для введения в них информации и выполнению дальнейшего отслеживания движения потоков данных для выявления устройств (120), участвующих в цепочке обмена и использованию данных пользователей.

[0038] На Фиг. 2 представлен алгоритм работы заявленного способа (200) по выявлению устройств (120) мошенников, связанных с фишинговыми веб-сайтами (110).

[0039] В начале работы способа (200) осуществляется анализ сведений веб-сайта (110) на предмет его использования для фишинга данных пользователей (201). Данная проверка может осуществляться с помощью анализа IP-адреса или домена веб-сайта (110) с базой данных (140), в которой может храниться обновляемый список веб-ресурсов, подлежащих проверки на предмет фишинговой активности.

[0040] Далее на этапе (202) выполняется анализ типов объектов на странице веб-сайта (110) по их атрибутам типа в языке разметки HTML для выявления элементов интерфейса,

представляющих формы для ввода данных (111, 112), которые используются для перехвата регистрационных данных пользователя, относящихся к финансовому продукту или услуге. Элементы, представляющие форму для ввода данных, выбираются из группы: кнопка графического интерфейса, область ввода текста, рамка, ссылка на переход с сайта и т.п.

[0041] Этап (202) может выполняться после полной загрузки страницы веб-сайта (110) и дополнительно установленного временного промежутка, например, 10 сек. Временной промежуток используется для обхода защиты от автозаполнения, при которой некоторые элементы формы веб-сайта (110) могут не отображаться сразу, имитируя загрузку.

[0042] После выявления одной или нескольких форм для ввода текста (111, 112), на этапе (203) выполняется анализ областей интерфейса для ввода текстовых или числовых данных в выявленные формы (111, 112).

[0043] На этапе (204) алгоритм анализа, выполняемый сервером (130), производит поиск текстовой информации, описывающей тип данных, подлежащих к вводу в соответствующие области форм (111, 112). Поиск может осуществляться с помощью анализа как области интерфейса рядом с полем ввода форм (111, 112), так и непосредственно внутри поля форм (111, 112), который может являться шаблоном информации, необходимой к заполнению, например, формат номера телефона, формат имени и фамилии и т.п.

[0044] Если текстовый или числовой пример вводимой информации в самом поле форм (111, 112) выявлен, то алгоритм, выполняемый сервером (130), активирует анализ ключевых слов, упомянутого примера символьного ввода. Если пример вводимой информации отсутствует, то происходит поиск ближайшего элемента к полю форм (111, 112) с подписью, поясняющей какую информацию нужно ввести в данное поле. Данная проверка может выполняться с помощью анализа DOM-дерева (Document Object Model), или с помощью локаторов типа XPath, близлежащих элементов, содержащих текст, длиной не менее трех символов.

[0045] После нахождения элемента, содержащего подпись к полю ввода, элемент проматывается до середины экрана, после чего делается скриншот. Затем, по координатам данного объекта, из скриншота вырезается интересующее поле, после чего, полученная картинка увеличивается в несколько раз, например, три раза и переводится в монохромное изображение, для увеличения качества распознавания текста. Эти действия необходимы для обхода защиты от автоматического заполнения – часто используются не кириллические символы, а похожие на них по написанию, другие символы, например, латиница и т.д.

[0046] Далее полученное изображение передается на распознавание с помощью модуля OCR (Optical Character Recognition). Результат распознавания текста проверяется на наличие

необходимых ключевых слов. Если при проверке не найдены ключевые слова, то поля ввода форм (111, 112) заполняются значением, заданным по умолчанию (например, случайным именем).

[0047] На этапе (205) осуществляется подстановка трекинговой информации в формы ввода текста (111, 112) на веб-сайте (110). Трекинговая информация, как правило, содержится в базе данных (140), связанной с сервером (130), и представляет собой заранее подготовленные сгенерированные данные, имитирующие персональную информацию пользователей. Для каждого данных в базе (140) содержится также номер телефона для целей осуществления регистрации на фишинговых ресурсах (110).

[0048] Трекинговая информация заполняется в выявленные формы (111, 112) на веб-сайте (110) с помощью алгоритма, реализуемого сервером (130). Трекинговая информация запрашивается из базы данных (140) в соответствии с определенными типами необходимых данных, подлежащих вводу в формы (111, 112) на веб-сайте (110) и вводится в упомянутые формы (111, 112). При этом, в процессе автозаполнения форм (111, 112) на веб-сайте (110) с помощью сервера (130) также анализируется и получается информация, идентифицирующая веб-сайт (110), в частности, IP-адрес, доменное имя, URL и т.п.

