



УКРАЇНА

(19) UA (11) 61612 (13) A

(51) 7 H04L9/00

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІОПИС
ДО ДЕКЛАРАЦІЙНОГО ПАТЕНТУ
НА ВИНАХІДВидається під
відповідальність
власника
патенту

(54) СПОСІБ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ І КРИПТОГРАФІЧНА СИСТЕМА ДЛЯ ЙОГО ЗДІЙСНЕННЯ

1

(21) 2003032304

(22) 17 03 2003

(24) 17 11 2003

(46) 17 11 2003, Бюл. № 11, 2003 р

(72) Горицький Віктор Михайлович, Полозюк Олександр Миколайович, Зубченко Артем Петрович

(73) ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ НАУКОВО-ВИРОБНИЧА ФІРМА "САЙФЕР"

(57) 1 Спосіб криптографічного захисту інформації, згідно з яким на станції відправника генерують початкову інформаційну послідовність \bar{S} і перетворюють її шляхом кодування в інформаційну послідовність \bar{X} , яку передають через вільний від помилок канал зв'язку до станції одержувача, де її шляхом декодування перетворюють у початкову інформаційну послідовність \bar{S} , який відрізняється тим, що згенеровану на станції відправника початкову інформаційну послідовність \bar{S} перетворюють в інформаційну послідовність \bar{X} за допомогою комбінованого кодування, у той же час на станції одержувача генерують рівномірну випадкову послідовність \bar{R} , яку затримують для подальшого використання, а її дубль передають через канал з перешкодами до станції відправника, де здійснюють складання за модулем 2 послідовності \bar{X} та послідовності \bar{R} , що пройшла через канал з перешкодами, у результаті чого отримують інформаційну послідовність \bar{Y} , яку передають через вільний від помилок канал до станції одержувача, де здійснюють складання за модулем 2 послідовності \bar{Y} та згаданої рівномірної випадкової послідовності \bar{R} , затриманої на час, необхідний для її проходження через канал з перешкодами від станції одержувача до станції відправника, складання за модулем 2 з послідовністю \bar{X} і повернення через вільний від помилок канал до станції одержувача, в результаті чого отримують інформаційну послідовність \bar{X} , яку шляхом комбінованого декодування перетворюють у початкову інформаційну послідовність \bar{S} .

2

2 Спосіб за п. 1, який відрізняється тим, що комбіноване кодування початкової інформаційної послідовності \bar{S} полягає у тому, що спочатку здійснюють її випадкове кодування в суміжних класах коду V , після чого - кодування перешкодостійким кодом G , а комбіноване декодування інформаційної послідовності \bar{X} полягає у тому, що спочатку здійснюють її декодування перешкодостійким кодом G , після чого - не випадкове декодування в суміжних класах коду V .

3 Спосіб за п. 1, який відрізняється тим, що комбіноване кодування початкової інформаційної послідовності \bar{S} полягає у тому, що спочатку здійснюють її кодування перешкодостійким кодом G , після чого - випадкове кодування в суміжних класах коду V , а комбіноване декодування інформаційної послідовності \bar{X} полягає у тому, що спочатку здійснюють її не випадкове декодування в суміжних класах коду V , після чого - декодування перешкодостійким кодом G .

4 Криптографічна система для захисту інформації, яка має станцію відправника і станцію одержувача, з'єднані між собою вільним від помилок каналом для передачі закодованої інформаційної послідовності від станції відправника до станції одержувача і каналом для передачі допоміжних даних від станції одержувача до станції відправника, причому станція відправника містить генератор початкової інформаційної послідовності, вихід якого з'єднаний з входом кодера, а станція одержувача містить декодер і блок зберігання, яка відрізняється тим, що канал для передачі допоміжних даних від станції одержувача до станції відправника є каналом з перешкодами, станція відправника містить перший суматор за модулем 2, перший вхід якого з'єднаний з виходом згаданого кодера, який є кодером комбінованого кодування, другий - з виходом каналу для передачі допоміжних даних від станції одержувача до станції відправника, а вихід - з входом каналу для передачі закодованої інформаційної послідовності від станції відправника до станції одержувача, яка містить генератор випадкової послідовності, лінію затримки і другий суматор за модулем 2, причому вихід генератора випадкової послідовності підключений до входу

