DOI: 10.18372/2410-7840.18.11093
УДК 621.391:519.2

НЕАСИМПТОТИЧНІ ОЦІНКИ ЙМОВІРНОСТІ ПРАВИЛЬНОГО ВІДНОВЛЕННЯ ПОВІДОМЛЕНЬ У ДВІЙКОВОМУ ВІДВІДНОМУ КАНАЛІ ЗІ СТИРАННЯМ

Антон Олексійчук, Юрій Сергієнко

Досліджується система передачі інформації, яка складається з безнадлишкового джерела двійкових повідомлень, ідеального основного каналу між відправником та законним отримувачем та відвідного каналу зі стиранням між відправником та супротивником. Для надійного захисту інформації у відвідному каналі використовується відомий метод випадкового кодування повідомлень двійковими лінійними кодами. У статті отримано точний вираз та неасимптотичні оцінки параметра, що характеризує практичну стійкість зазначених систем: ймовірності правильного відновлення повідомлень у відвідному каналі. Отримані оцінки є застосовними до широкого класу двійкових лінійних кодів з відомими значеннями довжини, вимірності та мінімальної (або дуальної) відстані. Вони дозволяють сформулювати критерії вибору кодів для побудови практично стійких та ефективних систем з випадковим кодуванням у двійковому каналі зі стиранням, а також встановити достатню умову асимптотичної досконалості таких систем. Отримані результати можуть бути використані у криптографічних застосуваннях, що базуються на використанні моделі каналу зв'язку з відводом.

Ключові слова: *криптографічний захист інформації, канал зв'язку з відводом, канал зі стиранням, випадкове кодування, ймовірність правильного відновлення повідомлень, обґрунтована стійкість.*

Вступ

Концепція відвідного каналу, що базується на теоретико-інформаційній моделі системи передачі дискретних повідомлень каналом зв'язку з відводом (wire-tap channel), вперше запропонована в [9] і отримала помітний розвиток протягом останніх десятиріч. На даний час ця концепція охоплює широке коло теоретичних і прикладних задач в галузі захисту інформації, складаючи наукову основу для створення теоретично стійких криптосистем і протоколів, які не вимагають розподілу ключів захищеними каналами зв'язку, квантово-криптографічних протоколів відкритого розподілу ключів, безумовно стійких схем розділення секрету, алгоритмічних методів захисту інформації від витоку побічними каналами тощо (відзначимо роботи [2, 6, 8], де наведено огляд публікацій та зазначено подальші застосування концепції відвідного каналу).

Традиційний метод безпечної передачі дискретних повідомлень каналом зв'язку з відводом полягає у застосуванні випадкового кодування, за яким для передачі довільного повідомлення s, що вироблено джерелом, використовується дискретний сигнал x, який вибирається випадкового та рівноймовірно з заданої множини сигналів. Як показано в [9], у випадку, коли основний канал зв'язку між відправником та законним отримувачем інформації є «менш шумним» в порівнянні з відвідним, метод випадкового кодування дозволяє забезпечити як завгодно близьку до досконалої стійкість захисту достатньо довгих повідомлень у відводі за умови, що швидкість передачі інформації обмежена зверху певною величиною, як залежить тільки від розподілів ймовірностей спотворень в каналах, – так званою секретною пропускною здатністю системи, що розглядається.

Зауважимо, що основні результати [9] отримані неконструктивним шляхом (методом випадкового вибору лінійних кодів) та є асимптотичними (справедливими лише для достатньо довгих повідомлень джерела). При цьому, не дивлячись на помітний прогрес у дослідженні окремих видів систем з випадковим кодуванням, переважно, з основним каналом без спотворень та двійковим симетричним відвідним каналом (див. публікації, наведені в [2, 6, 8]), задача конструктивного синтезу кодів для таких систем, що володіють зазначеними вище властивостями, залишається у загальному випадку не вирішеною. Відзначимо роботу [8], де побудовані послідовності лінійних кодів з потрібними властивостями для випадку, коли основний канал зв'язку є ідеальним (не має спотворень), а відвідний є двійковим каналом зі стиранням (ДКС). Дослідженню асимптотичної поведінки параметра, що характеризує теоретичну стійкість захисту інформації у відвідному каналі зі стиранням, присвячена робота [7] (відзначимо, що в [7] та [8] використовуються різні моделі каналів). Результати робіт [7, 8] мають асимптотичний характер та не надають можливості оцінювати практичну стійкість систем з випадковим

кодуванням в ДКС, що побудовані на основі довільних двійкових лінійних кодів фіксованої довжини.

