УДК 681.142.642.2

В.С. Глухов, А.О. Мельник, В.Я. Пуйда
Національний університет "Львівська політехніка",
кафедра “Електронні обчислювальні машини”

ДОСЛІДЖЕННЯ ШЛЯХІВ СТВОРЕННЯ КОДЕРА ТА ДЕКОДЕРА ВІДЕОСИГНАЛУ

Описано принципи побудови кодерів та декодерів для захисту телевізійних сигналів від несанкціонованого доступу у кабельних телевізійних мережах. Також описано реалізацію цих принципів у побутовій техніці з використанням сучасних мікроконтролерів та програмованих логічних інтегральних схем. Для забезпечення захисту пропонується реалізувати в кодерах і декодерах алгоритми шифрування типу ГОСТ 28147-89 або DES і методи завадостійкого кодування згідно з рекомендаціями Європейської космічної агенції (ESA).

The TV videosignal coder and decoder principals of building are described. Also realization of these principals in consumer electronics with modern microcontrollers and field programmable gate arrays usage is described. For signals protection the symmetric block syphers GOST 28147-89 or DES and data coding according to ESA recommendation are selected.

Вступ

Зростаючі вимоги до якості телевізійного сигналу та розширення функціональних можливостей систем прикладного телебачення приводять до необхідності використання цифрових методів при формуванні і прийомі телевізійних сигналів [1,2]. Водночас збільшується і коло задач, які вимагають застосування цифрових методів для свого вирішення. Одна з таких задач – запобігання несанкціонованого перегляду телевізійних трансляцій, в тому числі і трансляцій по кабельній мережі.

Для створення кодера та декодера, призначених для захисту телевізійного сигналу , що передається по кабельній мережі, від несанкціонованого перегляду, необхідно серед інших вирішити такі задачі:

- вибрати метод маскування сигналу (по ВЧ, відео, звуку);
- забезпечити оперативну дистанційну зміну коду в системі;
- забезпечити функціонування програмної оболонки (оперативну роботу оператора з абонентськими декодерами);
- мінімізувати конструктивні зв’язки між декодером та абонентським телевізійним приймачем.

Додатково можуть вирішуватись питання забезпечення адресної активації повідомлень, записаних в постійну пам’ять абонентського декодера, і надання адресних платних послуг.

1. Методи закриття відеосигналу

Процедура закриття відеосигналу складається з таких процесів:

- спотворення початкового сигналу у передавальному центрі і його відтворення у абонента згідно з обраним алгоритмом;
- вилучення із закритого відеосигналу непрямих ознак алгоритму закриття і його параметрів (ключів);
- пересилання в завадозахищеному вигляді алгоритму та його параметрів від передавального центру до абонента.

Залежно від організації методи закриття можуть бути:

- аналоговими (рис. 1);
- цифро-аналоговими (аналогове кодування–декодування, цифрове управління, рис. 2);
- цифровими (рис. 3).

Рис. 1. Структурна схема аналогового методу закриття відеосигналу

З наведених структурних схем видно, що найпростіше реалізується аналогове закриття відеосигналу (але таке закриття і найлегше розкривається зловмисниками – "піратами"), а найскладніше (із точки зору як реалізації, так і зламу) – цифрове.

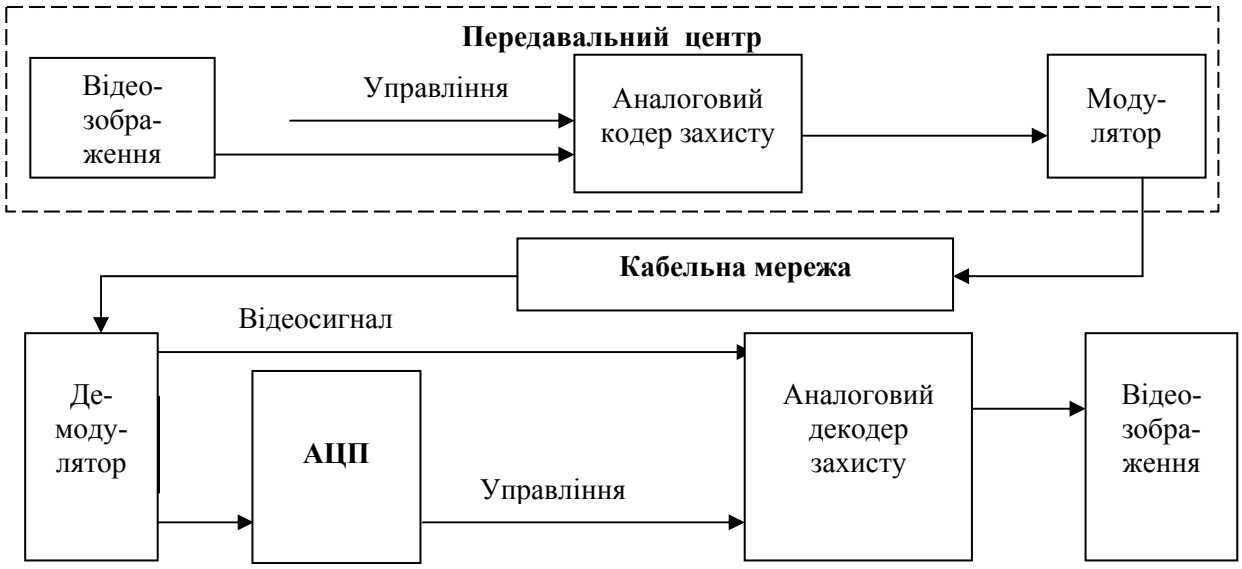

Рис. 2. Структурна схема цифро-аналогового методу закриття відеосигналу

При використанні цифро-аналогового методу, наприклад, інвертування рядків відеокадру у псевдовипадковому порядку, сам порядок інвертування визначається цифровими методами, а інвертування, тобто заміна білого кольору на чорний і навпаки, здійснюється аналоговими методами. Генератор псевдовипадкової послідовності формує для кожного рядка ознаку 0, якщо даний рядок не інвертується, і 1 – якщо інвертується. Але при такому

кодуванні форма сигналу на початку відеорядка може вказати “піратам” на те, інвертований він чи ні. Тому необхідно впроваджувати додаткові заходи для вилучення з відеокадру непрямих ознак того, що саме було зроблено з відеорядком під час його закриття.