(19) UA (11) 61612 (13) A

каналу для передачі допоміжних даних від станції одержувача до станції відправника і до входу лінії затримки, вихід якої з'єднаний з першим входом другого суматора за модулем 2, другий вхід якого з'єднаний з виходом каналу для передачі закодованої інформаційної послідовності від станції відправника до станції одержувача, а вихід - з входом декодера, який є декодером комбінованого декодування, вихід якого підключений до входу блока зберігання

5 Криптографічна система за п 4, яка відрізняється тим, що кодер комбінованого кодування містить послідовно з'єднані кодер випадкового кодування і кодер перешкодостійкого кодування, причому вхід кодера випадкового кодування є входом кодера комбінованого кодування, а вихід кодера перешкодостійкого кодування - виходом кодера комбінованого кодування, декодер комбінованого декодування містить послідовно з'єднані декодер невинного декодування і декодер перешкодостійкого декодування, причому вхід декодера невинного декодування є входом декодера комбінованого декодування, а вихід декодера перешкодостійкого декодування є входом декодера комбінованого декодування, а вихід декодера

невинного декодування - виходом декодера комбінованого декодування

6 Криптографічна система за п 4, яка відрізняється тим, що кодер комбінованого кодування містить послідовно з'єднані кодер перешкодостійкого кодування і кодер випадкового кодування, причому вхід кодера перешкодостійкого кодування є входом кодера комбінованого кодування, а вихід кодера випадкового кодування - виходом кодера комбінованого кодування, декодер комбінованого декодування містить послідовно з'єднані декодер невинного декодування і декодер перешкодостійкого декодування, причому вхід декодера невинного декодування є входом декодера комбінованого декодування, а вихід декодера перешкодостійкого декодування - виходом декодера комбінованого декодування

7 Криптографічна система за будь-яким із пп 4-6, яка відрізняється тим, що вільний від помилок канал для передачі закодованої інформаційної послідовності від станції відправника до станції одержувача має на своєму вході каналний кодер перешкодостійкого кодування, а на виході - каналний декодер перешкодостійкого декодування

Винахід належить до галузі електрозв'язку, а саме до криптографічних засобів захисту інформації, яка передається принаймні між двома станціями, і його може бути використано для безпечної обміну секретною інформацією через відкриті канали зв'язку у тому числі і для безпечного розповсюдження через такі канали криптографічних ключів з метою їх подальшого використання у відомих системах шифрування

У зв'язку з постійним зростанням цінності інформації усе більш актуальною стає задача її захисту від загроз, у тому числі від несанкціонованого доступу, зокрема, під час обміну даними через відкриті телекомунікаційні канали. Для вирішення цієї задачі, наряду з іншими засобами, використовують криптографічні способи і системи

Широко відомі криптографічні способи захисту інформації, які полягають у тому, що генеровану на станції відправника початкову інформаційну послідовність за допомогою секретного ключа і певної функції шифрування перетворюють у криптограму, яку передають через відкритий канал зв'язку до станції одержувача, де за допомогою цього ж секретного ключа, переданого через захищений канал, і відповідної функції дешифрування здійснюють зворотне перетворення отриманої криптограми у початкову інформаційну послідовність [1]

Для забезпечення достатньої стійкості криптографічної системи, тобто здатності протистояти всіляким загрозам, в тому числі розкриттю інформації, застосовують складні алгоритми перетворення інформації, в тому числі і такі, що задаються секретним ключем. Причому стійкість криптосистеми знаходиться у прямій залежності від розміру її секретного ключа