Метою даної статті є отриманя точного виразу та неасимптотичних оцінкок параметра, що характеризує практичну стійкість систем з лінійним випадковим кодуванням у ДКС: ймовірності правильного відновлення повідомлень у відвідному каналі. На відміну від результатів попередніх робіт [7, 8], отримані оцінки є неасимптотичними та можуть бути застосовані для усіх двійкових лінійних кодів фіксованої довжини з відомими вимірністю та мінімальною (чи дуальною) відстанню. Вони дозволяють сформулювати критерії вибору кодів для побудови практично стійких та ефективних систем з випадковим кодуванням у ДКС, а також встановити достатню умову асимптотичної досконалості таких систем. В подальшому отримані результати пропонується використати для оцінювання ефективності запропонованого в [3] способу запису інформації на магнітні носії.

1. Постановка задачі.

Нагадаємо [8], що двійковий канал зі стиранням визначається як дискретний канал без пам'яті з вхідним алфавітом $\{0,1\}$, вихідним алфавітом $\{0,1,*\}$ та перехідними ймовірностями, зазначеними на рис. 1. При передачі таким каналом зв'язку символ 0 або 1 не змінюється з ймовірністю $p \in (0,1)$ та стирається (тобто переходить у $*$) з ймовірністю $1-p$.

Розглянемо систему передачі інформації з випадковим кодуванням, побудовану на основі двійкового лінійного $(n, n-k)$-коду G з мінімальною відстанню d та дуальною відстанню d' (рис. 2). За означенням джерело виробляє випадкові рівноймовірні двійкові вектори довжини k. Для захисту повідомлень у відвідному каналі використовується випадкове кодування повідомлень кодом G (див., наприклад, [8]). Для цього спочатку визначається певна (загальновідома) взаємно однозначна відповідність між двійковими векторами довжини k та суміжними класами (СК) коду G. Потім для передачі довільного повідомлення S використовується вектор X, який вибирається випадково та рівноймовірно в СК, що відповідає повідомленню S. Якщо основний канал між відправником та законним отримувачем інформації є ідеальним, то отримувач швидко знайде повідомлення S за вектором X. При цьому супротивник, спостерігаючи на виході відвідного каналу спотворений варіант Y повідомлення X, буде вимушений відновлювати S за Y за допомогою певної статистичної процедури.

