



УКРАЇНА

(19) UA (11) 42756 (13) C2

(51) 7 G07F7/08, G07F7/10, G07F7/12

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС ДО ПАТЕНТУ НА ВИНАХІД

(54) СПОСІБ ТА СИСТЕМА ДЛЯ ЗДІЙСНЕННЯ РІЗНИХ ПРОЦЕСІВ ІДЕНТИФІКАЦІЇ З ВИКОРИСТАННЯМ ОДНОГО Й ТОГО Ж НОСІЯ ДАНИХ

(21) 96083237

(22) 12.08.1996

(24) 15.11.2001

(31) 1000988

(32) 16.08.1995

(33) NL

(46) 15.11.2001, Бюл. № 10, 2001 р.

(72) Хекстра Андріс Пітер, NL

(73) КОНІНКЛЕЙКЕ ПТТ НЕДЕРЛАНД Н.В., NL

(56) 1. US пат. 4700055, 13.10.1987.

2. US пат. 4837422, 06.06.1989.

3. EP, A, 0385290, 05.09.1990.

4. US пат. 5285055, 08.02.1994.

5. US пат. 5390331, 14.02.1995

(57) 1. Способ для осуществления различных процессов идентификации с использованием одного и того же носителя данных, на котором хранится по меньшей мере один код, причем при осуществлении первого процесса опознавания указанный способ включает стадии:

- прием первого кода, хранимого на носителе информации, и второго кода, исходящего от пользователя,

- осуществление по меньшей мере одного из следующих преобразований:

- первого преобразования первого кода в преобразованный первый код и

- второго преобразования второго кода в преобразованный второй код,

- сравнение полученных таким образом кодов для завершения на основе результатов сравнения первого процесса опознавания,

а при осуществлении второго процесса опознавания указанный способ включает стадии:

- прием третьего кода, хранимого на носителе информации, и четвертого кода, исходящего от пользователя,

- осуществление по меньшей мере одного из следующих преобразований:

- третьего преобразования третьего кода в преобразованный третий код и

- четвертого преобразования четвертого кода в преобразованный четвертый код,

- сравнение полученных таким образом кодов для завершения на основе результатов второго процесса опознавания,

отличающийся тем, что первый код и третий код равны, тогда как второй код и четвертый код отличны один от другого, причем по меньшей мере

одно из соответствующих первого и второго преобразований отличается от соответствующих третьего и четвертого преобразований.

2. Способ по п. 1, **отличающийся** тем, что первое преобразование отличается от третьего преобразования, причем второе преобразование равно четвертому преобразованию.

3. Способ по п. 1, **отличающийся** тем, что второе преобразование отличается от четвертого преобразования, причем первое преобразование равно третьему преобразованию.

4. Способ по п. 1, **отличающийся** тем, что первое преобразование отличается от третьего преобразования, а второе преобразование отличается от четвертого преобразования.

5. Способ по любому из пп. 1-4, **отличающийся** тем, что по меньшей мере одно из преобразований зависит от пятого кода, хранящегося на носителе информации.

6. Система для осуществления различных процессов идентификации с использованием одного и того же носителя данных, на котором хранится по меньшей мере один код, причем для осуществления первого процесса опознавания указанная система содержит:

- первое принимающее устройство, предназначенное для приема первого кода, хранимого на носителе информации, и второго кода, исходящего от пользователя,

- первое преобразующее устройство, предназначенное для осуществления по меньшей мере одного из следующих преобразований:

- первого преобразования первого кода в преобразованный первый код и

- второго преобразования второго кода в преобразованный второй код,

- первое сравнивающее устройство, предназначенное для сравнения полученных таким образом кодов с целью завершения на основе результатов сравнения первого процесса опознавания,

а для осуществления второго процесса опознавания указанная система содержит:

- второе принимающее устройство, предназначенное для приема третьего кода, хранимого на носителе информации, и четвертого кода, исходящего от пользователя,

(19) UA (11) 42756 (13) C2

- второе преобразующее устройство, предназначенное для осуществления по меньшей мере одного из следующих преобразований:

- третьего преобразования третьего кода в преобразованный третий код и

- четвертого преобразования четвертого кода в преобразованный четвертый код,

- второе сравнивающее устройство, предназначенное для сравнения полученных таким образом кодов с целью завершения на основе результатов сравнения второго процесса опознавания,

отличающаяся тем, что первый код и третий код равны, тогда как второй код и четвертый код отличны один от другого, причем по меньшей мере одно из соответствующих первого и второго преобразований отличается от соответствующих третьего и четвертого преобразований.