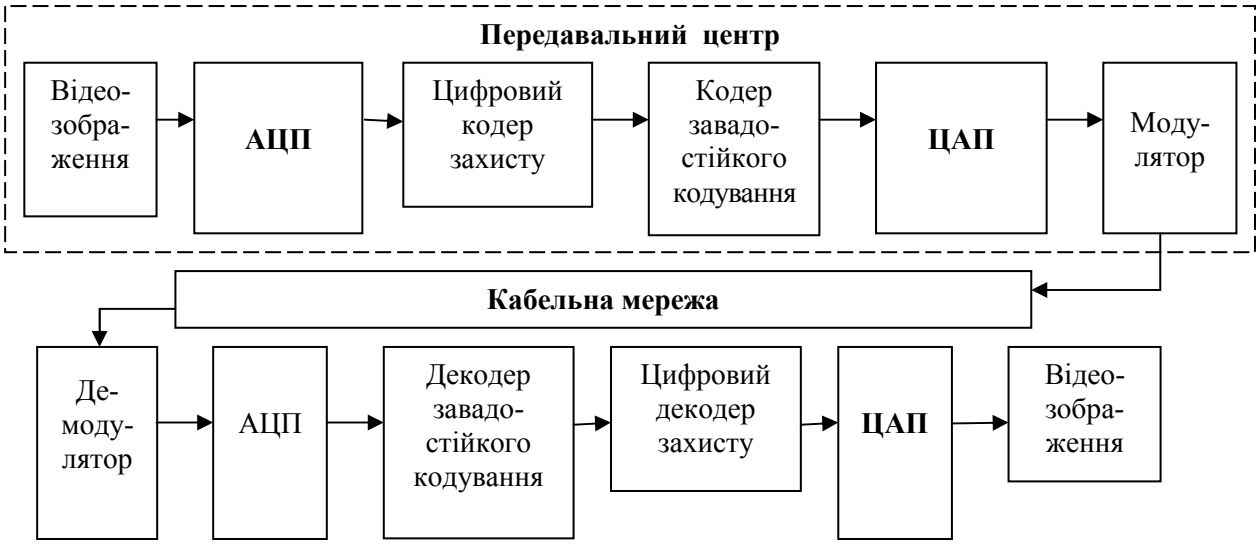

Рис. 3. Структурна схема цифрового методу закриття відеосигналу

Крім цього, потрібно передавати абонентам ознаки того, які рядки у відеокадрі будуть інвертуватися, а які – ні. Для цього кожному абоненту час від часу передається у закодованому вигляді нове значення початкового стану генератора псевдовипадкової послідовності. Цей генератор входить до складу декодера абонента.

Щоб управляти декодерами абонентів, кожному з них потрібно передавати початкові стани генераторів псевдовипадкової послідовності, закодовані власним ключем абонента для того, щоб тільки цей абонент і міг їх розшифрувати.

Для шифрування цифрової інформації відомі і широко використовуються алгоритми шифрування (ГОСТ 28147-89 [3], DES, а також інші алгоритми [4]), які гарантовано вилучають із зашифрованого повідомлення будь-яку інформацію про перетворення, які були зроблені. Це призводить до того, що розшифрувати таке повідомлення без знання ключа практично неможливо.

Для аналогових сигналів такі підходи невідомі, тобто аналогові сигнали несуть у собі відбиток тих перетворень, які над ними здійснювали, що полегшує дешифрацію (зворотне перетворення) таких сигналів.

Тому цифро-аналогові методи закриття відеосигналів забезпечують надійне закриття цифрових сигналів і ненадійне – аналогових, але є простішими і дешевшими у реалізації порівняно з цифровими методами.

При використанні суто цифрових методів закриття відеоінформації у цифровому вигляді зашифровується сама відеоінформація, що дозволяє вилучати з неї будь-які натяки на перетворення, яким вона підлягала. Це робить ці системи надзвичайно надійними, але дорожчими порівняно з цифро-аналоговими.

2. Забезпечення стійкості закриття відеосигналу

Стійкість цифрового коду залежить від часу його розкриття. Теоретично можна методом простого перебору розкрити будь-який шифр, питання тільки в тому, скільки на це піде часу. При кодуванні телесигналу стійкість визначається такими моментами:

1) неможливістю дізнатися про ключ конкретного користувача і повторити схему з цим ключем та програму його використання. Для цього в декодерах використовуються мікроконтролери, з яких не можна прочитати програму їхньої роботи;

2) неможливістю розкриття ключа при підслуховуванні закодованого телесигналу. Це забезпечується використанням надійного алгоритму шифрування, наприклад, DES;

3) неможливістю відтворення телесигналу методом простого перебору усіх можливих варіантів шифрування. Це можна забезпечити існуванням такої кількості варіантів, яку можна перебрати і візуально оцінити лише за час, більший ніж період зміни ключа шифрування.

При використанні цифро-аналогового методу закриття відеосигналу доцільно транслювати управляючу інформацію у форматі телетексту [5], а для її виділення використовувати мікросхеми декодерів телетексту. Це дасть можливість крім виконання основної функції з закриття, реалізувати додаткові функції, такі як телетекст або частково Інтернет. Блок-схеми пропонованих декодера і кодера наведені на рис. 4 і 5 відповідно.