Так, відомі способи криптографічного захисту

інформації від несанкціонованого доступу, які полягають у тому, що формують секретний ключ, і початкову інформаційну послідовність розбивають на блоки певного розміру, кожен із яких у свою чергу розбивають на два підблоки. Ці підблоки перетворюють відповідно до секретного ключа з використанням операцій перестановки, підстановки і складання за модулем 2, після чого підблоки міняють місцями [2]. У криптографічних системах для здійснення таких способів використовують секретні ключі відносно невеликого розміру (56 бітів), які можна підібрати, зважаючи на потужність сучасних комп'ютерних засобів аналізу

Більш складні перетворення і відповідно більшу стійкість забезпечує відомий криптографічний спосіб захисту інформації, згідно з яким формують секретний ключ у вигляді сукупності підключів, розбивають кожний з блоків початкової інформаційної послідовності на підблоки, які по чергову перетворюють, здійснюючи над ними операцію складання за модулем 2, що виконується над підблоком і підключем, а також над обома підблоками, і операцію циклічного зсуву вліво. При цьому число бітів, на яке зсувається перетворюваний підблок, залежить від значення іншого підблоку [3]. Стійкість криптографічних систем для здійснення цього способу залежить від можливого числа варіантів циклічного зсуву і обмежена кількістю бінарних розрядів підблоку. Такі криптосистеми можуть бути розкриті з використанням диференціального і лінійного аналізу за допомогою сучасних комп'ютерних засобів

Підвищити стійкість криптосистеми щодо диференціального і лінійного аналізу шляхом збільшення числа варіантів операцій, пов'язаних з перетворенням, і забезпечення недетермінованості модифікації цих варіантів дозволяє спосіб, згідно з

яким кожний блок початкової інформаційної послідовності розбивають принаймні на два підблоки, які по чергові перетворюють шляхом виконання над кожним із них операції перестановки бітів, яка залежить від секретного ключа, від значення іншого підблока і від результатів попереднього кроку перетворення іншого підблока [4].

Однак цей спосіб, як і усі раніше згадані, не може забезпечити такої стійкості криптографічної системи, при якій криптоаналітик (підслухувач), підключившись відвідним каналом до відкритого каналу зв'язку, через який передається криптограма, не міг би за певних здійснених умов розшифрувати її, володіючи достатньо ефективними аналітичними ресурсами.

Для забезпечення теоретичної стійкості криптограми (неможливості її розкриття без володіння секретним ключем) невизначеність секретного ключа повинна бути не менше невизначеності початкової інформаційної послідовності, що підлягає шифруванню. Це означає, що ключ повинен бути не коротшим за цю послідовність, тобто неприпустимо великим для більшості використань, що робить абсолютно стійкий шифр дуже дорогим і непрактичним. При цьому, усіх законних користувачів криптографічної системи необхідно завчасно забезпечити запасом секретних ключів із виключенням можливості їхнього повторного використання. Спосіб доставки секретних ключів повинен бути абсолютно безпечним, що навіть для сучасних телекомунікаційних систем є дуже непростюю задачею. Дотепер єдиною надійною системою доставки секретного ключа є довірений кур'єр. Однак цей канал є порівняно дорогим, повільним, а іноді, наприклад під час конфліктних ситуацій, нездійсненним.

На принципово новому підході до шляхів захисту інформації, а саме на врахуванні різниці між шумовими характеристиками каналу законних користувачів і каналу криптоаналітика (відвідного каналу), базуються описані у патенті США [5] спосіб і криптографічна система для його здійснення, які за своєю суттю найбільш близькі до запропонованого винаходу.

Згідно з цим відомим способом, на станції відправника генерують початкову інформаційну послідовність і перетворюють її шляхом кодування в іншу інформаційну послідовність, яку передають через вільний від помилок канал зв'язку до станції одержувача. Кодування здійснюють шляхом конкатенації згаданої початкової інформаційної послідовності з випадковою послідовністю, згенерованою на станції відправника. На станції одержувача прийняту закодовану інформаційну послідовність декодують і обробляють певним чином із метою визначення, чи є вона достатньо надійною. За результатами обробки генерують відповідні допоміжні дані, які через інший вільний від помилок канал зв'язку передають до станції відправника, де вони враховуються при подальшому генеруванні інформаційної послідовності.