7. Система по п. 6, **отличающаяся** тем, что первое преобразование отличается от третьего преобразования, причем второе преобразование равно четвертому преобразованию.

8. Система по п. 6, **отличающаяся** тем, что второе преобразование отличается от четвертого преобразования, причем первое преобразование равно третьему преобразованию.

9. Система по п. 6, **отличающаяся** тем, что первое преобразование отличается от третьего преобразования, а второе преобразование отличается от четвертого преобразования.

10. Система по любому из пп. 6-9, **отличающаяся** тем, что по меньшей мере одно из преобразований зависит от пятого кода, хранящегося на носителе информации.

Настоящее изобретение относится к способу, позволяющему осуществлять различные процессы опознавания с одним и тем же носителем информации, на котором хранится по меньшей мере один код, причем при осуществлении первого процесса опознавания указанный способ включает стадии:

- приема первого кода, хранимого на носителе информации, и второго кода, исходящего от пользователя,

- осуществления по меньшей мере одного из следующих преобразований:

- первое преобразование первого кода в преобразованный первый код и

- второе преобразование второго кода в преобразованный второй код,

- сравнения кодов для завершения на его основе первого процесса опознавания,

а при осуществлении второго процесса опознавания указанный способ включает стадии:

- приема третьего кода, хранимого на носителе информации, и четвертого кода, исходящего от пользователя,

- осуществления по меньшей мере одного из следующих преобразований:

- третье преобразование третьего кода в преобразованный третий код и

- четвертое преобразование четвертого кода в преобразованный четвертый код,

- сравнения кодов для завершения на его основе второго процесса опознавания.

Такой способ раскрыт в патенте США № 4837422. Здесь показан носитель информации, выполненный в виде интеллектуальной карточки (фиг. 2 патента США № 4837422), на которой запомнен первый код (код персонального идентификационного номера, хранимый в запоминающем устройстве 210, показанном на фиг. 2 патента США № 4837422) и на которой запомнен третий код (код персонального идентификационного подномера, хранимый в запоминающем устройстве 207, показанном на фиг. 2 патента США № 4837422). Как правило, указанные коды персональных идентификационных номера и подномера хранятся в зашифрованной форме.

При осуществлении первого процесса опознавания, относящегося, например, к первой системе, и, например, к первому пользователю, генерируется реальный код персонального идентификационного номера (второй код), который принимается первой системой, после чего код персонального идентификационного номера, хранимый в зашифрованной форме (первый код), считывается и (путем первого преобразования) расшифровывается, что обеспечивает получение кода персонального идентификационного номера (преобразованного первого кода). Последний затем сравнивается с генерируемым реальным кодом персонального идентификационного номера (вторым кодом) и на основе этого сравнения первый процесс опознавания завершается с положительным результатом (в случае равенства) или с отрицательным результатом (в случае неравенства). Вместо расшифровки зашифрованного кода персонального идентификационного номера (преобразования путем осуществления первого преобразования первого кода в преобразованный первый код) или в дополнение к ней, в зависимости от обстоятельств, одной из опций является также преобразование реального кода персонального идентификационного номера, генерируемого первым пользователем (второго кода), путем осуществления второго преобразования в преобразованный второй код, после чего, с одной стороны, указанный преобразованный второй код сравнивается, с другой стороны, с первым кодом или с преобразованным первым кодом, в зависимости от обстоятельств, и т.д.