Враховуючи поширеність неліцензійних декодерів систем платного кабельного телебачення, які побудовані на базі простих методів кодування, доцільним є використання сучасних цифрових методів шифрування, які практично неможливо розкрити в умовах обмеженого часу, наприклад, стандарт шифрування США DES або ГОСТ 28147-89. Крім цього, для розкривання таких систем необхідно використовувати потужні технічні ресурси, що робить економічно невигідним випуск неліцензійних декодерів.

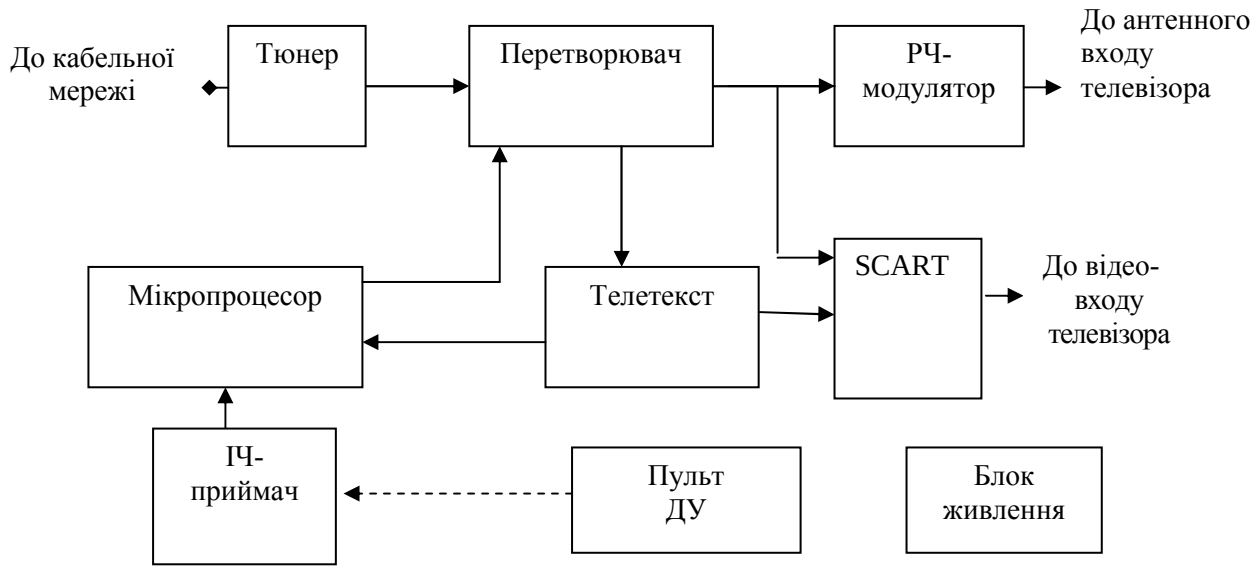

Рис. 4. Блок-схема декодера

На рис. 6 показаний один із варіантів структури такого декодера. Вхідним сигналом декодера є високочастотний (ВЧ) телевізійний сигнал. Вбудований тюнер дозволяє вибирати необхідний телеканал за допомогою пульта дистанційного керування або в дешевшому варіанті – з передньої панелі декодера. Декодер виділяє складові Y, R–Y, B–Y, які дешифруються за заданим алгоритмом, наприклад, DES або ГОСТ 28147-89. Шифрування складових яскравості та кольорових складових відеосигналу зводить до мінімуму спотворення зображення. Відновлені складові Y, R–Y, B–Y формують відновлений відеосигнал, який подається на відеовхід EURO SCART TV. Така структура за необхідності також дозволяє шифрувати звук.

