РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 703 975**(13) **C1**

(51) МПК
G06Q 40/00 (2012.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06Q 40/00 (2019.08)

(21)(22) Заявка: **2019102547, 30.01.2019**

(24) Дата начала отсчета срока действия патента:
30.01.2019

Дата регистрации:
22.10.2019

Приоритет(ы):
(22) Дата подачи заявки: **30.01.2019**

(45) Опубликовано: **22.10.2019** Бюл. № **30**

Адрес для переписки:
109431, Москва, ул. Привольная, 70, ООО "Джи Пи Джи"

(72) Автор(ы):
Изотов Олег Владимирович (RU)

(73) Патентообладатель(и):
Изотов Олег Владимирович (RU)

(56) Список документов, цитированных в отчете о поиске: **WO 2010/123471 A1, 28.10.2010. AU 2013101112 A4, 10.10.2013. US 2016/0358059 A1, 08.12.2016. US 2018/0060578 A1, 01.03.2018. US 8622297 B1, 07.01.2014. RU 114543 U1, 27.03.2012.**

(54) СПОСОБ АКТИВНОГО ПРОТИВОДЕЙСТВИЯ СКИММИНГУ И УСТРОЙСТВО ЗАЩИТЫ БАНКОМАТА

(57) Реферат:

Изобретение относится к способу и устройству для активного противодействия скиммингу. Технический результат заключается в повышении эффективности работы антискиммингового устройства. Способ, в котором устройство для активного противодействия скиммингу устанавливают на полку в терминале, или банкомате, или устройстве самообслуживания с помощью монтажной скобы, причем установка устройства выполнена так, что один кабель идет на накладку-излучатель для генерации помехового поля, а второй кабель вставляют в цепь питания картридера для того, чтобы управлять обрывом питания в случае обнаружения скиммера, еще один кабель идет от разъема датчика положения карты на устройстве на два датчика положения карты на картридере для определения положения датчиков положения карты на картридере, затем анализируют положение датчиков положения карты в картридере при помощи опроса двух концевых выключателей, подключенных к устройству, причем если датчики положения карты закрыты больше определенного времени – питание в цепи отключают и шторка картоприемника закрывается после определенного времени. 2 н. и 11 з.п. ф-лы.

RU 2703975 C1

RU 2703975 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 703 975**(13) **C1**

(51) Int. Cl.
G06Q 40/00 (2012.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06Q 40/00 (2019.08)

(21)(22) Application: **2019102547, 30.01.2019**

(24) Effective date for property rights:
30.01.2019

Registration date:
22.10.2019

Priority:
(22) Date of filing: **30.01.2019**

(45) Date of publication: **22.10.2019** Bull. № **30**

Mail address:
109431, Moskva, ul. Privolnaya, 70, OOO "Dzhi Pi Dzhi"

(72) Inventor(s):
Izotov Oleg Vladimirovich (RU)

(73) Proprietor(s):
Izotov Oleg Vladimirovich (RU)

(54) ACTIVE SKIMMING PROTECTION METHOD AND ATM PROTECTION DEVICE

(57) Abstract:

FIELD: automatic tellers and terminals.

SUBSTANCE: invention relates to method and device for active counteraction to skimming. Method, in which device for active counteraction of skimming is installed on shelf in terminal or ATM, or self-service device by means of mounting bracket, wherein device installation is made so that one cable goes to radiator pad for generation of interference field, and second cable is inserted into carder supply circuit in order to control supply breakage in case of skimmer detection, one more cable goes from the card position sensor connector on the device to two position sensors of the card on the card reader to determine the position of the card position sensors on the card reader, then the position of the card position sensors in the card reader is analyzed by polling the two limit switches connected to the device, wherein if the position sensors of the card are closed for more than a certain period of time, power in the circuit is disconnected, and the cardpinter cover is closed after a certain time.

EFFECT: technical result consists in improvement of anti-comming device operation efficiency.