[0049] После того как трекинговые данные были введены (206) на веб-сайте (110) выполняется процедура регистрации на фишинговом ресурсе (110). Трекинговые данные, как правило, передаются на одно или несколько устройств мошенников (120) для последующего их использования.

[0050] Веб-сайт (110) может также содержать запрос на подтверждение процесса регистрации с помощью двухфакторной верификации, в частности, с помощью ввода кода подтверждения из SMS-сообщения, которое направляется по номеру мобильного телефона или адресу электронной почты пользователя. В этом случае, для записей трекинговой информации в базе данных (140) хранится один или несколько номеров телефона, используемый для получения кода подтверждения, или адресов электронной почты. После анализа веб-сайта (110) на предмет необходимости ввода кода подтверждения авторизации, алгоритм сервера (130) осуществляет отслеживание поступления кода по указанным трекинговым данным, и при поступлении необходимого кода подтверждения в SMS-сообщении или электронном письме осуществляет его ввод в соответствующую форму веб-сайта (110).

[0051] Далее алгоритм работы сервера (130) осуществляет мониторинг использования введенных трекинговых данных (207). Мошенники, как правило, осуществляют регистрационные действия с финансовыми продуктами или услугами с помощью данных пользователя, полученные с помощью веб-сайта (110). Регистрация выполняется с

помощью устройства (120) мошенника для выполнения будущих операций, например, попытки получения доступа к финансовому счету пользователя или связанным с ними финансовыми сервисами.

[0052] В момент применения трекинговых данных с помощью устройств мошенников (120) на этапе (208) выполняется получение их уникальных аппаратных идентификаторов (УАИД), которые впоследствии заносятся в черный список для блокирования выполнения активности, связанной с финансовыми сервисами (209). Блокирование действий устройств (120) выполняется с помощью сравнения их УАИД с информацией, внесенной в черный список. УАИД также позволяет отследить группу устройств (120), которые участвуют в мошеннической схеме, что реализует возможность блокирования нескольких устройств, пытающихся получить доступ к услугам с помощью данных пользователей.

[0053] УАИД устройства (120) определяется на основании логов мониторинга процессе применения трекинговых данных для финансовых продуктов или услуг. Как пример, злоумышленники, получившие с помощью веб-сайта (110) данные пользователей, могут попытаться осуществить регистрацию в таких финансовых продуктах как мобильный банкинг (Сбербанк Онлайн), программы лояльности (например, Сбербанк Спасибо) и т.п. для совершения финансовых транзакций или операций по информации, полученной с помощью фишингового веб-сайта (110). УАИД при регистрации с помощью устройств (120) по трекинговым данным сервера (130) может определяться как хэш от конкатенации настроек окружения операционной системы телефона, разрешением экрана, набором установленного программного обеспечения, настройками программного обеспечения на телефоне и других характеристик устройства мошенника (120). Конкатенация представляет собой операцию объединения объектов линейной структуры, например, строк данных, символов, значений и т.п.

[0054] Ниже будет представлен пример получения УАИД по хэшу от конкатенации данных с устройства (120) мошенника по трекинговым данным.

PHONE_PARAMETERS_STRING:

```
pm_fposp=&pm_fpacn=Mozilla&BROWSER=mozilla/5.0+(windows+nt+6.1;+wow64)+applewebkit/537.36+(khtml,+like+gecko)+chrome/43.0.2357.132+safari/537.36|5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/43.0.2357.132+Safari/537.36|Win32&EXTERNAL_TIMEOUT=&BROWSER_TYPE=Chrome&SUPPRESSED=false&LANGUAGE=lang%3Dru|syslang%3D|userlang%3D&version=3.4.0.0_2&BROWSER_MAJOR_VERSION=43&pm_fpspd=24&pm_fpsaw=1440&LANGUAGE_BROWSER=ru&DISPLAY=24|1440|900|860&JAVA=1&OS=Windows&COOKIE=1&SOFTWARE=&pm_fgup=&pm_fpol=true&pm_fpsbd=&ACCEPT_LANGUAGE=ru-RU,ru;q%3D0.8,en-
```