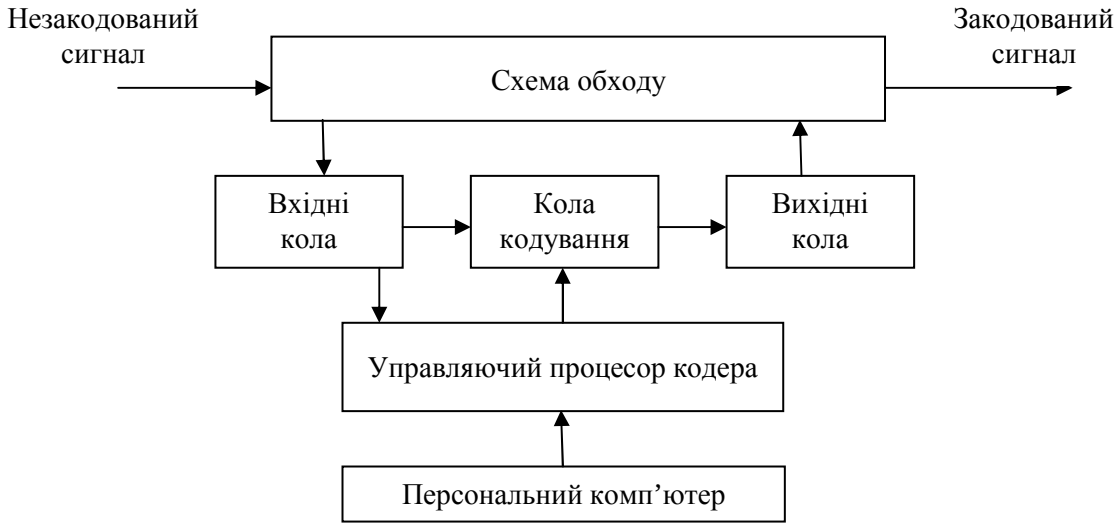

Рис. 5. Блок-схема кодера

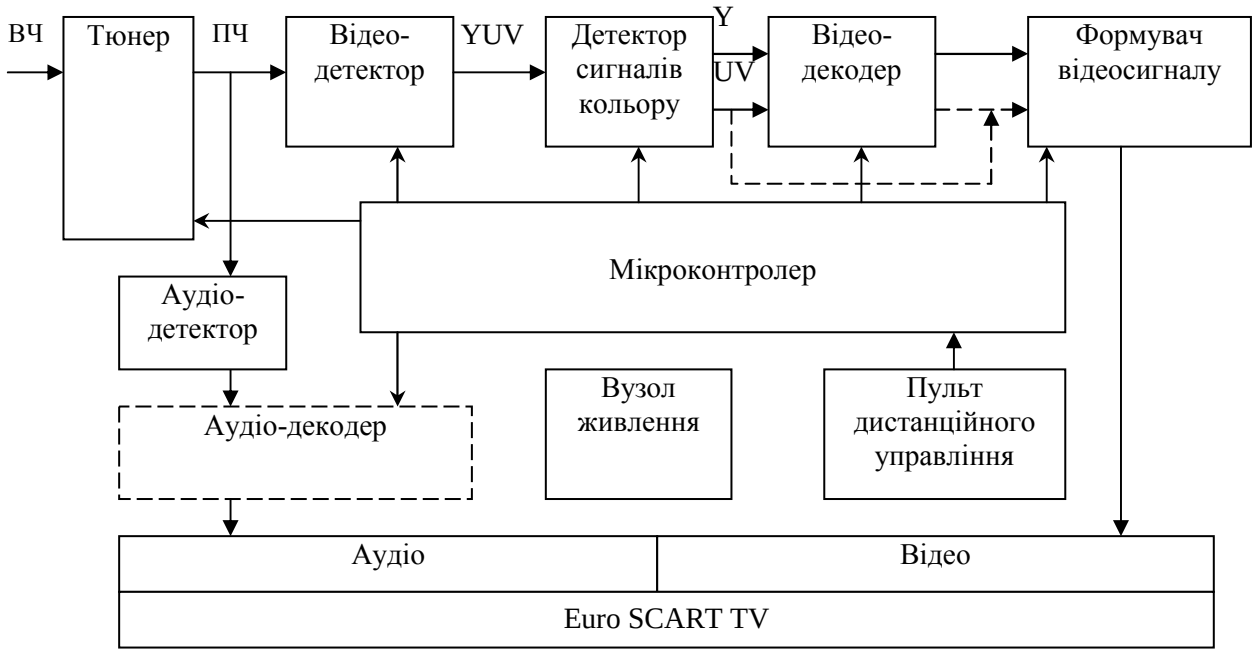

Рис. 6. Структура декодера з використанням сучасних методів цифрового шифрування

Декодер забезпечує адресну активацію повідомлень для абонента та можливість декодування окремого каналу. Адресна активація та передача ключів може здійснюватись декількома способами, наприклад, в потоці даних телетексту за окремо виділеним TV каналом, в потоці цифрових Y, R–Y, B–Y.

Використання входу по ВЧ та відеовходу EURO SCART TV дозволяє мінімізувати конструктивні зв'язки між декодером та абонентським TV.

Основні переваги описаного декодера:

- максимально високий рівень захисту при використанні алгоритмів DES або ГОСТ 28147-89;
- модульна структура, що дозволяє випускати різні варіанти для зменшення собівартості, наприклад, без дистанційного керування, без кодування звуку;
- можливість переходу на нові, більш потужні алгоритми шифрування.

Нижче описано особливості реалізації вузла Декодер Video, що входить до складу описаного декодера (рис. 6). Особливо слід підкреслити, що вузол Декодер Video повинен бути реалізований у вигляді замовленої або напівзамовленої мікросхеми (програмованої логічної інтегральної схеми – ПЛІС).

3. Забезпечення надійної передачі відеосигналу

Саме по собі цифрове закриття телевізійного каналу складностей не викликає. Існує багато стандартів закриття цифрової інформації. Наприклад, у ТзОВ "Інтрон" розроблений ряд бібліотечних елементів (ядер) ПЛІС, які реалізують функції шифрування і дешифрування кодів у стандарті DES та інших стандартах [11]. Основною проблемою цифрового закриття аналогового відеосигналу є надійна і достовірна передача закритої цифрової інформації існуючими аналоговими каналами зв'язку із завадами (рис. 7). Для забезпечення такої передачі необхідно використовувати спеціальні коди, які дозволяють виправляти на прийомному кінці каналу помилки, які можуть виникати внаслідок:

- використання аналого-цифрових і цифро-аналогових перетворювачів у каналах передачі інформації;
- завад, які діють на канали передачі.

Як правило, такі коди формуються з послідовним використанням:

- вузла ущільнення інформації;
- кодера Ріда–Соломона;
- перемішувача;
- формувача згорткового коду.

Безпомилковий код відтворюється у зворотному порядку з використанням:

- декодера згорткового коду (дешифратора Вітербі);
- перемішувача;
- декодера Ріда-Соломона;
- вузла відтворення ущільненої інформації.

Рис. 7. Функціональна схема цифрового закриття і розкриття

Оскільки формувачі згорткового коду збільшують кількість інформації, яка повинна передаватися каналами зв'язку, то це збільшення потрібно компенсувати ущільненням інформації, тобто зменшенням її кількості.

Коди Ріда–Соломона рекомендується використовувати у випадках, коли смуга пропускання каналів є обмеженою і коли потрібно виявляти невиправлені помилки. Як правило, коди Ріда–Соломона використовуються разом із згортковими кодами і декодерами Вітербі, що ілюструється функціональною схемою, наведеною на рис. 7 [6]. При цьому код Ріда–Соломона є так званим зовнішнім кодом, а згортковий код – внутрішнім. Послідовне використання двох кодів значно покращує можливість виявлення і виправлення помилок, які виникають під час передачі інформації каналами зв'язку.