При осуществлении второго процесса опознавания, относящегося, например, ко второй системе, и, например, ко второму пользователю, генерируется реальный код персонального идентификационного подномера (четвертый код), который принимается второй системой, после чего код персонального идентификационного подномера, хранимый в зашифрованной форме (третий код), считывается и (путем третьего преобразования) расшифровывается, что обеспечивает получение кода персонального идентификационного подномера (преобразованного третьего кода). Последний затем сравнивается с генерируемым реаль-

ным кодом персонального идентификационного подномера (четвертым кодом) и на основе этого сравнения второй процесс опознавания завершается с положительным результатом (в случае равенства) или с отрицательным результатом (в случае неравенства). Вместо расшифровки зашифрованного кода персонального идентификационного подномера (преобразования путем осуществления третьего преобразования третьего кода в преобразованный третий код) или в дополнение к ней, в зависимости от обстоятельств, одной из опций является также преобразование реального кода персонального идентификационного подномера, генерируемого вторым пользователем (четвертого кода), путем осуществления четвертого преобразования в преобразованный четвертый код, после чего, с одной стороны, указанный преобразованный четвертый код сравнивается, с другой стороны, с третьим кодом или с преобразованным третьим кодом, в зависимости от обстоятельств, и т.д.

Оба процесса опознавания могут дополнительно относиться к различным системам, имеющим одного пользователя, или же могут относиться (как в патенте США № 4837422) к одной системе, имеющей различных пользователей.

Такой способ имеет, в частности, недостаток, заключающийся в том, что для осуществления первого процесса опознавания первый код должен быть на носителе информации и что для осуществления второго процесса опознавания третий код должен быть на этом же носителе информации. В результате становится невозможным использовать носители информации, которые уже находятся в постоянном обращении, что лишает дополнительной возможности запоминания следующего кода для каждого следующего процесса опознавания.

Одной из целей настоящего изобретения является создание способа, осуществление которого позволяет использовать носители информации, уже находящиеся в постоянном обращении, которые исключают дополнительную возможность запоминания следующего кода для каждого следующего процесса опознавания.

Для достижения этой цели согласно настоящему изобретению предложен способ, характеризующийся тем, что первый код и третий код равны, а второй код и четвертый код отличны один от другого, причем по меньшей мере одно из соответствующих первого и второго преобразований отличается от соответствующих третьего и четвертого преобразований.

Поскольку по меньшей мере одно из соответствующих первого и второго преобразований отличается от соответствующих третьего и четвертого преобразований, первый код и третий код могут быть равны и полностью совпадать, в то время, как второй код и четвертый код оставаться по-прежнему отличными один от другого. В данном случае появляется дополнительная возможность использования носителей информации, где храниться лишь первый код, который равен третьему коду и совпадает с ним, при этом указанные носители информации могут быть по-прежнему использованы с целью, например, осуществления двух различных процессов опознавания, что тре-

бует последующего генерирования второго кода и четвертого кода соответственно.

Изобретение основано, в частности, на предположении, что первый процесс опознавания основывается по меньшей мере на трех параметрах, а именно, на первом коде, втором коде и по меньшей мере одним (первом или втором) преобразовании, а второй процесс опознавания основывается по меньшей мере на трех параметрах, а именно, на третьем коде, четвертом коде и по меньшей мере одним (третьем или четвертом) преобразовании, и что в случае, когда один из по меньшей мере трех параметров принимает заданное значение, другие по меньшей мере два параметра могут быть по-прежнему выбраны свободно.

Таким образом, проблема невозможности использования носителей информации, уже находящихся в постоянном обращении, которые исключают дополнительную возможность хранения следующего кода для каждого следующего процесса опознавания, решается по меньшей мере одной системой, регулирующей по меньшей мере одно преобразование.

Первый вариант осуществления способа, предложенного в соответствии с настоящим изобретением, характеризуется тем, что первое преобразование отличается от третьего преобразования, причем второе преобразование равно четвертому преобразованию.