US;q%3D0.6,en;q%3D0.4&pm_fpsfse=&pm_fpslx=&pm_fpsly=&TIMEZONE=4&pm_fpan=N
etscape&pm_fpasw=widevinecdmadapter|mhjfbmdgcfjbbpaeojofohoefgihjai|pepflashplayer|int
ernal-remoting-viewer|internal-nacl-plugin|internal-pdf-
viewer&pm_fpsdx=&pm_fpsui=&pm_fpsdy=&INTERNAL_TIMEOUT=

**DEVICE_ID = sha256 (PHONE_PARAMETERS_STRING) =
ad83f8280f66ae603b4e1ab58795bba63bb7ca62d7b971fabe10b040825868a8 .**

[0055] На Фиг. 3 представлен пример частного случая анализа форм для ввода информации (113) на этапе (203). Некоторые типы форм (113) могут содержать элементы автозаполнения (1131, 1132, 1133), которые выбираются при взаимодействии с веб-сайтом (110). В этом случае алгоритм сервера (130) осуществляет анализ информации, представленный в элементах (1131, 1132, 1133) формы автозаполнения (113). Осуществляется проверка количества пунктов в каждом списке форм (113) и пункты (элементы) (1131, 1132, 1133) формы выбираются в случайном порядке. После выбора элементов для автозаполнения формы (113) алгоритм продолжает свою работу по анализу веб-сайта (110) на предмет полей форм для ввода пользовательской информации для целей регистрации на веб-сайте (110).

[0056] На Фиг. 4 представлен общий вид вычислительного устройства (300). На базе устройства (300) может быть реализовано мошенническое устройство (120), сервер (130) и иные непредставленные устройства, но которые могут участвовать в общей информационной архитектуре (100) заявленного решения.

[0057] В общем случае, вычислительное устройство (300) содержит объединенные общей шиной информационного обмена один или несколько процессоров (301), средства памяти, такие как ОЗУ (302) и ПЗУ (303), интерфейсы ввода/вывода (304), устройства ввода/вывода (305), и устройство для сетевого взаимодействия (306).

[0058] Процессор (301) (или несколько процессоров, многоядерный процессор) могут выбираться из ассортимента устройств, широко применяемых в текущее время, например, компаний Intel™, AMD™, Apple™, Samsung Exynos™, MediaTek™, Qualcomm Snapdragon™ и т.п.

[0059] ОЗУ (302) представляет собой оперативную память и предназначено для хранения исполняемых процессором (301) машиночитаемых инструкций для выполнение необходимых операций по логической обработке данных. ОЗУ (302), как правило, содержит исполняемые инструкции операционной системы и соответствующих программных компонент (приложения, программные модули и т.п.).

[0060] ПЗУ (303) представляет собой одно или более устройств постоянного хранения данных, например, жесткий диск (HDD), твердотельный накопитель данных (SSD), флэш-

память (EEPROM, NAND и т.п.), оптические носители информации (CD-R/RW, DVD-R/RW, BlueRay Disc, MD) и др.

[0061] Для организации работы компонентов устройства (300) и организации работы внешних подключаемых устройств применяются различные виды интерфейсов В/В (304). Выбор соответствующих интерфейсов зависит от конкретного исполнения вычислительного устройства, которые могут представлять собой, не ограничиваясь: PCI, AGP, PS/2, IrDa, FireWire, LPT, COM, SATA, IDE, Lightning, USB (2.0, 3.0, 3.1, micro, mini, type C), TRS/Audio jack (2.5, 3.5, 6.35), HDMI, DVI, VGA, Display Port, RJ45, RS232 и т.п.

[0062] Для обеспечения взаимодействия пользователя с вычислительным устройством (300) применяются различные средства (305) В/В информации, например, клавиатура, дисплей (монитор), сенсорный дисплей, тач-пад, джойстик, манипулятор мышь, световое перо, стилус, сенсорная панель, трекбол, динамики, микрофон, средства дополненной реальности, оптические сенсоры, планшет, световые индикаторы, проектор, камера, средства биометрической идентификации (сканер сетчатки глаза, сканер отпечатков пальцев, модуль распознавания голоса) и т.п.

[0063] Средство сетевого взаимодействия (306) обеспечивает передачу данных устройством (300) посредством внутренней или внешней вычислительной сети, например, Интранет, Интернет, ЛВС и т.п. В качестве одного или более средств (306) может использоваться, но не ограничиваясь: Ethernet карта, GSM модем, GPRS модем, LTE модем, 5G модем, модуль спутниковой связи, NFC модуль, Bluetooth и/или BLE модуль, Wi-Fi модуль и др.