Код Ріда–Соломона часто використовують з характеристиками, наведеними у табл.1.

Таблиця 1

Характеристики коду Ріда–Соломона

Параметр	Позначення	Величина
Розрядність символу	J	8
Глибина перемішування коду (interleaving)	I	1, 2, 3, 4 і 5.
Кількість символів у кодовому слові	$n = 2^J - 1$	255
Кількість контрольних символів коду	2E	16 або 32
Кількість інформаційних символів коду	$k = n-2E$	239 або 223
Коректуюча здатність коду (255,239)	E	8 символів
Коректуюча здатність коду (255,223)	E	16 символів
Поліном, що утворює поле GF(2).	$F(x) = x^8 + x^7 + x^2 + x + 1$	
Поліном, що утворює код у полі $GF(2^J)= GF(2^8)$, де $F(\alpha) = 0$.	$g(x) = \prod_{j=128-E}^{127+E} (x - \alpha^{11j})$	
Примітивний елемент поля $GF(2^8)$,	α^{11}	

Функціональна схема, яка пояснює формування символів коду Ріда–Соломона c(x) з інформаційних символів a(x), наведена на рис. 8, де прийнято $g_i = G_i$ у табл. 1.

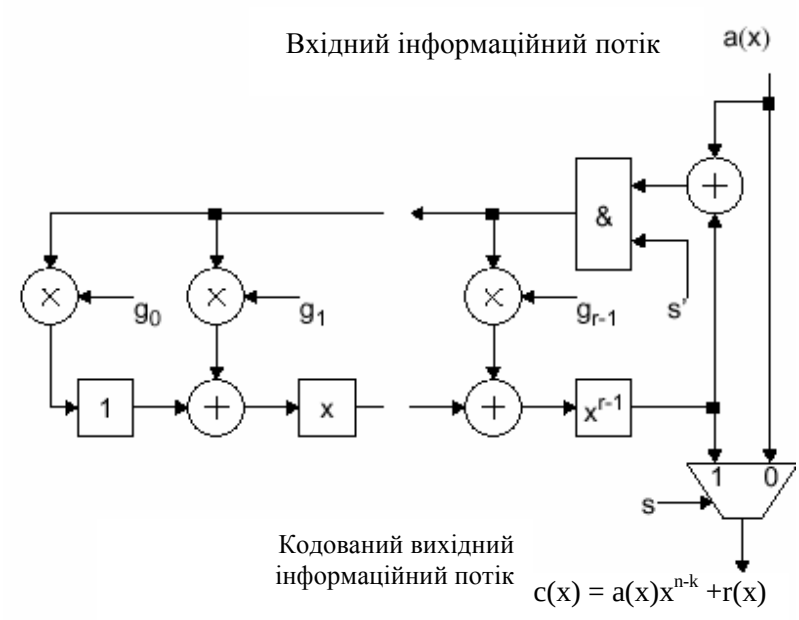

Рис. 8. Формувач коду Ріда–Соломона

Значення множників g_i (G_i) для коду (255,223) наведені у табл. 2, а для коду (255,239) – у табл. 3.

Таблиця 2

Значення множників g_i (G_i) для E=16

	α^7	α^6	α^5	α^4	α^3	α^2	α^1	α^0
$G_0=G_{32}=\alpha^0$	0	0	0	0	0	0	0	1
$G_1=G_{31}=\alpha^{249}$	0	1	0	1	1	0	1	1
$G_2=G_{30}=\alpha^{59}$	0	1	1	1	1	1	1	1
$G_3=G_{29}=\alpha^{66}$	0	1	0	1	0	1	1	0
$G_4=G_{28}=\alpha^4$	0	0	0	1	0	0	0	0
$G_5=G_{27}=\alpha^{43}$	0	0	0	1	1	1	1	0
$G_6=G_{26}=\alpha^{126}$	0	0	0	0	1	1	0	1
$G_7=G_{25}=\alpha^{251}$	1	1	1	0	1	0	1	1
$G_8=G_{24}=\alpha^{97}$	0	1	1	0	0	0	0	1
$G_9=G_{23}=\alpha^{30}$	1	0	1	0	0	1	0	1
$G_{10}=G_{22}=\alpha^3$	0	0	0	0	1	0	0	0
$G_{11}=G_{21}=\alpha^{213}$	0	0	1	0	1	0	1	0
$G_{12}=G_{20}=\alpha^{50}$	0	0	1	1	0	1	1	0
$G_{13}=G_{19}=\alpha^{66}$	0	1	0	1	0	1	1	0
$G_{14}=G_{18}=\alpha^{170}$	1	0	1	0	1	0	1	1
$G_{15}=G_{17}=\alpha^5$	0	0	1	0	0	0	0	0
$G_{16}=\alpha^{24}$	0	1	1	1	0	0	0	1

Перемішування коду ілюструється рис. 9, звідки видно, що перший формувач коду Ріда–Соломона (R–S Encoder #1) виробляє контрольні символи для інформаційних символів 1, J+1, 2J+1 і т.д., другий – для символів 2, J+2, 2J+2 і т.д., а останній – для інформаційних символів J, 2J, 3J і т.д. Процес перемішування дозволяє уникнути групових помилок у послідовності інформаційних символів.