В данном случае при осуществлении первого процесса опознавания, относящегося к первой системе и к первому пользователю, указанным первым пользователем генерируется второй код, который принимается первой системой, после чего первый код, хранимый в зашифрованной форме, или третий код, хранимый в зашифрованной форме, считывается и расшифровывается путем первого преобразования, что приводит к получению первого кода, преобразованного первым способом, или третьего кода, преобразованного первым способом, который затем сравнивается с генерируемым (и, возможно, преобразованным вторым способом) вторым кодом, в результате чего на основе этого сравнения первый процесс опознавания завершается с положительным результатом (в случае равенства) или с отрицательным результатом (в случае неравенства). При осуществлении второго процесса опознавания, относящегося ко второй системе и ко второму пользователю, указанным вторым пользователем генерируется четвертый код, который принимается второй системой, после чего первый код, хранимый в зашифрованной форме, или третий код, хранимый в зашифрованной форме, считывается и расшифровывается путем третьего преобразования, что приводит к получению первого кода, преобразованного третьим способом, или третьего кода, преобразованного третьим способом, который затем сравнивается с генерируемым (и, возможно, преобразованным четвертым способом) четвертым кодом, в результате чего на основе этого сравнения второй процесс опознавания завершается с положительным результатом (в случае равенства) или с отрицательным результатом (в случае неравенства). Поскольку первое преобразование и третье преобразование отличаются

один от другого, следовательно, для каждой системы пользователем должен генерироваться другой код (второй или четвертый), тогда как на носителе информации по-прежнему остается лишь один код (первый или третий). Второе преобразование и четвертое преобразование взаимно равны и, в простейшем случае, могут не приниматься во внимание, что, однако, в общем не способствует обеспечению защиты.

Второй вариант осуществления способа, предложенного в соответствии с настоящим изобретением, характеризуется тем, что второе преобразование отличается от четвертого преобразования, причем первое преобразование равно третьему преобразованию.

В данном случае при осуществлении первого процесса опознавания, относящегося к первой системе и к первому пользователю, указанным первым пользователем генерируется второй код, который принимается первой системой и преобразуется во второй код, преобразованный вторым способом, после чего первый код (возможно, хранимый в зашифрованной форме) или третий код (возможно, хранимый в зашифрованной форме) считывается и, возможно, расшифровывается путем первого преобразования, что приводит к получению первого кода (возможно, преобразованного первым способом) или третьего кода (возможно, преобразованного первым способом), который затем сравнивается с генерируемым вторым кодом, преобразованным вторым способом, в результате чего на основе этого сравнения первый процесс опознавания завершается с положительным результатом (в случае равенства) или с отрицательным результатом (в случае неравенства). При осуществлении второго процесса опознавания, относящегося ко второй системе и ко второму пользователю, указанным вторым пользователем генерируется четвертый код, который принимается второй системой и преобразуется в четвертый код, преобразованный четвертым способом, после чего первый код (возможно, хранимый в зашифрованной форме) или третий код (возможно, хранимый в зашифрованной форме) считывается и, возможно, расшифровывается путем третьего преобразования, что приводит к получению первого кода (возможно, преобразованного третьим способом) или третьего кода (возможно, преобразованного третьим способом), который затем сравнивается с генерируемым четвертым кодом, преобразованным четвертым способом, в результате чего на основе этого сравнения второй процесс опознавания завершается с положительным результатом (в случае равенства) или с отрицательным результатом (в случае неравенства). Поскольку второе преобразование и четвертое преобразование отличаются одно от другого, следовательно, для каждой системы пользователем должен генерироваться другой код (второй или четвертый), тогда как на носителе информации по-прежнему остается лишь один код (первый или третий). Первое преобразование и третье преобразование взаимно равны и, в простейшем случае, могут не приниматься во внимание, что, однако, в общем не способствует обеспечению защиты.

Третий вариант осуществления способа, предложенного в соответствии с настоящим изобретением, характеризуется тем, что первое преобразование отличается от третьего преобразования, а второе преобразование отличается от четвертого преобразования.