13 cl

RU 2703975 C1

RU 2703975 C1

Настоящее изобретение в целом относится к предотвращению несанкционированного считывания данных карт с магнитной полосой в банкоматах/терминалах (так же и любых других устройствах самообслуживания, принимающих в качестве средства оплаты платежные карты. Более конкретно, настоящее изобретение относится к предотвращению возможности незаметного размещения мошеннических устройств, считывающих данные с магнитной полосы карты (скимминг-атака), или препятствующих возврату карты из штатного считывателя карт (карт-ридера) терминала/банкомата/устройства самообслуживания.

В настоящее время карты с магнитной полосой (в частности банковские карты) являются наиболее распространенными и активно использующимися видом карт по типу носителя информации. Данный вид карт имеет такой существенный недостаток, как возможность изготовления копии, содержащей данные магнитной полосы оригинала. Несанкционированное получение данных, закодированных на магнитной полосе (Скимминг (от англ. skimming) – кража данных карты при помощи специального считывающего устройства (скиммера)) и изготовление с их использованием копий карт является распространенным видом мошенничества.

Для получения данных о картах мошенники используют скимминговые устройства – скиммеры, которые чаще всего размещаются перед считывателем магнитных карт банкомата. Для того чтобы затруднить их обнаружение, скиммеры имитируют части лицевых панелей банкоматов различных производителей и моделей, которые расположены перед считывателями карт.

В борьбе со скиммингом банки обычно используют три технологии – физический мониторинг, пассивный антискимминг и активный антискимминг.

Физический мониторинг банкоматов – включает в себя периодический осмотр банкомата сотрудниками банка, инкассаторами либо специалистами сервисной службы на аутсерсинге. Физический мониторинг по факту оказывается самым ненадежным и дорогим способом борьбы со скиммингом.

Пассивный антискимминг – банк устанавливает на щель картоприемника специальные антискимминговые накладки, препятствующие установке посторонних устройств. Пассивный антискимминг – это бюджетный, компромисный, но не лучший вариант борьбы со скиммингом. Недостаток пассивного антискимминга в том, что многие держатели карт, увидев постороннее устройство, боятся пользоваться таким банкоматом. Частично успокоить держателей карт удается, разместив на экране банкомата или на специальной наклейке под картоприемником изображения правильного вида картоприемника.

Активный антискимминг – это самый дорогой, но эффективный способ борьбы со скиммингом. Устройство устанавливается внутри банкомата и незаметно снаружи. Активный антискиммер контролирует пространство перед банкоматом и позволяет моментально выявить несанкционированную установку на него посторонних устройств.

Однако, контролирование только пространства перед банкоматом является недостаточно эффективным методом в борьбе с мошенничеством.

Наиболее близким аналогом в части способа активного противодействия скиммингу является способ активного противодействия скиммингу (ИНСТРУКЦИЯ ПО УСТАНОВКЕ (ЗАМЕНЕ) И НАСТРОЙКЕ СРЕДСТВ АКТИВНОГО ПРОТИВОДЕЙТСВИЯ СКИММИНГУ «CERBER» (условное наименование АЕРВ.468200.053) НА БАНКОМАТАХ, редакция от 29.03.2018) в котором в котором устройство для активного противодействия скиммингу устанавливают на полку в терминале или банкомате или устройстве самообслуживания с помощью монтажной

скобы, причем установка устройства выполнена так, что один кабель идет на накладку-излучатель для генерации помехового поля, а второй кабель вставляют в цепь питания картридера для того, чтобы управлять обрывом питания в случае обнаружения скиммера. Недостатком известного способа является то что дополнительно не устанавливают еще один кабель идет от разъема датчика положения карты на устройстве на два датчика положения карты на картридере для определения положения датчиков положения карты на картридере для того, чтобы анализировать положение датчиков положения карты в картридере при помощи опроса двух концевых выключателей, подключенных к устройству. Также недостатком известного способа является то, что если датчики положения карты закрыты больше определенного времени – питание в цепи отключают и шторка картоприемника закрывается после определенного времени.

Таким образом, задача настоящего изобретения является устранения указанных выше недостатков.

Технический результат настоящего изобретения является повышение эффективности антискиммингового устройства.

Также технический результат настоящего изобретения заключается в том, чтобы обезопасить пользователя от несанкционированного чтения карты злоумышленником.