Таблиця 3

Значення множників g_i (G_i) для E=8

	α^7	α^6	α^5	α^4	α^3	α^2	α^1	α^0
$G_0=G_{16}=\alpha^0$	0	0	0	0	0	0	0	1
$G_1=G_{15}=\alpha^{30}$	1	0	1	0	0	1	0	1
$G_2=G_{14}=\alpha^{230}$	0	1	1	0	1	0	0	1
$G_3=G_{13}=\alpha^{49}$	0	0	0	1	1	0	1	1
$G_4=G_{12}=\alpha^{235}$	1	0	0	1	1	1	1	1
$G_5=G_{11}=\alpha^{129}$	0	1	1	0	1	0	0	0
$G_6=G_{10}=\alpha^{81}$	1	0	0	1	1	0	0	0
$G_7=G_9=\alpha^{76}$	0	1	1	0	0	1	0	1
$G_8=\alpha^{173}$	0	1	0	0	1	0	1	0

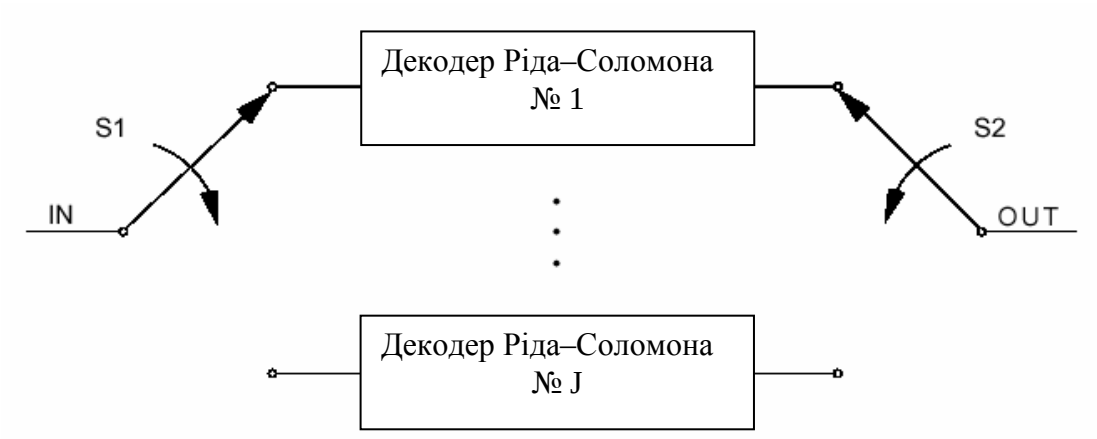

Рис. 9. Перемішування кодів

Для покращання характеристик каналів передачі інформації бажано мати мінімальну частотну смугу, яку займає сигнал. Для цього доцільно передавати корисну інформацію із замішаним у неї шумоподібним сигналом [7]. Функціональна схема замішування сигналу наведена на рис. 10.