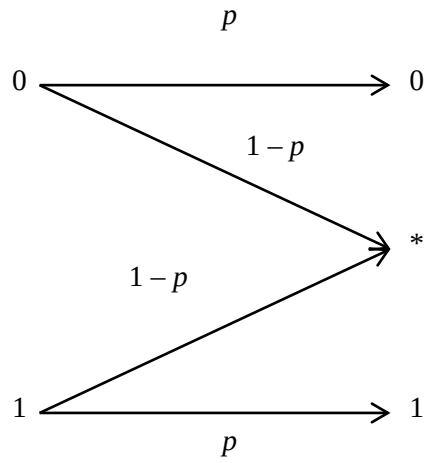

Рис. 1. Двійковий канал зі стиранням

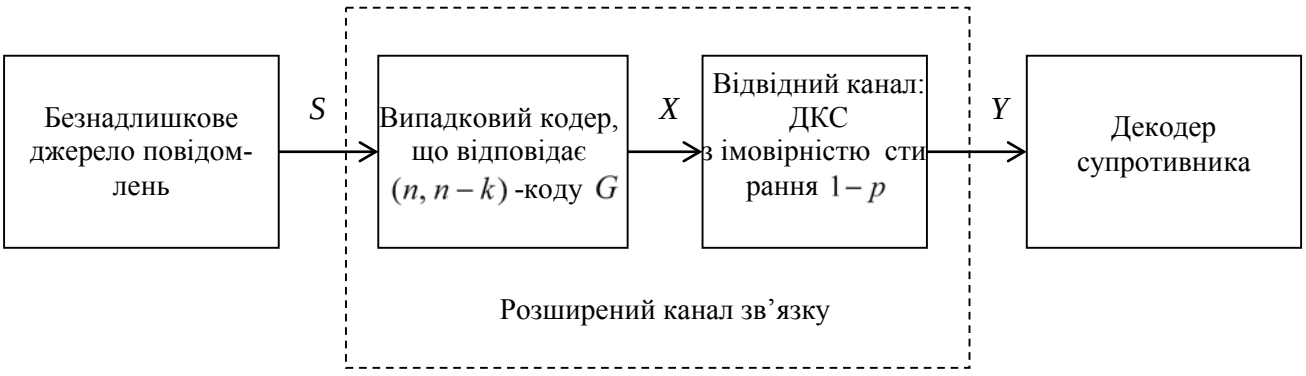

Рис. 2. Система з випадковим кодуванням у відвідному каналі зі стиранням

Позначимо $p(G)$ ймовірність правильного відновлення повідомлень в розширеному каналі зв'язку, що утворений шляхом послідовного з'єднання випадкового кодера та ДКС. Треба описати процедуру оптимального відновлення повідомлень та отримати оцінки ймовірності $p(G)$.

2. Основні результати

Введемо низку допоміжних позначень. Для будь-якого $y=(y_1,\dots,y_n)\in\{0,1,*\}^n$ позначимо $S_y=\{i\in\overline{1,n}\mid y_i=*\}$, $s_y=\#S_y$ (потужність множини S_y), $A(y)=\{x\in V_n\mid \forall i\notin S_y:\ x_i=y_i\}$ (тут і далі V_m позначає множину двійкових векторів довжини m, $m=1,2,\dots$). Слідуючи [4], назвемо слова з множини $A(y)$ сумісними зі словом y. Помітимо, що згідно з означенням ДКС, ймовірність переходу слова $x\in V_n$ в слово $y\in\{0,1,*\}^n$ при передачі каналом зі стиранням визначається за формулою

$$p(y/x)=p^{n-s_y}(1-p)^{s_y}\ ,\text{ якщо } x\in A(y);$$
$$p(y/x)=0\ -\text{ у протилежному випадку.} \quad (1)$$

Нехай $s\in V_k$ є довільним повідомленням, що виробляється безнадлишковим джерелом, G_s є суміжним класом коду G, який відповідає повідомленню s. Назвемо повідомлення s та СК G_s сумісними зі словом $y\in\{0,1,*\}^n$, якщо $G_s\cap A(y)\neq\varnothing$. Зауважимо, що елементи множини $G_s\cap A(y)$ і тільки вони є словами, що належать множині G_s, з яких слово y може бути отримано на виході ДКС.

Позначимо H перевірочну матрицю (розміру $k\times n$) коду G; для будь-якого $A\subseteq\overline{1,n}$ позначимо H_A підматрицю матриці H, яка міститься в її стовпцях з номерами із множини A, покладемо $r(A)=\operatorname{rank}H_A$. У випадку $A=S_y$, де $y\in\{0,1,*\}^n$, будемо писати r_y замість $r(S_y)$. Нарешті, для будь-якого $l\in\overline{0,n}$ покладемо

$$\rho_l=\binom{n}{l}^{-1}\sum_{\substack{A\subseteq\overline{1,n}:\\ \#A=l}}2^{-r(A)}. \quad (2)$$

Лема 1. Для будь-якого $y\in\{0,1,*\}^n$ існує точно 2^{r_y} СК коду G, сумісних зі словом y. Кожен такий СК містить $2^{s_y-r_y}$ слів, сумісних з y.

Доведення. Нехай $s\in V_k$ і $G_s\cap A(y)\neq\varnothing$. Тоді для будь-якого $x\in G_s\cap A(y)$ виконується рівність

$$G_s\cap A(y)=\{x+z\colon z\in G,\ \operatorname{supp}(z)\subseteq S_y\}, \quad (3)$$

де $\operatorname{supp}(z)$ – носій (множина номерів ненульових координат) слова z. З формули (3) випливає, що елементи множини $G_s\cap A(y)$ знаходяться у взаємно однозначній відповідності зі словами коду G, носії яких містяться в S_y. У свою чергу, ці слова взаємно однозначно відповідають розв'язкам системи лінійних рівнянь $H_{S_y}x^T=0$, кількість яких дорівнює $2^{s_y-r_y}$.

Отже, кожен СК G_s, сумісний зі словом y, містить точно $2^{s_y-r_y}$ слів, сумісних з y. Оскільки загальне число слів у множині $A(y)$ дорівнює 2^{s_y}, то кількість СК, сумісних зі словом y, дорівнює 2^{r_y}. Лему доведено.

Наступна лема доводиться аналогічно лемі 4.1 в [7].