[0064] Дополнительно могут применяться также средства спутниковой навигации в составе устройства (300), например, GPS, ГЛОНАСС, BeiDou, Galileo.

[0065] Представленные материалы заявки раскрывают предпочтительные примеры реализации технического решения и не должны трактоваться как ограничивающие иные, частные примеры его воплощения, не выходящие за пределы испрашиваемой правовой охраны, которые являются очевидными для специалистов соответствующей области техники.

ФОРМУЛА

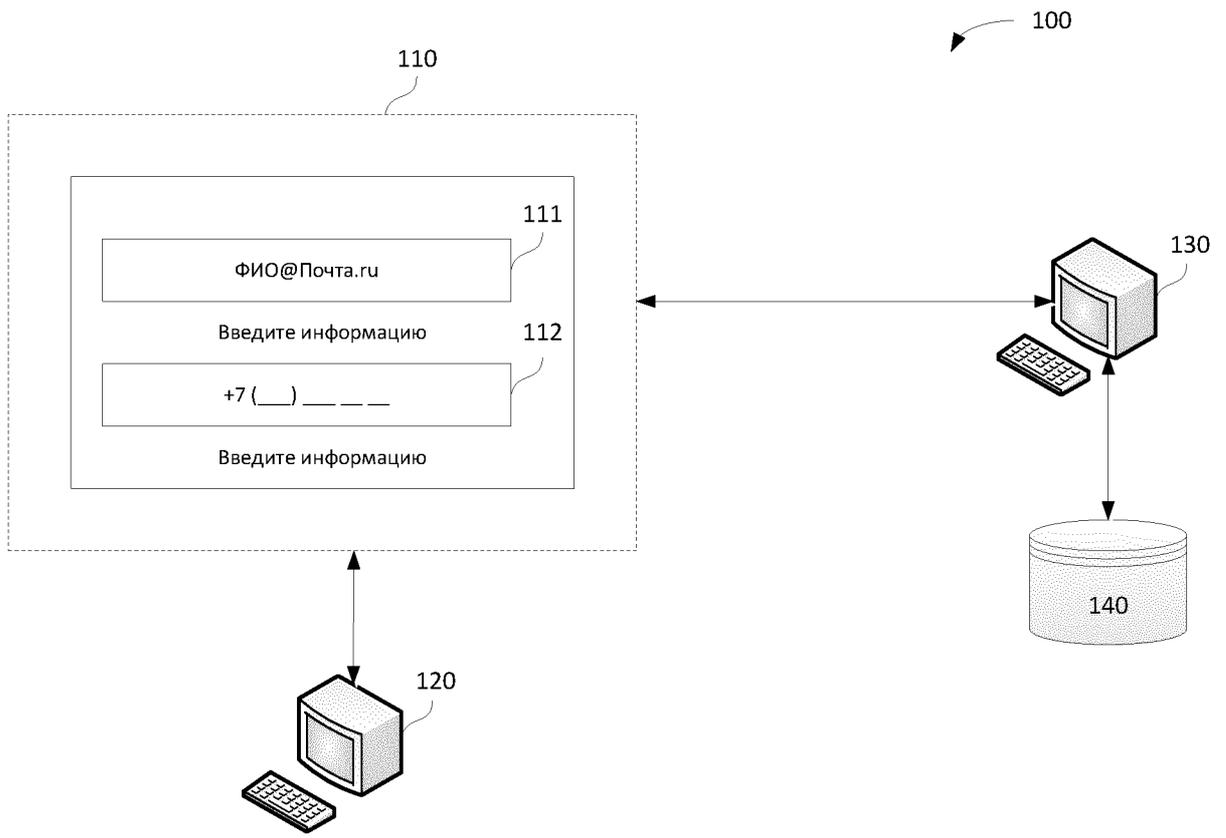
1. Способ выявления устройств, связанных с мошеннической фишинговой активностью, содержащий этапы, на которых:

осуществляют с помощью процессора вычислительного устройства

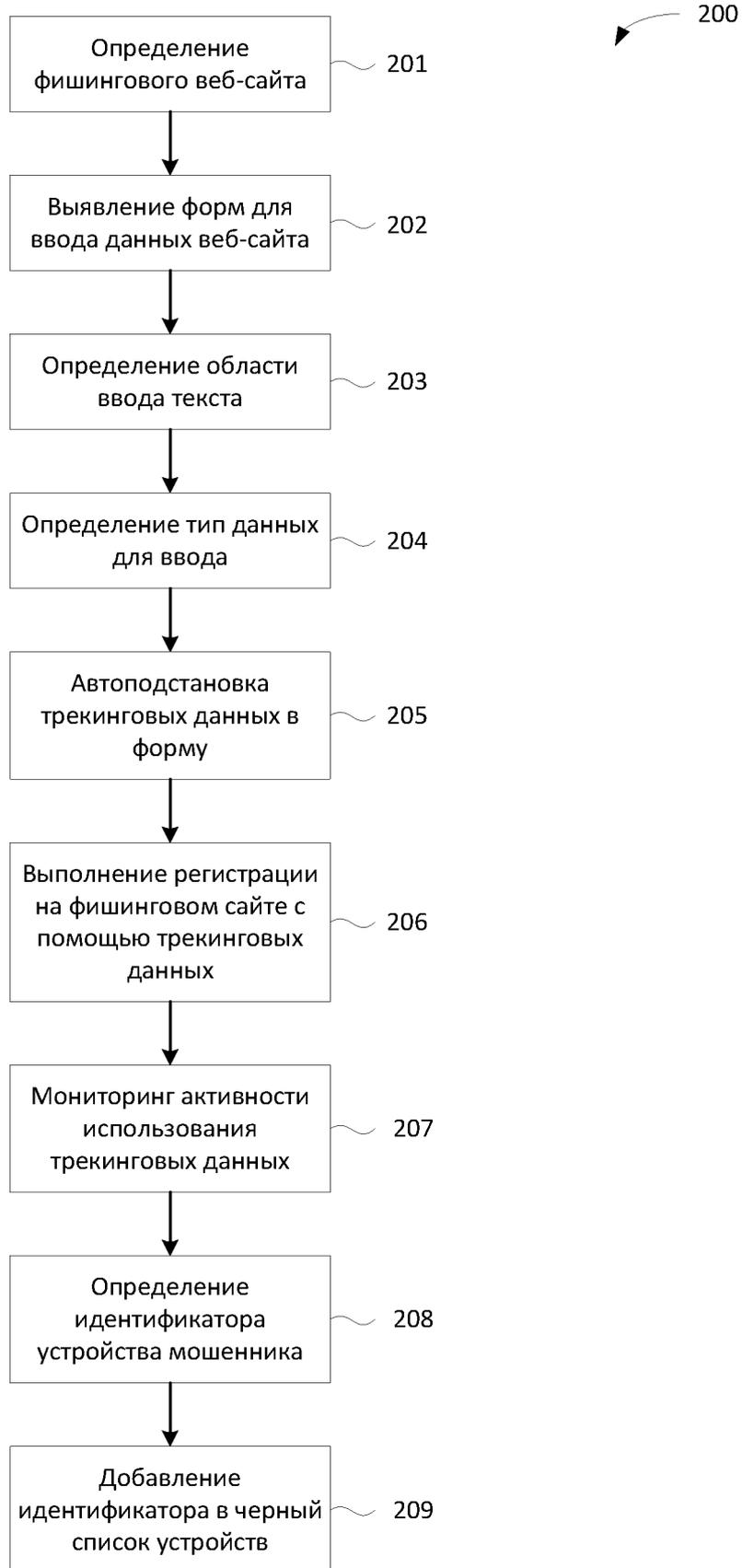
- a) определение веб-сайта, подлежащего проверке на предмет фишинговой активности;
- b) выявляют элементы интерфейса веб-сайта, представляющую по меньшей мере одну форму для ввода данных, причем веб-сайт предназначен для перехвата регистрационных данных пользователя, относящихся к финансовому продукту или услуге;
- c) определяют по меньшей мере одну область интерфейса для ввода текста в форму ввода данных;
- d) определяют тип данных, подлежащий вводу в каждую из выявленных форм для ввода данных;
- e) выполняют обращение к базе данных, содержащей трекингую информацию, необходимую для ввода данных в по меньшей мере одну форму данных, выявленную на этапе d);
- f) осуществляют автоматическое заполнение каждой из упомянутой формы упомянутыми трекингowymi данными;
- g) выполняют регистрацию на веб-сайте с помощью упомянутых трекингowych данных для доступа к финансовой услуге или продукту;
- h) осуществляют мониторинг активности использования упомянутых трекингowych данных для по меньшей мере одного устройства, связанного с мошеннической активностью;
- i) получают на основании упомянутого мониторинга уникальный аппаратный идентификатор (УАИД) упомянутого устройства, связанного с мошеннической активностью; и
- j) передают УАИД в базу данных для добавления в черный список для последующего блокирования транзакционных операций с помощью соответствующего аппаратного идентификатора.