Криптографічна система для здійснення цього способу містить станцію відправника і станцію одержувача, з'єднані між собою вільним від помилок каналом для передачі закодованої інформаційної послідовності від станції відправника до

станції одержувача і вільним від помилок каналом для передачі допоміжних даних від станції одержувача до станції відправника, причому станція відправника містить генератор (засіб зберігання) початкової інформаційної послідовності, вихід якого з'єднаний з входом кодера, а станція одержувача містить декодер і блок зберігання.

Цей спосіб і система для його здійснення, які призначені для формування спільного секретного ключа двома користувачами відкритого каналу, хоча і забезпечують абсолютну секретність (теоретичну стійкість) такого ключа, однак лише за умови, що канал криптоаналітика більш зашумлений, ніж канал законних користувачів. Але на практиці цю умову не завжди може бути дотримано. Крім того, подальше використання у криптографічних системах отриманого таким чином секретного ключа супроводжується усіма притаманними таким системам недоліками, які зазначені вище при характеристиці аналогів.

Задачею винаходу є створення такого криптографічного способу і такої системи для захисту інформації, які б забезпечували її теоретичну стійкість без використання секретного ключа навіть у разі, коли канал криптоаналітика менш зашумлений, ніж канал законних користувачів. Ця задача вирішується шляхом використання системи комбінованого кодування-декодування і створення при цьому таких умов, щоб ймовірність помилки в розрахунку на один біт у каналі криптоаналітика перевищувала ймовірність помилки в розрахунку на один біт у каналі законних користувачів.

Для вирішення цієї задачі у способі криптографічного захисту інформації, згідно з яким на станції відправника генерують початкову інформаційну послідовність \bar{S} і перетворюють її шляхом кодування в інформаційну послідовність \bar{X} , яку передають через вільний від помилок канал зв'язку до станції одержувача, де її шляхом декодування перетворюють у початкову інформаційну послідовність \bar{S} , відповідно до винаходу, генеровану на станції відправника початкову інформаційну послідовність \bar{S} перетворюють в інформаційну послідовність \bar{X} за допомогою комбінованого кодування. У той же час на станції одержувача генерують рівномірну випадкову послідовність \bar{R} , яку затримують для подальшого використання, а її дубль передають через канал із перешкодами до станції відправника, де здійснюють складання за модулем 2 послідовності \bar{X} та послідовності \bar{R} , що пройшла через канал із перешкодами. У результаті отримують інформаційну послідовність \bar{Y} , яку передають через вільний від помилок канал до станції одержувача, де здійснюють складання за модулем 2 послідовності \bar{Y} та згаданої рівномірної випадкової послідовності \bar{R} , затриманої на час, необхідний для її проходження через канал з перешкодами від станції одержувача до станції відправника, складання по модулю 2 з послідовністю \bar{X} і повернення через вільний від помилок канал до станції одержувача. В результаті отримують інформаційну послідовність \bar{X}' , яку

шляхом комбінованого декодування перетворюють у початкову інформаційну послідовність \bar{S}

Комбіноване кодування початкової інформаційної послідовності \bar{S} полягає у тому, що спочатку здійснюють її випадкове кодування в суміжних класах обраного коду V , після чого - кодування перешкодостійким кодом G , а комбіноване декодування інформаційної послідовності \bar{X} полягає у тому, що спочатку здійснюють її декодування перешкодостійким кодом G , після чого - не випадкове декодування в суміжних класах коду V

Згідно з іншим варіантом способу, комбіноване кодування початкової інформаційної послідовності \bar{S} полягає у тому, що спочатку здійснюють її кодування перешкодостійким кодом G , після чого - випадкове кодування в суміжних класах обраного коду V , а комбіноване декодування інформаційної послідовності \bar{X} полягає у тому, що спочатку здійснюють її не випадкове декодування в суміжних класах коду V , після чого - декодування перешкодостійким кодом G