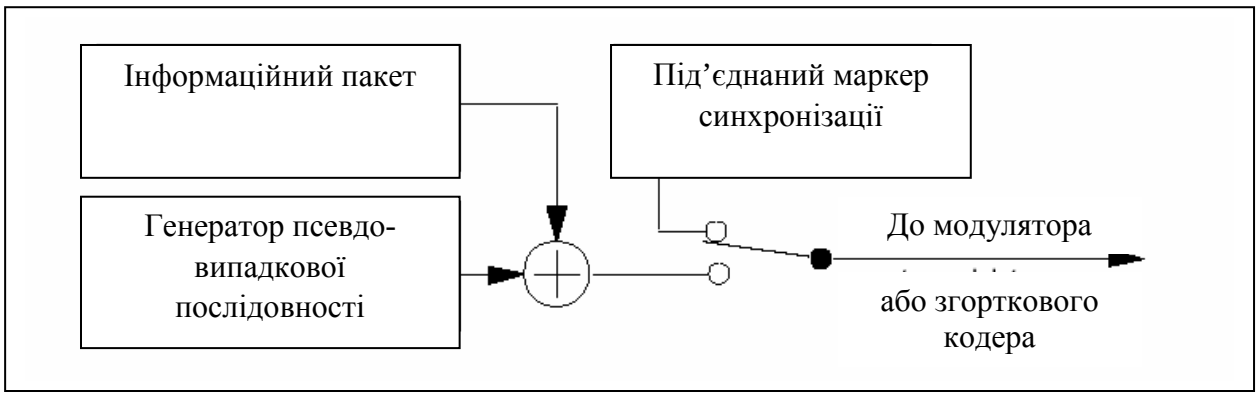

Рис. 10. Замішування із шумоподібним сигналом

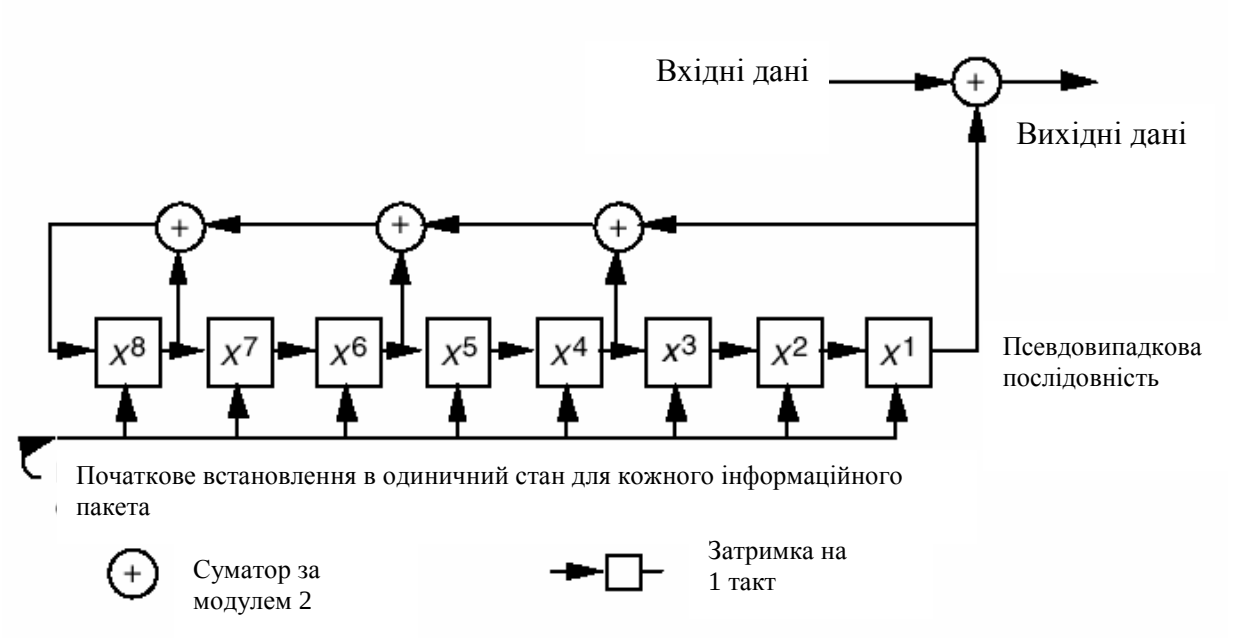

Рис. 11. Генератор псевдовипадкового коду

Псевдовипадковий сигнал генерується за схемою, наведеною на рис. 11, з використанням полінома $h(x) = x^8 + x^7 + x^5 + x^3 + 1$.

Приймачі та передавачі коду Ріда–Соломона реалізуються з використанням відповідних ядер фірми Xilinx [8,9]. При реалізації на ПЛІС Virtex коду (255,223) ці вузли мають характеристики, наведені у табл. 4.

Таблиця 4

Характеристики приймачів і передавачів коду Ріда–Соломона

Параметр	Приймач	Передавач
Тривалість обробки, символів	660	
Початкова затримка, символів	921	3
Апаратні витрати, Slices	1012	167
Максимальна тактова частота, МГц	55	102

У рекомендаціях, наведених у роботі [7], запропоновано декілька схем кодування інформації в каналах передачі. Рекомендується використовувати згортковий код із пропорцією згортки 1/2, що у деяких випадках може бути достатнім. Функціональна схема, яка пояснює утворення такого коду, наведена на рис. 12.

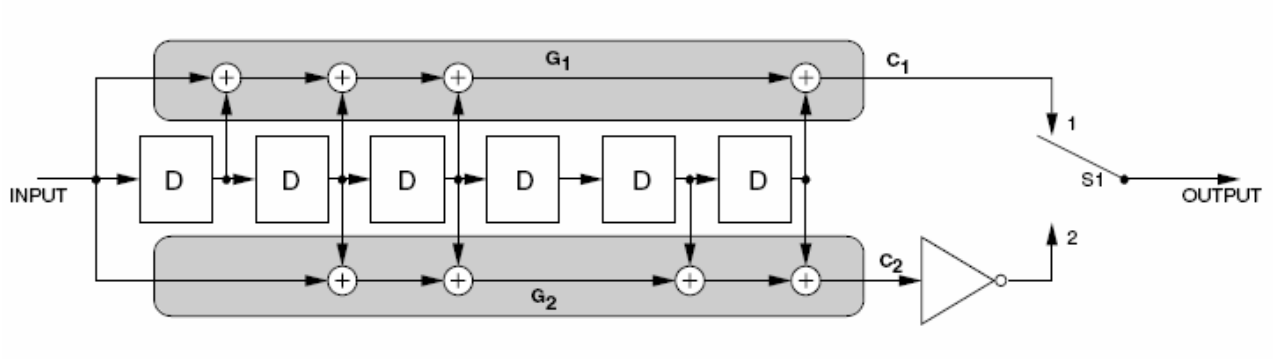

Рис. 12. Формувач згорткового коду

Там, де не можуть бути використані канали із широкою смугою пропускання, рекомендується використовувати згорткові коди з проріджанням. Функціональна схема, яка пояснює утворення такого коду, наведена на рис. 13.

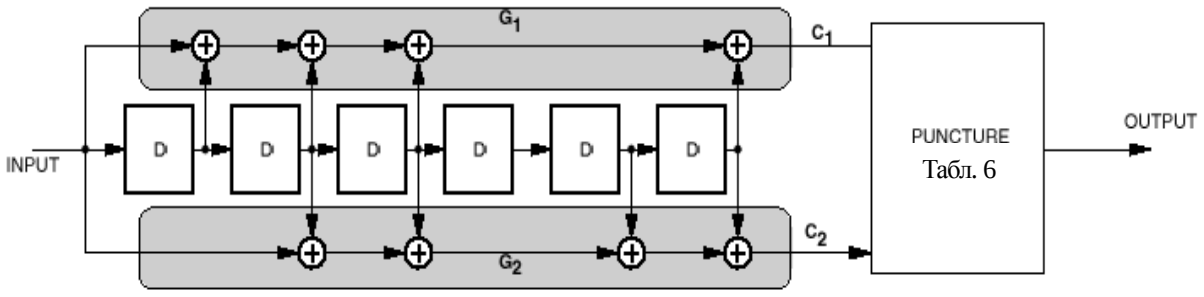

Рис. 13. Формувач згорткового коду з проріджанням

Основну специфікацію для згорткового коду наведено у табл. 5.

Таблиця 5

Специфікація для згорткового коду

Характеристика	Значення
Тип згортки	З декодування за максимальною подібністю (декодер Вітербі)
Пропорція згортки без проріджения	½
Пропорція згортки з проріджением	2/3, 3/4, 5/6, 7/8
Довжина вхідного коду	7 біт
Вектор зв`язку G1	$1111001_2 = 171_8$
Вектор зв`язку G2	$1011011_2 = 133_8$
Інверсія символу	На виході G2
Вихідна послідовність	$C_1(1), -C_2(1), C_1(2), -C_2(2)...$

Вихідні послідовності при різних варіантах проріджения згортки наведені у табл. 6.