2. Способ по п.1, характеризующийся тем, что элементы, представляющие форму для ввода данных, выбираются из группы: кнопка графического интерфейса, область ввода текста, рамка, ссылка на переход с сайта.

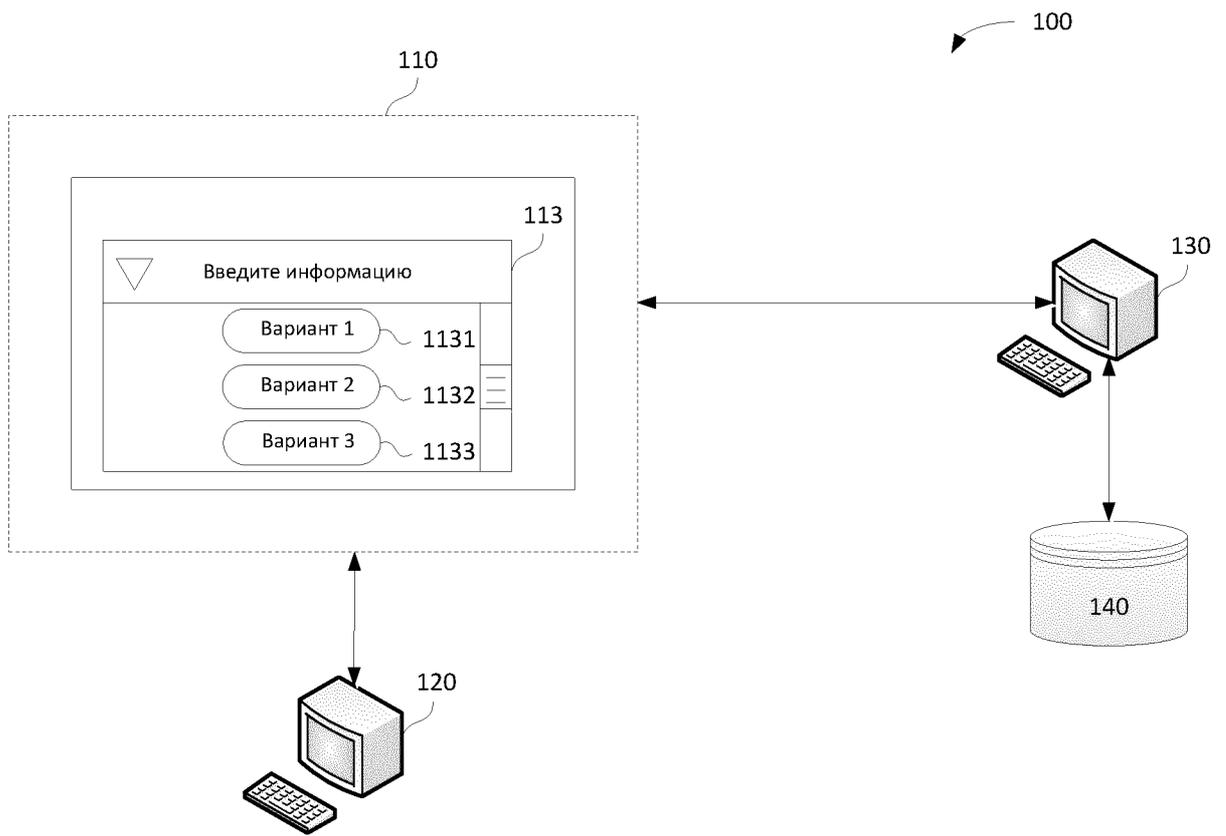
3. Способ по п.1, характеризующийся тем, что этап f) начинается после полной загрузки страницы веб-сайта и дополнительно установленного временного промежутка.
4. Способ по п.1, характеризующийся тем, что для каждой области текста проверяется наличие элементов автозаполнения.
5. Способ по п.4, характеризующийся тем, что для элементов автозаполнения определяется количество пунктов вариантов автозаполнения.
6. Способ по п.5, характеризующийся тем, что выполняется случайный выбор пунктов вариантов автозаполнения.
7. Способ по п.1, характеризующийся тем, что для каждой области текста проверяется наличие шаблона текста для ввода.
8. Способ по п.7, характеризующийся тем, что шаблон проверяется на наличие ключевых слов.
9. Способ по п.8, характеризующийся тем, что по выявленным ключевым словам выполняется обращение в базу данных трекинговой информации для получения данных, соответствующих шаблону для заполнения.
10. Способ по п.8, характеризующийся тем, что проверка выполняется по DOM-дереву и/или с помощью локатора близлежащих элементов, содержащих текст, длиной не менее трех символов.
11. Способ по п.8, характеризующийся тем, что в случае если шаблон содержит ключевые слова, указывающие на подтверждение регистрации с помощью SMS-сообщения, то выполняется шаг его отправки на номер телефона, связанный с трекинговыми данными.
12. Способ по п.11, характеризующийся тем, что определяют поступление SMS-сообщения с на указанный номер телефона, связанный с трекинговыми данными.
13. Способ по п.12, характеризующийся тем, что определение выполняется с помощью программного модуля, определяющего поступление SMS-сообщения и его передачу в базу данных.
14. Способ по п.13, характеризующийся тем, что информация, переданная в базу данных, проверяется модулем анализа на наличие информации для авторизации в полученном SMS-сообщении.
15. Система выявления устройств, связанных с мошеннической фишинговой активностью, содержащая:
 - по меньшей мере один процессор
 - по меньшей мере одну память, связанную с процессором, содержащую машиночитаемые инструкции, которые при их выполнении по меньшей мере одним процессором осуществляют способ по любому из пп. 1-14.