Технический результат достигается за счет того, что устройство для активного противодействия скиммингу устанавливают на полку в терминале или банкомате или устройстве самообслуживания с помощью монтажной скобы, причем установка устройства выполнена так, что один кабель идет на накладку-излучатель для генерации помехового поля, а второй кабель вставляют в цепь питания картридера для того, чтобы управлять обрывом питания в случае обнаружения скиммера, еще один кабель идет от разъема датчика положения карты на устройстве на два датчика положения карты на картридере для определения положения датчиков положения карты на картридере, затем анализируют положение датчиков положения карты в картридере при помощи опроса двух концевых выключателей, подключенных к устройству, причем если датчики положения карты закрыты больше определенного времени – питание в цепи отключают и шторка картоприемника закрывается после определенного времени.

Наиболее близким аналогом в части устройства активного противодействия скимминга является устройство активного противодействия скиммингу «Cerber» (СейлСервиСолюшенс, Средства защиты устройств самообслуживания, Перспективы и направления развития банковских информационных технологий в 2014 г., Раубичи Июнь 2014), принцип работы которого заключается в создании направленных электромагнитных импульсных помех в районе картридера терминала, препятствующих доступу к карте всех несанкционированных устройств. При этом «защитное поле» генерируется постоянно, а при входе (выходе) карты в (из) картридер(-а) терминала — в наиболее уязвимый момент, мощность силового поля усиливается в несколько раз. Однако, недостатком известного устройства является то, что не учитывается положение и время работы датчиков положения (роликов) карты.

Таким образом, задача настоящего изобретения является устранения указанных выше недостатков.

Технический результат настоящего изобретения является повышение эффективности антискиммингового устройства, облегчение установки и замены оборудования.

Также технический результат настоящего изобретения заключается в том, чтобы обезопасить пользователя от несанкционированного чтения карты злоумышленником.

Технический результат достигается за счет того, что устройство для активного противодействия скиммингу выполнено с возможностью установки на полке в терминале

или банкомате или устройстве самообслуживания и содержит:

контроллер управления, который питается от цепи картридера, пропуская через себя питание на картридер и выполненный с возможностью выработки сигнала на накладку-излучатель для генерации помехового поля, также контроллер выполнен с возможностью определения положения датчиков положения карты в картридере при помощи опроса двух концевых выключателей, причем если датчики положения карты замкнуты больше определенного времени – питание в цепи отключается и шторка картоприемника закрывается после определенного времени.

накладку-излучатель, выполненную с возможностью генерации защитного поля вокруг накладки, которая устанавливается на картоприемник для подавления оборудования злоумышленников, которые пытаются установить сторонний считыватель-перехватчик на картоприемнике.

крепежную скобу, которая позволяет произвести установку оборудования без сверления банкомата, не нарушая изначально конструкции устройства, причем установка происходит в штатные отверстия на полке банкомата.

Устройство активного антискимминга включает в себя:

• Контроллер управления, выполненный с возможностью выработки сигнала на накладку-излучатель, для генерации . Причем сигнал подается по коммутационным проводам на накладку. Также контроллер управляет питанием в цепи на основании состояния датчиков положения карты в картоприемнике.

• Антенну (накладка-излучатель), выполненная с возможностью генерации защитного поля вокруг накладки, которая устанавливается на картоприемник. Причем такое защитное поле представляет собой шумоподобный сигнал со случайной составляющей, отфильтровать который практически невозможно. Таким образом накладка (антенна-излучатель) подавляет приёмное оборудование злоумышленников, которые пытаются установить сторонний считыватель-перехвадчик на картоприемник.

• Соединительные провода.

• Крепежная скоба, которая позволяет произвести установку оборудования без сверления банкомата, не нарушая изначально конструкции устройства. Установка происходит в штатные отверстия на полке банкомата, такой вид скобы значительно упрощает установку оборудования.

Известно, что карторпримник (картридер) любого банкомата снабжен по меньшей мере следующими датчиками:

•Два подпружиненных ролика

•Датчик считывания магнитной полосы

Принцип работы первого датчика: когда что-то попадает в картридер соответствуя размерам стандартной пластиковой карты 54 х 86 х 0,76 мм, ролики пропуская карту вперед раздвигаются. Раздвигаясь, они замыкают концевые выключатели (концевики) которые сообщают на картридер о необходимостиначать сканировать наличие считывающей полосы.