Таблиця 6

Вихідні послідовності

Послідовність сигналів проріджения (1 – символ передається, 0 – символ не передається)	Пропорція згортки	Вихідна послідовність сигналів у моменти часу t: $C_1(t), -C_2(t),$
C_1: 1 0 C_2: 1 1	2/3	$C_1(1), -C_2(1), -C_2(2)...$
C_1: 1 0 1 C_2: 1 1 0	3/4	$C_1(1), -C_2(1), -C_2(2), C_1(3)...$
C_1: 1 0 1 0 1 C_2: 1 1 0 1 0	5/6	$C_1(1), -C_2(1), -C_2(2), C_1(3), -C_2(4), C_1(5)...$
C_1: 1 0 0 0 1 0 1 C_2: 1 1 1 1 0 1 0	7/8	$C_1(1), -C_2(1), -C_2(2), -C_2(3), -C_2(4), C_1(5), -C_2(6), C_1(7)...$

Ідея використання дешифратора Вітербі така (рис. 14).

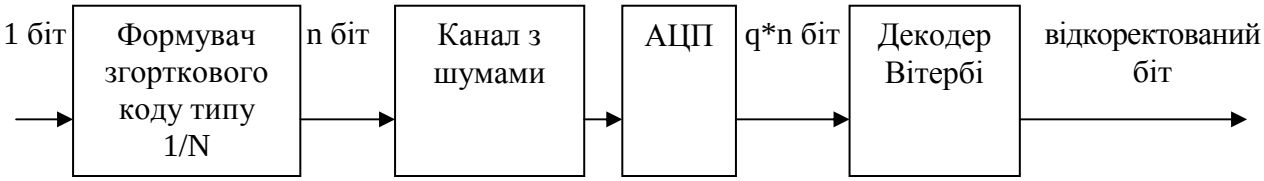

Рис. 14. Використання декодера Вітербі

Один біт інформації, який треба передати каналами зв’язку з завадами, за допомогою схеми згортки (1/N Convolutional Encoder) перетворюється на N біт, які передаються каналом. Приймач сприймає цифровий сигнал як аналоговий і за допомогою АЦП перетворює його у цифровий вигляд. Декодер Вітербі (Viterbi Decoder) відтворює найбільш імовірне значення інформаційного біта. Декодер Вітербі може бути реалізований на ПЛІС Virtex [10] із такими характеристиками: апаратні витрати – 241 Slice, тактова частота – до 63 МГц.

Висновки

1. Аналіз систем засекречування телевізійного сигналу дозволив поділити їх на 3 основні групи: аналогові; цифро-аналогові; цифрові.

2. Аналогова система умовного доступу не є надійно захищеною, й існує висока ймовірність її зламу.

3. Цифрова частина цифро-аналогової системи умовного доступу може бути надійно захищеною від зламу, але аналогове спотворення відеосигналу недостатнє для повного спотворення зображення на екрані телевізора і містить непрямі ознаки, які дозволяють здійснити несанкціоноване розкриття інформації.

4. Найбільш захищеною і надійною є цифрова система умовного доступу. Така система буде надійно захищеною від зламу і буде забезпечувати повне спотворення як відеозображення на екрані телевізора, так і його звукового супроводу.

5. Існують суттєві наробки у частині основних вузлів цифрової системи умовного доступу – ядер шифрування та дешифрування, перетворення кодів кольорового зображення та інших.

6. Цифрова система умовного доступу є цікавою з точки зору перспектив її продажу як в Україні, так і за кордоном. Цифрова система умовного доступу має найбільші перспективи розвитку в плані виконуваних функцій та здешевлення.

7. Основною проблемою цифрового закриття аналогового відеосигналу є надійна і достовірна передача закритої цифрової інформації існуючими аналоговими каналами зв'язку із завадами. Для забезпечення такої передачі необхідно використовувати спеціальні коди, які дозволяють виправляти на прийомному кінці каналу помилки. Коди Ріда–Соломона доцільно використовувати у випадках, коли смуга пропускання каналів є обмеженою, і коли потрібно виявляти присутність невиправлених помилок. Як правило, коди Ріда–Соломона використовуються разом із згортковими кодерами і декодерами Вітербі. Послідовне використання двох кодів значно покращує можливість виявлення і виправлення помилок, які виникають під час передачі інформації каналами зв'язку.

1. Цифровое телевидение / Под ред. М.И. Кривошеева. – М.: Связь, 1980. 2. Птачек М. Цифровое телевидение. Теория и техника / Пер. с чешск; Под ред. Л.С.Виленчика. – М.: Радио и связь, 1990. 3. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. 4. Баричев С., Серов Р.. Основы современной криптографии. – М.: Горячая линия – Телеком, 2001. 5. Виноградов В. Уроки телемастера: Учебно-справочное пособие. – СПб.: Корона Принт, Лань, 1997. – 416 с. ил. 6. The Reed-Solomon Solution – Customer Tutorial. Xilinx at Work in Hot New Technologies. February 2000. 7. RECOMMENDATION FOR SPACE. DATA SYSTEM STANDARDS. TELEMETRY CHANNEL CODING. CCSDS 101.0-B-5. BLUE BOOK. June 2001. 8. January 12, 2000. Reed-Solomon Encoder. Product Specification Xilinx Inc. URL: www.support.xilinx.com/support/techsup/tappinfo.htm 9. January 12, 2000. Reed-Solomon Decoder. Product Specification Xilinx Inc. URL: www.support.xilinx.com/support/techsup/tappinfo.htm 10. Soft-Decision Viterbi Decoder. Product Specification. CAST, Inc. April 19, 1999. URL: www.cast-inc.com 11. www.intron.lviv.ua.