



ФЕДЕРАЛЬНАЯ СЛУЖБА
 ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
 ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) **ЗАЯВКА НА ИЗОБРЕТЕНИЕ**

(21), (22) Заявка: **2003137601/09, 28.06.2002**

(30) Приоритет: **01.07.2001 DE 10131254.7**

(43) Дата публикации заявки: **27.05.2005 Бюл. № 15**

(85) Дата перевода заявки РСТ на национальную фазу: **02.02.2004**

(86) Заявка РСТ:
DE 02/02348 (28.06.2002)

(87) Публикация РСТ:
WO 03/005307 (16.01.2003)

Адрес для переписки:
**193036, Санкт-Петербург, а/я 24, "НЕВИНПАТ",
 пат.пов. А.В.Поликарпову, рег.№ 0009**

(71) Заявитель(и):
Дойче Пост АГ (DE)

(72) Автор(ы):
**ДЕЛИЦ Александр (DE),
 ФЕРИ Петер (DE),
 ХЕЛЬМУС Юрген (DE),
 ХЕЛЬ Алоизиус (DE),
 МАЙЕР Гюнтер (DE),
 РОБЕЛЬ Эльке (DE),
 ШТУММ Дитер (DE)**

(74) Патентный поверенный:
Поликарпов Александр Викторович

(54) **СПОСОБ ПРОВЕРКИ ДЕЙСТВИТЕЛЬНОСТИ ЦИФРОВЫХ ОТМЕТОК О ФРАНКИРОВАНИИ**

Формула изобретения

1. Способ проверки подлинности цифровой отметки о франкировании, нанесенной на почтовое отправление, включающий дешифрование содержащейся в указанной отметке криптографической информации и ее использование для проверки подлинности этой отметки, отличающийся тем, что проверочное устройство управляет ходом частичных проверок, при этом первая частичная проверка включает считывание матричного кода, содержащегося в цифровой отметке о франкировании, проверочное устройство управляет разделением содержимого матричного кода, указанные частичные проверки осуществляют в виде проверочных шагов, проверочное устройство выполнено с возможностью одновременного выполнения нескольких запросов на проверку и, параллельно с этим, части проверочных шагов, причем при помощи проверочных шагов определяют неправомерно созданные отметки о франкировании, результат проверки передают в виде цифрового сообщения, и в результате этого отправление изымают из нормального процесса обработки почтовых отправлений.

2. Способ по п.1, отличающийся тем, что одна из частичных проверок включает дешифрование криптографической информации, содержащейся в отметке о франкировании.

3. Способ по п.1 или 2, отличающийся тем, что одна из частичных проверок включает сравнение даты создания отметки о франкировании и текущей даты.

4. Способ по п.1 или 2, отличающийся тем, что считывающее устройство и проверочное устройство обмениваются информацией с использованием синхронного протокола.

5. Способ по п.4, отличающийся тем, что указанный протокол основан на удаленном вызове процедуры (RPC).

6. Способ по п.1 или 2, отличающийся тем, что считывающее устройство и проверочное

устройство взаимодействуют друг с другом с использованием асинхронного протокола.

7. Способ по п.6, отличающийся тем, что считывающее устройство посылает в проверочное устройство сообщение с данными.

8. Способ по п.7, отличающийся тем, что указанное сообщение включает в себя содержание отметки о франкировании.

9. Способ по п.7, отличающийся тем, что сообщение с данными содержит запрос на запуск криптографической проверочной подпрограммы.

10. Способ по п.1 или 2, отличающийся тем, что при помощи криптографического интерфейса осуществляют распределение загрузки между несколькими проверочными средствами.

11. Способ по п.1 или 2, отличающийся тем, что содержание отметки о франкировании разделяют на отдельные поля.

12. Способ по п.1 или 2, отличающийся тем, что из отметки о франкировании определяют идентификационный номер (почтовый идентификатор) клиентской системы, управлявшей созданием отметки о франкировании.

13. Способ по п.1 или 2, отличающийся тем, что идентификационные данные (почтовые идентификаторы) отдельных клиентских систем регистрируют в "черном списке", и отправления с такими почтовыми идентификаторами изымают из нормального процесса обработки почтовых отправлений.

14. Способ по п.1 или 2, отличающийся тем, что содержащиеся в отметке о франкировании зашифрованные данные об адресе получателя сравнивают с адресом получателя, указанным для доставки почтового отправления.

15. Способ по п.1 или 2, отличающийся тем, что параметры проверки для этого способа можно изменять.

16. Способ по п.15, отличающийся тем, что изменение параметров способа осуществляют только после ввода персонального цифрового ключа (секретного ключа) системного администратора.