У криптографічній системі для захисту інформації від несанкціонованого доступу, яка має станцію відправника і станцію одержувача, з'єднані між собою вільним від помилок каналом для передачі закодованої інформаційної послідовності від станції відправника до станції одержувача і каналом для передачі допоміжних даних від станції одержувача до станції відправника, причому станція відправника містить генератор початкової інформаційної послідовності, вихід якого з'єднано з входом кодера, а станція одержувача містить декодер і блок зберігання, відповідно до винаходу, канал для передачі допоміжних даних від станції одержувача до станції відправника є каналом з перешкодами. Крім того, станція відправника містить перший суматор за модулем 2, перший вхід якого з'єднано з виходом згаданого кодера, який є кодером комбінованого кодування, другий - з виходом каналу для передачі допоміжних даних від станції одержувача до станції відправника, а вихід - з входом каналу для передачі закодованої інформаційної послідовності від станції відправника до станції одержувача. Станція одержувача містить генератор випадкової послідовності, лінію затримки і другий суматор за модулем 2. Вихід генератора випадкової послідовності підключено до входу каналу для передачі допоміжних даних від станції одержувача до станції відправника, і до входу лінії затримки. Вихід лінії затримки з'єднано з першим входом другого суматора за модулем 2. Другий вхід суматора за модулем 2 з'єднано з виходом каналу для передачі закодованої інформаційної послідовності від станції відправника до станції одержувача, а вихід - з входом декодера, який є декодером комбінованого декодування, вихід якого підключено до входу блока зберігання.

Кодер комбінованого кодування містить послідовно з'єднані кодер випадкового кодування і кодер перешкодостійкого кодування. Вхід кодера випадкового кодування є входом кодера комбінованого кодування, а вихід кодера перешкодостійкого кодування - виходом кодера комбінованого кодування. Декодер комбінованого декодування

містить послідовно з'єднані декодер перешкодостійкого декодування і декодер не випадкового декодування. Вхід декодера перешкодостійкого декодування є входом декодера комбінованого декодування, а вихід декодера не випадкового декодування - виходом декодера комбінованого декодування.

Згідно з іншим варіантом криптографічної системи, кодер комбінованого кодування містить послідовно з'єднані кодер перешкодостійкого кодування і кодер випадкового кодування. Вхід кодера перешкодостійкого кодування є входом кодера комбінованого кодування, а вихід кодера випадкового кодування - виходом кодера комбінованого кодування. Декодер комбінованого декодування містить послідовно з'єднані декодер не випадкового декодування і декодер перешкодостійкого декодування. Вхід декодера не випадкового декодування є входом декодера комбінованого декодування, а вихід декодера перешкодостійкого декодування - виходом декодера комбінованого декодування.

Для уникнення помилок канал для передачі закодованої інформаційної послідовності від станції відправника до станції одержувача може мати на своєму вході каналний кодер перешкодостійкого кодування, а на виході - каналний декодер перешкодостійкого декодування.

Суть винаходу пояснюється графічними матеріалами, де зображені у вигляді функціональної схеми

Фіг. 1 - криптографічна система,

Фіг. 2 - вільний від помилок канал для передачі закодованої інформаційної послідовності від станції відправника до станції одержувача,

Фіг. 3 - перший варіант кодера комбінованого кодування,

Фіг. 4 - перший варіант декодера комбінованого декодування,

Фіг. 5 - другий варіант кодера комбінованого кодування,

Фіг. 6 - другий варіант декодера комбінованого декодування.

Запропонована криптографічна система містить станцію 1 відправника і станцію 2 одержувача. Вони з'єднані між собою вільним від помилок каналом 3, призначеним для передачі закодованої інформаційної послідовності від станції 1 відправника до станції 2 одержувача, і каналом 4 з перешкодами, призначеним для передачі допоміжних даних від станції 2 одержувача до станції 1 відправника. Причому, канал 4 може, за потреби, мати засоби для штучного створення перешкод. Обидва канали 3, 4 є складовими каналу законних користувачів.