В данном случае при осуществлении первого процесса опознавания, относящегося к первой системе и к первому пользователю, указанным первым пользователем генерируется второй код, который принимается первой системой и преобразуется во второй код, преобразованный вторым способом, после чего первый код, хранимый в зашифрованной форме, или третий код, хранимый в зашифрованной форме, считывается и расшифровывается путем первого преобразования, что приводит к получению первого кода, преобразованного первым способом, или третьего кода, преобразованного первым способом, который затем сравнивается с генерируемым вторым кодом, преобразованным вторым способом, в результате чего на основе этого сравнения первый процесс опознавания завершается с положительным результатом (в случае равенства) или с отрицательным результатом (в случае неравенства). При осуществлении второго процесса опознавания, относящегося ко второй системе и ко второму пользователю, указанным вторым пользователем генерируется четвертый код, который принимается второй системой и преобразуется в четвертый код, преобразованный четвертым способом, после чего первый код, хранимый в зашифрованной форме, или третий код, хранимый в зашифрованной форме, считывается и расшифровывается путем третьего преобразования, что приводит к получению первого кода, преобразованного третьим способом, или третьего кода, преобразованного третьим способом, который затем сравнивается с генерируемым четвертым кодом, преобразованным четвертым способом, в результате чего на основе этого сравнения второй процесс опознавания завершается с положительным результатом (в случае равенства) или с отрицательным результатом (в случае неравенства). Поскольку отличаются между собой не только первое и третье преобразования, но также и второе и четвертое преобразования, следовательно, для каждой системы пользователем должен генерироваться другой код (второй ли четвертый), тогда как на носителе информации по-прежнему остается лишь один код (первый или третий), причем в данном случае можно говорить о хорошо защищенной системе.

Четвертый вариант осуществления способа, предложенного в соответствии с настоящим изобретением, характеризуется тем, что по меньшей мере одно из преобразований зависит от пятого кода, хранимого на носителе информации.

Поскольку по меньшей мере одно из преобразований зависит от пятого кода, хранимого на носителе информации, например, от номера (жиро- или банковского) счета или от даты рождения, становится значительно более трудным разгадать способ, предложенный в соответствии с изобретением, что обеспечивает защиту.

Изобретение относится также к системе, позволяющей осуществлять различные процессы опознавания с одним и тем же носителем инфор-

мации, на котором хранится по меньшей мере один код, причем при осуществлении первого процесса опознавания указанная система содержит:

- первое принимающее устройство, предназначенное для приема первого кода, хранящегося на носителе информации, и второго кода, исходящего от пользователя,
- первое преобразующее устройство, предназначенное для осуществления по меньшей мере одного из следующих преобразований:
 - первое преобразование первого кода в преобразованный первый код и
 - второе преобразование второго кода в преобразованный второй код,
 - первое сравнивающее устройство, предназначенное для сравнения кодов с целью завершения на его основе первого процесса опознавания,

а при осуществлении второго процесса опознавания указанная система содержит:

- второе принимающее устройство, предназначенное для приема третьего кода, хранящегося на носителе информации, и четвертого кода, исходящего от пользователя,
- второе преобразующее устройство, предназначенное для осуществления по меньшей мере одного из следующих преобразований:
 - третье преобразование третьего кода в преобразованный третий код и
 - четвертое преобразование четвертого кода в преобразованный четвертый код,
 - второе сравнивающее устройство, предназначенное для сравнения кодов с целью завершения на его основе второго процесса опознавания.

Система, предложенная в соответствии с настоящим изобретением, характеризуется тем, что первый код и третий код равны, а второй код и четвертый код отличны один от другого, причем одно из соответствующих первого и второго преобразований отличается от соответствующих третьего и четвертого преобразований.

Первый вариант выполнения системы, предложенной в соответствии с настоящим изобретением, характеризуется тем, что первое преобразование отличается от третьего преобразования, причем второе преобразование равно четвертому преобразованию.

Второй вариант выполнения системы, предложенной в соответствии с настоящим изобретением, характеризуется тем, что второе преобразование отличается от четвертого преобразования, причем первое преобразование равно третьему преобразованию.

Третий вариант выполнения системы, предложенной в соответствии с настоящим изобретением, характеризуется тем, что первое преобразование отличается от третьего преобразования, а второе преобразование отличается от четвертого преобразования.

Четвертый вариант выполнения системы, предложенной в соответствии с настоящим изобретением, характеризуется тем, что по меньшей мере одно из преобразований зависит от пятого кода, хранящегося на носителе информации.

Ссылки

- Патент США № 4837422
- "Contemporary Cryptology", The Science of Information Integrity ("Современная криптология", Наука о информационной целостности), издано Gustavus J. Simmons, IEEE Press, 1992
- "Cryptography: a new dimension in computer data security", A guide for the Design and Implementation of Secure Systems, ("Криптография: новый аспект в защите компьютерных данных", Руководство по проектированию и применению защитных систем), Carl H. Meyer, Stephen M. Matyas, A Wiley-Interscience Publication, John Wiley & Sons, 1982

- Патентная заявка Нидерландов № 1000988

Все ссылки считаются включенными в настоящий патент.