Нормальный режим работы этих датчиков – кратковременное замыкание концевиков. Карточку вставили, и она «прошла» дальше. Оборудование скиммера вставляется в щель стандартного картоприёмника раздвигая ролики, но так как это не карта, оно остается в щели для перехвата карты жертвы.

Устройство активного антискимминга устанавливается на полку в банкомате с помощью монтажной скобы. Один кабель идет на антенну (накладка-излучатель), второй кабель подключается в разрыв цепи питания картридера (питание от картридера отключается и подключается к кабелю, один конец подключается обратно в картридер).

Таким образом устройство активного антискимминга отключает питание в случае обнаружения скиммера. Также один кабель идет от разъема датчиков (сенсоров) на два датчика положения карты на картридере (ролики) для контроля положения роликов (нормально –разомкнуты, если замкнуты - значит что-то вставлено в щель картоприемника).

Контроллер питается от цепи картридера, пропуская через себя питание на картридер (картоприемник). При включении контроллер генерирует алгоритм защитного поля и тут же его включает (накладка-антенна начинает издавать тихий писк). При этом сразу же устройство активного антискимминга анализирует датчики картридера банкомата контролируя их текущее состояние. Если датчики положения карты замкнуты больше определённого времени – питание в цепи кардридера отключается и шторка картоприемника закрывается.

Таким образом, в случае, если злоумышленник установил антискимминговое оборудование непосредственно в щель картоприемника, а не в качестве дополнительной считывающей головки (устанавливает какнакладка), концевые выключатели передают сигнал на модуль обработки, который отключает питание картридера в результате чего блокируется шторка картоприемника не позволяя проникнуть карте внутрь и быть прочитанной до тех пор, пока оборудование не будет удалено из щели картоприемника.

Подобный метод позволяет на 100% обезопасить пользователя от несанкционированного чтения карты злоумышленником, так как картридер будет обесточен.

В частности, но не ограничиваясь этим, в накладку-излучатель встроен направленный излучатель (две катушки генерации помехового поля). Причем помеховое поле распространяется на 180 градусов исключая проникновение помехового поля внутрь банкомата.

В частности, но не ограничиваясь этим, устройство содержит дисплей с подсветкой отображающий всю необходимую информацию (дату атаки, если такая была, текущий статус картридера, текущий статус ошибок, если таковые присутствуют). Таким образом получить информацию из устройства (антисктимминга) не представляет труда и не требует демонтажа устройства

В частности, но не ограничиваясь этим, антискимминг поставляется с программным обеспечением позволяющим подключить устройство к ПК посредствам USB- кабеля для настройки входов, чтения журнала событий, установки времени (мощность сигнала, время отключение и включения картридера).

В частности, но не ограничиваясь этим, устройство имеет возможность установки GSM модуля или LAN модуля. Таким образом при атаке устройство мгновенно отправит SMS или Push-уведомление в Банк об инциденте сообщив дату, время, ID-банкомата. Данный способ позволяет оперативно среагировать сотрудникам службы безопасности банка на инцидент

В частности, но не ограничиваясь этим, устройство позволяет легко настроить такие параметры как:

- Мощность излучателя (больше-меньше)
- Время, через которое произойдёт отключение питания картоприёмника
- Время, восстановления питания на картоприемнике при условии, что датчики вернуться в исходное положение (лже карта или скиммер будет удален с банкомата)

В частности, но не ограничиваясь этим, устройство содержит разъем для подключения датчиков охранной и пожарной сигнализации имеющих релейный выход. Наиболее

востребованы следующие датчики:

- Датчик открытия двери (геркон)
- Датчик наклона банкомата
- Датчик удара
- Датчик газа

При подключении датчиков система автоматически начинает отслеживать их состояние. Как-только сработает любой датчик информация запишется в память устройства. На дисплее устройства отобразится информация о наличии критической информации. Ознакомиться с информацией можно как с самого устройства (без демонтажа), так и получив уведомление либо на почту (lan-подключение), либо в смс или push-уведомлении (GSM-уведомление).

Модуль защиты также снабжен GPS модулем. В случае, если банкомат перемещается банкомат автоматически отключает картоприемник и уведомляет по всем каналам связи банк (LAN, GSM).