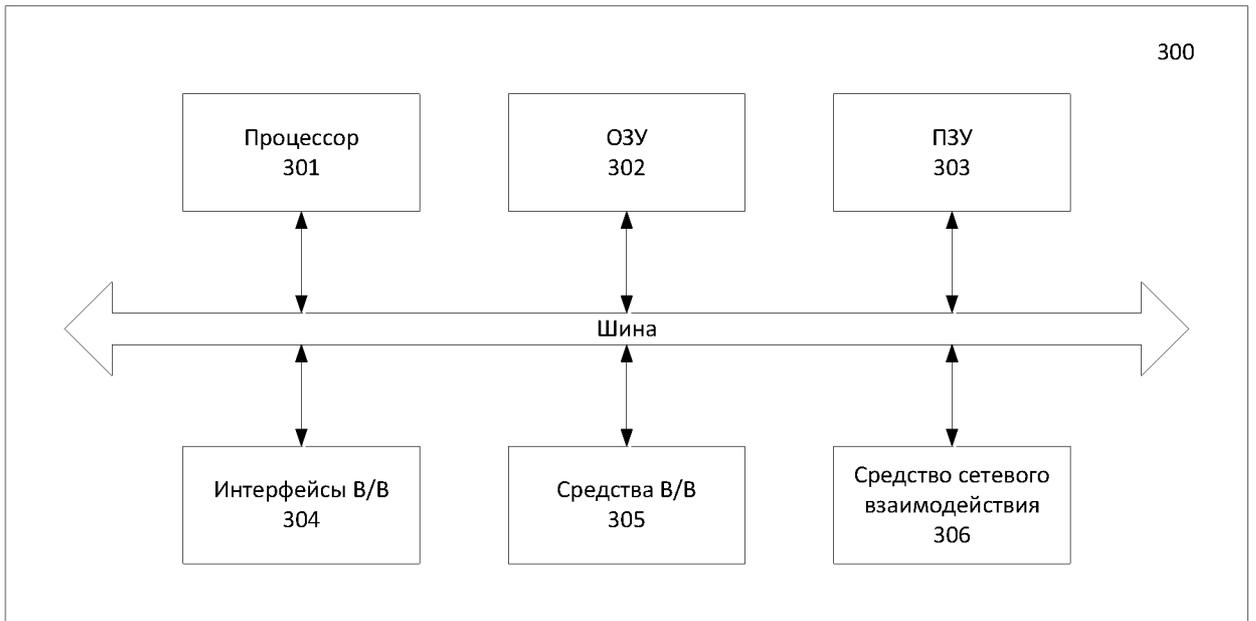
Фиг. 1



Фиг. 2



Фиг. 3

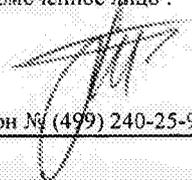


Фиг. 4

ЕВРАЗИЙСКОЕ ПАТЕНТНОЕ ВЕДОМСТВО

**ОТЧЕТ О ПАТЕНТНОМ
ПОИСКЕ**
(статья 15(3) ЕАПК и правило 42
Патентной инструкции к ЕАПК)

Номер евразийской заявки:
201892372

Дата подачи: 19 ноября 2018 (19.11.2018)		Дата испрашиваемого приоритета: 15 ноября 2018 (15.11.2018)	
Название изобретения: СПОСОБ И СИСТЕМА ВЫЯВЛЕНИЯ УСТРОЙСТВ, СВЯЗАННЫХ С МОШЕННИЧЕСКОЙ ФИШИНГОВОЙ АКТИВНОСТЬЮ			
Заявитель: ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "СБЕРБАНК РОССИИ" ("ПАО СБЕРБАНК")			
<input type="checkbox"/> Некоторые пункты формулы не подлежат поиску (см. раздел I дополнительного листа) <input type="checkbox"/> Единство изобретения не соблюдено (см. раздел II дополнительного листа)			
А. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:			
МПК:	G06F 21/56 (2013.01)	СПК:	G06F 21/566 (2013-01) H04L 63/1483 (2013-01) H04L 63/1433 (2013-01)
Согласно Международной патентной классификации (МПК) или национальной классификации и МПК			
Б. ОБЛАСТЬ ПОИСКА:			
Минимум просмотренной документации (система классификации и индексы МПК) G06F 21/00, 21/10, 21/30, 21/45, 21/50, 21/55, 21/56, 21/60, 21/70, 21/71, G06Q 20/00, 20/38, 20/40, 40/00, H04L 9/00, 9/32, 29/00, 29/02, 29/06			
Другая проверенная документация в той мере, в какой она включена в область поиска:			
В. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ			
Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей		Относится к пункту №
Y	US 2016/0019546 A1 (THE 41ST PARAMETER, INC.) 21.01.2016, абзацы [0006]-[0007], [0034], [0036]-[0037], [0042]-[0043], [0046], [0054], [0070], [0076], [0198]-[0200]		1-15