Станція 1 відправника містить генератор 5 початкової інформаційної послідовності (ГПП), кодер 6, і перший суматор 7 за модулем 2. Як генератор 5 початкової інформаційної послідовності може використовуватися засіб її зберігання або генератор рівномірної випадкової послідовності. Вихід ГПП з'єднано з входом кодера 6. Перший вхід суматора 7 за модулем 2 з'єднано з виходом кодера 6, другий - з виходом каналу 4 з перешкодами, а вихід - з входом вільного від помилок каналу 3.

Станція 2 одержувача містить другий суматор

8 за модулем 2, декодер 9, блок 10 зберігання (БЗ), генератор 11 випадкової послідовності (ГВП) і лінію 12 затримки (ЛЗ). Вихід ГВП 11 підключено до входу каналу 4 з перешкодами і до входу ЛЗ 12, вихід якої з'єднано з першим входом другого суматора 8 за модулем 2. Другий вхід суматора 8 за модулем 2 з'єднано з виходом вільного від помилок каналу 3, а вихід - з входом декодера 9, вихід якого підключено до входу БЗ 10.

Під каналом розуміється сукупність засобів, необхідних для перенесення інформації від однієї станції до іншої. Звичайно, канал містить провідну або безпроводну лінію зв'язку, на одному кінці якої знаходиться передавач 14, на іншому - приймач 15.

Для безпомилкової передачі закодованої інформаційної послідовності від станції 1 відправника до станції 2 одержувача канал 3 може містити (але не обов'язково) на вході каналний кодер 16 перешкодостійкого кодування (КПК), а на виході - каналний декодер 17 перешкодостійкого декодування (КДПД).

Кодер 6 є кодером комбінованого кодування. Декодер 9 є декодером комбінованого декодування.

В одному з варіантів (Фіг. 3, 4) кодер 6 комбінованого кодування містить послідовно з'єднані кодер 18 випадкового кодування (КВК) і кодер 19 перешкодостійкого кодування (КПК). Вхід КВК 18 є входом кодера 6 комбінованого кодування, а вихід КПК 19 - виходом кодера 6 комбінованого кодування. У цьому ж варіанті декодер 9 комбінованого декодування містить послідовно з'єднані декодер 20 перешкодостійкого декодування (ДПД) і декодер 21 не випадкового декодування (ДНД). Вхід ДПД 20 є входом декодера 9 комбінованого декодування, а вихід ДНД 21 - виходом декодера 9 комбінованого декодування.

В іншому варіанті (Фіг. 5, 6) кодер 6 комбінованого кодування містить послідовно з'єднані КПК 19 і КВК 18. Вхід КПК 19 є входом кодера 6 комбінованого кодування, а вихід КВК 18 - виходом кодера 6 комбінованого кодування. У цьому ж варіанті декодер 9 комбінованого декодування містить послідовно з'єднані ДНД 21 і ДПД 20. Вхід ДНД 21 є входом декодера 9 комбінованого декодування, а вихід ДПД 20 - виходом декодера 9 комбінованого декодування.

Елементи запропонованої криптографічної системи можуть бути виконані як апаратно, так і програмно. Функціонує вона, як викладено далі.

На станції 1 відправника початкова інформаційна послідовність \bar{S} з виходу ГПП 5 надходить на вхід кодера 6, де її шляхом комбінації випадкового кодування і перешкодостійкого кодування з урахуванням помилок, властивих каналу 4 з перешкодами, перетворюють у послідовність \bar{X} , яка надходить на перший вхід першого суматора 7 за модулем 2. У той же час на станції 2 одержувача ГВП 11 генерує допоміжні дані у вигляді рівномірної випадкової послідовності R , яка надходить на вхід ЛЗ 12, а її дубль передається через канал 4 з перешкодами, після чого надходить на другий вхід суматора 7. На виході суматора 7 за модулем 2 з'являється інформаційна послідовність

$\bar{Y} = \bar{X} \oplus \bar{R}$, де \bar{R} - інформаційна послідовність \bar{R} , що пройшла через канал з перешкодами.