Более подробно изобретение поясняется со ссылкой на примерный вариант его осуществления, показанный на чертеже, на котором представлена система, предложенная в соответствии с изобретением и предназначенная для осуществления способа, предложенного в соответствии с изобретением.

Система, показанная на чертеже (фиг.), согласно изобретению, содержит первое принимающее устройство 1, которое снабжено, например, клавиатурой 2 и устройством 3 считывания карт, а также содержит первое преобразующее устройство 4, соединенное с первым принимающим устройством 1, причем первое преобразующее устройство снабжено, например, шифратором 5, обрабатывающим устройством 6 и шифратором 7. Первый вход шифратора 5 соединен посредством соединительной линии 9 с клавиатурой 2, а первый вход шифратора 7 и вход обрабатывающего устройства 6 соединены посредством соединительной линии 10 с выходом устройства 3 считывания карт. Первый выход обрабатывающего устройства 6 соединен посредством соединительной линии 11 со вторым входом шифратора 5, а второй выход обрабатывающего устройства 6 соединен посредством соединительной линии 12 со вторым входом шифратора 7. Выход шифратора 5 соединен посредством соединительной линии 13 с первым входом первого сравнивающего устройства 8, а выход шифратора 7 соединен посредством соединительной линии 14 со вторым входом первого сравнивающего устройства 8, которое снабжено также выходом 15.

Система, показанная на чертеже, согласно изобретению, содержит также второе принимающее устройство 21, которое снабжено, например, клавиатурой 22 и устройством 23 считывания карт, а также содержит второе преобразующее устройство 24, соединенное со вторым принимающим устройством 21, причем второе преобразующее устройство снабжено, например, шифратором 25, обрабатывающим устройством 26 и шифратором 27. Первый вход шифратора 25 соединен посредством соединительной линии 29 с выходом клавиатуры 22, а первый вход шифратора 27 и выход обрабатывающего устройства 26 соединены посредством соединительной линии 30 с выходом устройства 23 считывания карт. Первый выход обрабатывающего устройства 26 соединен посредством соединительной линии 31 со

вторым входом шифратора 25, а второй выход обрабатывающего устройства 26 соединен посредством соединительной линии 32 со вторым входом шифратора 27. Выход шифратора 25 соединен посредством соединительной линии 33 с первым входом второго сравнивающего устройства 28, а выход шифратора 27 соединен посредством соединительной линии 34 со вторым входом второго сравнивающего устройства 28, которое снабжено также выходом 35.

Система, показанная на фигуре, работает следующим образом. Первый пользователь, в чьем владении находится в данный момент носитель информации, например, магнитная карточка, на которой хранится первый код 40, помещает указанную магнитную карточку в устройство 3 считывания карт, которое считывает первый код 40 и дополнительные данные (например, номер счета, а также имя и адрес), после чего первый код 40 загружается посредством соединительной линии 10 в шифратор 7, а дополнительные данные загружаются посредством соединительной линии 10 в обрабатывающее устройство 6. Кроме того, указанный первый пользователь посредством клавиатуры 2 генерирует второй код, который загружается посредством соединительной линии 9 в шифратор 5. В ответ на дополнительные данные обрабатывающее устройство 6 генерирует первый ключ, который вводится посредством соединительной линии 12 в шифратор 7, который на основе указанного первого ключа преобразует первый код в преобразованный первый код и передает последний посредством соединительной линии 14 в первое сравнивающее устройство 8. В ответ на дополнительные данные обрабатывающее устройство 6 генерирует также второй ключ, который вводится посредством соединительной линии 11 в шифратор 5, который на основе указанного второго ключа преобразует второй код в преобразованный второй код и передает последний посредством соединительной линии 13 в первое сравнивающее устройство 8, которое сравнивает оба преобразованных кода друг с другом и в случае их равенства генерирует на выходе 15 положительный сигнал опознавания, а в случае их неравенства генерирует на выходе 15 отрицательный сигнал опознавания. На основе положительного сигнала опознавания первый пользователь получает доступ, например, в автомат для выдачи наличных.