Y	US 2014/0041021 A1 (LARKINS JOSHUA ENOCH et al.) 06.02.2014, абзацы [0002]-[0005], [0007]-[0009], [0022]-[0028], [0030]-[0031]		1-15
Y	US 2014/0189808 A1 (LOOKOUT, INC.) 03.07.2014, абзацы [0048], [0050], [0071], [0133]		10-14
A	US 2009/0077637 A1 (SANTOS PAULO A et al.) 19.03.2009		1-15
<input type="checkbox"/> последующие документы указаны в продолжении графы В		<input type="checkbox"/> данные о патентах-аналогах указаны в приложении	
* Особые категории ссылочных документов:			
"А" документ, определяющий общий уровень техники		"Т" более поздний документ, опубликованный после даты приоритета и приведенный для понимания изобретения	
"Е" более ранний документ, но опубликованный на дату подачи евразийской заявки или после нее		"Х" документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну или изобретательский уровень, взятый в отдельности	
"О" документ, относящийся к вступному раскрытию, экспонированию и т.д.		"У" документ, имеющий наиболее близкое отношение к предмету поиска, порочащий изобретательский уровень в сочетании с другими документами той же категории	
"Р" документ, опубликованный до даты подачи евразийской заявки, но после даты испрашиваемого приоритета		"&" документ, являющийся патентом-аналогом	
"D" документ, приведенный в евразийской заявке		"I" документ, приведенный в других целях	
Дата действительного завершения патентного поиска:		29 апреля 2019 (29.04.2019)	
Наименование и адрес Международного поискового органа: Федеральный институт промышленной собственности РФ, 125993, Москва, Г-59, ГСП-3, Бережковская наб., д. 30-1. Факс: (499) 243-3337, телетайп: 114818 ПОДАЧА		Уполномоченное лицо:  Т. М. Иванова Телефон № (499) 240-25-91	