Отдельные устройства снабжены автономным источником питания (батарейкой) обеспечивающей возможность отправить уведомление даже при отсутствии питания. Время работы автономного устройства – менее пяти минут.

В одном варианте настоящего изобретения устройство активного антискимминга представляет собой пластиковую коробку размером мм.140*110*35

На лицевой панели установлен дисплей, 4 кнопки управлением навигацией (влево, вправо, вверх, вниз), 1 кнопка подтверждения выбора, 2 световых индикатора (питание и ошибка).

На задней панели установлено:

1 разъем питания

1 разъем для антенны

1 разъем для подключения датчиков (сигнацизация и состояние датчиков картоприемника)

1 разъем для подключения антенны на GSM

1 разъем для подключения антенны на GPS

1 разъем для подключения LAN-кабеля

1 разъём для подключения USB

(57) Формула изобретения

1. Способ активного противодействия скиммингу, в котором устройство для активного противодействия скиммингу устанавливают на полку в терминале, или банкомате, или устройстве самообслуживания с помощью монтажной скобы, причем установка устройства выполнена так, что один кабель идет на накладку-излучатель для генерации помехового поля, а второй кабель вставляют в цепь питания картридера для того, чтобы управлять обрывом питания в случае обнаружения скиммера, еще один кабель идет от разъема датчика положения карты на устройстве на два датчика положения карты на картридере для определения положения датчиков положения карты на картридере, затем анализируют положение датчиков положения карты в картридере при помощи опроса двух концевых выключателей, подключенных к устройству, причем если датчики положения карты закрыты больше определенного времени – питание в цепи отключают и шторка картоприемника закрывается после определенного времени.

2. Способ по п. 1, в котором в накладку-излучатель встроен направленный излучатель для генерации помехового поля, которое распространяют на 180 градусов исключая

проникновение помехового поля внутрь банкомата.

3. Способ по п. 2, в котором тип генерации помехового поля является генерация белого шума.

4. Способ по п. 1, в котором при определении скимминга устройство мгновенно отправляет SMS или Push-уведомление в Банк об инциденте сообщив дату, время, ID-банкомата.

5. Устройство для активного противодействия скиммингу, выполненное с возможностью установки на полке в терминале, или банкомате, или устройстве самообслуживания, характеризующееся тем, что содержит:

контроллер управления, который питается от цепи питания картридера, пропуская через себя питание на картридер, и выполненный с возможностью выработки сигнала на накладку-излучатель для генерации защитного поля, также контроллер выполнен с возможностью определения состояния положения карты в картридере при помощи опроса датчиков, причем если датчики положения карты замкнуты больше определенного времени – питание в цепи отключается и шторка картоприемника закрывается;

накладку-излучатель, выполненную с возможностью создания защитного поля вокруг накладки, которая устанавливается на картоприемник для подавления оборудования злоумышленников, которые пытаются установить сторонний считыватель-перехвадчик на картоприемник;

крепежную скобу, которая позволяет произвести установку оборудования без сверления банкомата, не нарушая изначально конструкции устройства, причем установка происходит в штатные отверстия на полке банкомата.

6. Устройство по п. 5, в котором дополнительно установлены следующие датчики:

датчик открытия двери – геркон,

датчик наклона банкомата,

датчик удара,

датчик газа.

7. Устройство по п. 6, в котором дополнительно имеется возможность установки GSM модуля.

8. Устройство по п. 6, в котором дополнительно установлен GPS модуль.

9. Устройство по. 6, в котором в накладку-излучатель встроен направленный излучатель.

10. Устройство по п. 9, в котором помеховое поле распространяется на 180 градусов исключая проникновение помехового поля внутрь банкомата.

11. Устройство по п. 6, в котором устройство дополнительно содержит дисплей с подсветкой отображающий всю необходимую информацию.

12. Устройство по п. 11, в котором информация содержит дату атаки, если такая была, текущий статус картридера, текущий статус ошибок, если таковые присутствуют.

13. Устройство по п. 6, в котором устройство поставляется с программным обеспечением, позволяющим подключить устройство к ПК посредствам USB- кабеля для тонкой настройки.