Второй пользователь, в чьем владении находится в данный момент этот же носитель информации, например, магнитная карточка, на которой хранится первый код 40, помещает указанную магнитную карточку в устройство 23 считывания карт, которое считывает первый код 40 и дополнительные данные (например, номер счета, а также имя и адрес), после чего первый код 40 загружается посредством соединительной линии 30 в шифратор 27, а дополнительные данные загружаются посредством соединительной линии 30 в обрабатывающее устройство 26. Кроме того, указанный второй пользователь посредством клавиатуры 22 генерирует четвертый код, который загружается посредством соединительной линии 29 в шифратор 25. В ответ на дополнительные данные обрабатывающее устройство 26 генерирует

третий ключ, который вводится посредством соединительной линии 32 в шифратор 27, который на основе указанного третьего ключа преобразует первый код в преобразованный первый код и передает последний посредством соединительной линии 34 во второе сравнивающее устройство 28. В ответ на дополнительные данные обрабатывающее устройство 26 генерирует также четвертый ключ, который вводится посредством соединительной линии 31 в шифратор 25, который на основе указанного четвертого ключа преобразует четвертый код в преобразованный четвертый код и передает последний посредством соединительной линии 33 во второе сравнивающее устройство 28, которое сравнивает оба преобразованных кода друг с другом и в случае их равенства генерирует на выходе 35 положительный сигнал опознавания, а в случае их неравенства генерирует на выходе 35 отрицательный сигнал опознавания. На основе положительного сигнала опознавания второй пользователь получает доступ, например, в автомат для отправки посылок, причем почтовые расходы на подлежащую отправке посылку определяются и взимаются автоматически.

Поскольку второй пользователь не знаком со вторым кодом, ему не удастся получить доступ в автомат для выдачи наличных. Как правило, первый пользователь, если он, например, является владельцем носителя информации или же руководителем фирмы, являющейся владельцем носителя информации и нанимателем второго пользователя, знаком как со вторым, так и с четвертым кодом, хотя это не является обязательным требованием. Таким образом, с помощью одного и того же носителя информации, на котором хранятся первый код и некоторые дополнительные данные, могут быть осуществлены различные процессы опознавания, причем по меньшей мере один из пользователей, ввиду его незнания по меньшей мере одного из кодов, не в состоянии получить положительный результат при завершении по меньшей мере одного из процессов опознавания.

Первый код, хранящийся на носителе записи, является, следовательно, (возможно, зашифрованным) кодом персонального идентификационного номера, и этим, поскольку либо по меньшей мере первый код на основе первого ключа и первый код на основе третьего ключа преобразуются различными способами, либо по меньшей мере второй код на основе второго ключа и четвертый код на основе четвертого ключа преобразуются различными способами, исключается необходимость хранения различных кодов персонального идентификационного номера (например, кода персонального идентификационного номера и кода персонального идентификационного подномера или первого кода и третьего кода) на одном и том же носителе информации. В результате появляется возможность использования широко распространенных в мире стандартных носителей информации (например, магнитных карточек или информационных карточек с встроенной ИС), что, без сомнения, является большим преимуществом.

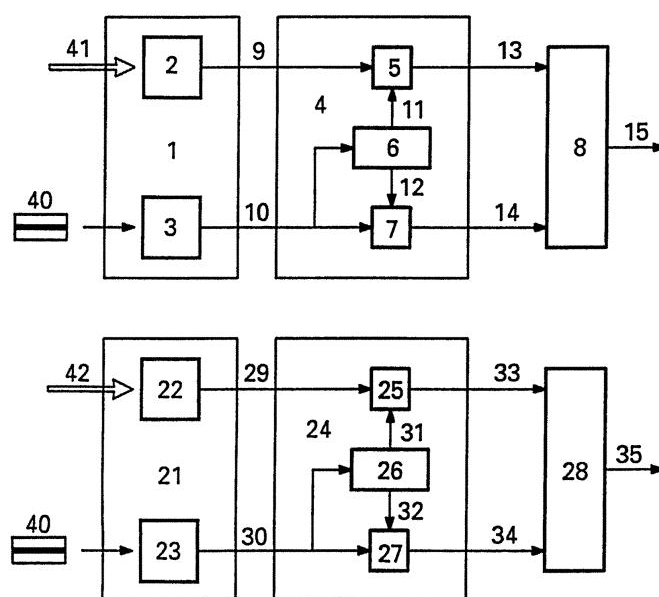
Если как первый код на основе первого ключа и первый код на основе третьего ключа, так и дополнительно второй код на основе второго ключа и четвертый код на основе четвертого ключа пре-