Інформаційна послідовність \bar{Y} через вільний від помилок канал 3 надходить на вхід другого суматора 8 за модулем 2. На інший вхід суматора 8 з виходу ЛЗ 12 подається випадкова інформаційна

послідовність \bar{R} , затримана на час, необхідний для проходження даних через канал 4 від станції 2 одержувача до станції 1 відправника, складання їх за модулем 2 у суматорі 7 і повернення через канал 3 від станції 1 відправника до станції 2 одержувача. В результаті, з виходу суматора 8 на вхід декодера 9 надходить інформаційна послідовність \bar{X} , яка настільки відрізняється від послідовності \bar{X} , наскільки R відрізняється від R .

$$\bar{X}' = \bar{Y} \oplus \bar{R} = \bar{X} \oplus \bar{R} \oplus \bar{R}$$

Отже у суматорі 8 за модулем 2 відбувається звільнення інформаційної послідовності \bar{Y} , отриманої через вільний від помилок канал 3, від послідовності \bar{R} , але із записанням у ній помилок, внесених каналом 4 з перешкодами.

Декодер 9 шляхом комбінації не випадкового декодування і перешкодостійкого декодування, яке враховує помилки, що вносить канал 4 з перешкодами, перетворює інформаційну послідовність \bar{X}' у початкову інформаційну послідовність \bar{S} .

Комбіноване кодування-декодування може здійснюватися з використанням кодової книги, яка утворюється шляхом декомпозиції лінійного двійкового коду G на 2^k суміжних класів по його підкоду V . Причому, код G обирається з урахуванням помилок каналу 4 з перешкодами і має параметри (n, n') , де n - довжина кодового слова, n' - число інформаційних символів у кодовому слові коду G , а підкод V має параметри $(n, n' - k)$, де n - довжина кодового слова, $(n' - k)$ - число інформаційних символів у кодовому слові підкоду V , $k = (n - n')$ - число перевірючих символів у кодовому слові коду G . При цьому кожному суміжному класу ставиться в однозначну відповідність двійковий k -мірний вектор $s = s_1, s_2, \dots, s_k$, який відповідає слову інформаційної послідовності \bar{S} на вході кодера. Якщо на вхід кодера надходить слово s_j , $j = 1, 2, \dots, 2^k$, то на його виході з'являється випадково та рівномірно обране слово x з j -го суміжного класу підкоду V , тобто $x = f(s_j, r)$, $r = 1, 2, \dots, 2^{n-k}$, де r - номер згаданого рівномірно обраного слова. Декодування

інформаційної послідовності \bar{X}' полягає у тому, що спочатку визначається номер j суміжного класу коду G , який відповідає прийнятому слову x' інформаційної послідовності \bar{X}' , потім один з представників лідера цього суміжного класу складається поелементно з прийнятим кодовим словом, в якому враховано помилки каналу 4 з перешкодами, і за результатами складання однозначно визначається передане слово s_j інформаційної послідовності \bar{S} [6].

Отже, завдяки накладанню на випадкову інформаційну послідовність помилок каналу 4 з перешкодами, які враховуються законними користу-

вачами при прямому і зворотному перетворенні даних у системі, але не можуть бути у достатній мірі враховані криптоаналітиком, запропонований спосіб і криптографічна система для його здійснення створюють такі умови, за яких ймовірність помилки в розрахунку на один біт у каналі криптоаналітика перевищує ймовірність помилки в розрахунку на один біт у каналі законних користувачів, що забезпечує теоретичну стійкість криптограми без використання секретного ключа навіть у разі, коли канал криптоаналітика менш зашумлений, ніж канал законних користувачів

ДЖЕРЕЛА ШФОРМАЦІЇ

1 Мессі Дж Л Введение в современную криптологию // ТИИЭР - Т 76 - 1988 - № 5 - С 24 -