образуются различными способами, защита, как правило, является наилучшей. Путем обеспечения зависимости по меньшей мере одного из преобразований от пятого кода (например, по меньшей мере части дополнительных данных), хранящегося на носителе информации, упомянутая выше защита становится еще более надежной. В этом случае обрабатывающее устройство 6 в ответ на первую часть дополнительных данных (например, номер счета) может генерировать из таблицы первое значение и второе значение, после чего в ответ на вторую часть дополнительных данных (например, имя) первое значение используется для расчета первого ключа, а в ответ на третью часть дополнительных данных (например, адрес) второе значение используется для расчета второго ключа. Кроме того, обрабатывающее устройство 26 в ответ на первую часть дополнительных данных (например, номер счета) может генерировать из таблицы третье значение и четвертое значение, после чего в ответ на вторую часть дополнительных данных (например, имя) третье значение используется для расчета третьего ключа, а в ответ на третью часть дополнительных данных (например, адрес) четвертое значение используется для расчета четвертого ключа. Кроме того, по меньшей мере одно из преобразований может быть осуществлено в зависимости от, например, пятого кода, объединенным способом, известным специалистам в данной области техники, с кодом, поступающим по меньшей мере по одной из соединительных линий 9, 10, 29 и 30.

Обрабатывающее устройство 6 (26) содержит, например, детектор, предназначенный для распознавания дополнительных данных, табличную память, имеющую по меньшей мере три колонки, причем первая колонка предназначена для хранения, например, номеров счетов, вторая колонка предназначена для хранения первого (третьего) ключа или первого (третьего) значения, а третья

колонка предназначена для хранения второго (четвертого) ключа или второго (четвертого) значения, а также содержит процессор, предназначенный для управления детектором и табличной памятью и, возможно, обеспечивающий расчет первого и второго (третьего и четвертого) ключей соответственно на основе первого и второго (третьего и четвертого) значений соответственно и, например, имен и адресов. Шифраторы 5 и 7 (25 и 27) представляют собой, например, схемы кодирования, известные специалистам в данной области техники, которые, например, преобразуют x-битовое входное слово в функции y-битового ключевого слова в z-битовое выходное слово, причем, как правило, применяется соотношение $x=y=z$, хотя это требование не является абсолютно обязательным. Сравнивающее устройство 8 (28) представляет собой, например, компаратор, известный специалистам в данной области техники.

Таким образом, первое преобразующее устройство 4 осуществляет посредством шифратора 7 первое преобразование первого кода в преобразованный первый код на основе первого ключа и, следовательно, осуществляет посредством шифратора 5 второе преобразование второго кода в преобразованный второй код на основе второго ключа. Второе преобразующее устройство 24 осуществляет, таким образом, посредством шифратора 27 третье преобразование первого (= третьего) кода в преобразованный первый (= преобразованный третий) код на основе третьего ключа и, следовательно, осуществляет посредством шифратора 25 четвертое преобразование четвертого кода в преобразованный четвертый код на основе четвертого ключа. Разумеется, могут быть применены и многие другие способы преобразования, известные специалистам в данной области техники, например, не основанные на использовании ключей.



Фиг.

ДП "Український інститут промислової власності" (Укрпатент)
Україна, 01133, Київ-133, бульв. Лесі Українки, 26
(044) 295-81-42, 295-61-97

Підписано до друку _____ 2002 р. Формат 60х84 1/8.
Обсяг _____ обл.-вид. арк. Тираж 50 прим. Зам. _____

УкрІНТЕІ, 03680, Київ-39 МСП, вул. Горького, 180.
(044) 268-25-22