42

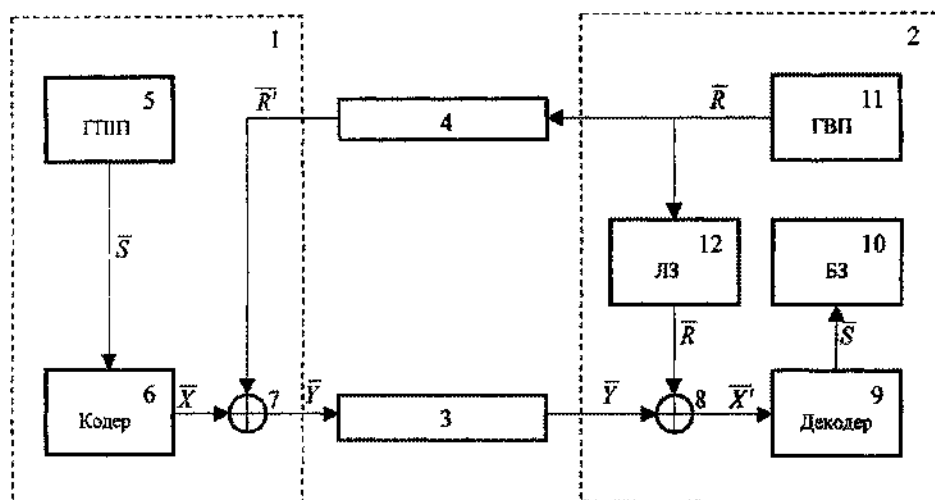
2 National Bureau of Standards Data Encryption Standard Federal Information Processing Standards Publication 46 January 1977

3 R. Rivest, The RC5 Encryption Algorithm, Fast Software Encryption, Second International Workshop Proceedings (Leuven, Belgium, December 14 - 16, 1994), Lecture Notes in Computer Science, v 1008, Springer-Verlag, 1995, P 86 - 96

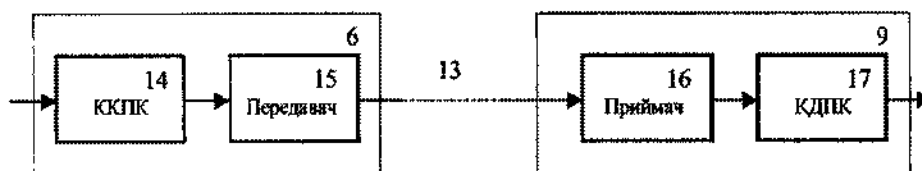
4 Патент України №49102

5 Патент США №5161244

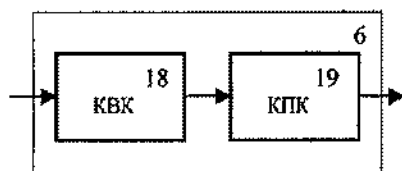
6 Коржик В И, Яковлев В А Пропускная способность канала связи с внутренним случайным кодированием // Пробл передачи информ 1992 Т 28 №4 С 24 - 34



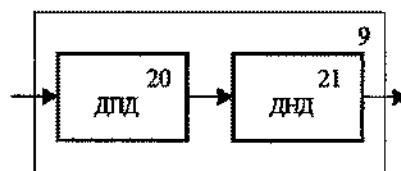
Фиг. 1



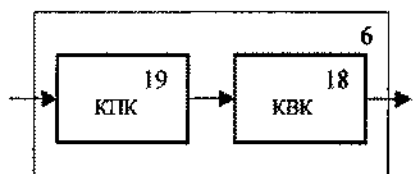
Фиг. 2



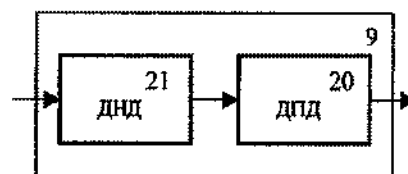
Фиг. 3



Фиг. 4



Фиг. 5



Фиг. 6