Лема 2. Для чисел (2) справедливі такі співвідношення:

$$\rho_l=2^{-l},\ l\in\overline{0,d-1}, \quad (4)$$
$$\rho_l=2^{-k},\ l\in\overline{n-d'+1,n}, \quad (5)$$
$$2^{-\min\{k,\,l\}}\le\rho_l\le2^{-(d-1)},\ l\in\overline{d,n-d'}. \quad (6)$$

Позначимо $p(y/s)$ ймовірність переходу повідомлення $s\in V_k$, виробленого джерелом, у повідомлення $y\in\{0,1,*\}^n$ на виході розширеного каналу системи з випадковим кодуванням, що розглядається. Справедливі співвідношення

$$p(y/s)=2^{k-n}\,2^{s_y-r_y}\,p^{n-s_y}(1-p)^{s_y},\ \text{якщо}$$
$$G_s\cap A(y)\neq\varnothing;\ p(y/s)=0,\ \text{якщо} \quad (7)$$
$$G_s\cap A(y)=\varnothing.$$

Дійсно, якщо СК G_s є сумісним зі словом y, то згідно з лемою 1 існує точно $2^{s_y-r_y}$ слів $x\in G_s$, сумісних зі словом y. При випадковому кодуванні кожне з цих слів вибирається з множини G_s з ймовірністю 2^{k-n} та переходить в y з ймовірністю (1). Звідси випливає справедливість рівностей (7).

Позначимо $\delta^*\colon\{0,1,*\}^n\to V_k$ оптимальну процедуру відновлення (оптимальний декодер) повідомлень у розширеному каналі системи з ви-

падковим кодуванням, що розглядається. Нагадаємо (див., наприклад, [2]), що ця процедура полягає в знаходженні для кожного слова $y \in \{0,1,*\}^n$ такого повідомлення $s^* \in V_k$, для якого досягається максимум ймовірностей (7) за всіма $s \in V_k$. Оскільки зазначені ймовірності є однаковими для усіх s, сумісних з y, то процедура δ^* полягає у випадковому рівноймовірному виборі повідомлення s^* серед усіх 2^{r_y} повідомлень, сумісних зі словом y. Зокрема, для будь-яких фіксованих $s \in V_k$, $y \in \{0,1,*\}^n$ ймовірність правильного відновлення слова y за умови, що s було передано, а y – отримано на виході ДКС, дорівнює

$$\pi^*(s;y) = 2^{-r_y}, \text{ якщо } G_s \cap A(y) \neq \varnothing;\ \pi^*(s;y) = 0, \text{ якщо } G_s \cap A(y) = \varnothing. \quad (8)$$

Наступне твердження встановлює явний вираз, а також оцінки ймовірності $p(G) = \mathbf{P}\{\delta^*(Y) = S\}$.

Твердження 1. Справедливі співвідношення

$$p(G) = \sum_{l=0}^{n} \rho_l\ p_{n,l}, \quad (9)$$

$$\sum_{l=0}^{d-1} 2^{-l}\, p_{n,l} + \sum_{l=d}^{n-d'} 2^{-\min\{k,\,l\}}\, p_{n,l} + \sum_{l=n-d'+1}^{n} 2^{-k}\, p_{n,l} \le p(G) \le$$

$$\le \sum_{l=0}^{d-1} 2^{-l}\, p_{n,l} + \sum_{l=d}^{n-d'} 2^{-(d-1)}\, p_{n,l} + \sum_{l=n-d'+1}^{n} 2^{-k}\, p_{n,l}, \quad (10)$$

де числа ρ_l визначаються за формулою (2), а

$$p_{n,l} = \binom{n}{l} (1-p)^l\, p^{n-l},\ \ l \in \overline{0,n}.$$

Доведення. Переконаємося у справедливості формули (9). Згідно з означенням ймовірності $p(G)$, виконуються рівності

$$p(G) = 2^{-k} \sum_{s \in V_k} \mathbf{P}\{\delta^*(Y) = S \mid S = s\} = 2^{-k} \sum_{s \in V_k} \sum_{\substack{y \in \{0,1,*\}^n: \\ A(y) \cap G_s \neq \varnothing}} p(y/s)\, \pi^*(s;y).$$

Звідси, використовуючи формули (7), (8), отримаємо, що

$$p(G) = \sum_{s \in V_k} \sum_{\substack{y \in \{0,1,*\}^n: \\ A(y) \cap G_s \neq \varnothing}} 2^{-2r_y} (2^{-1}p)^{n-s_y} (1-p)^{s_y} = \sum_{\substack{y \in \{0,1,*\}^n: \\ A(y) \cap G_s \neq \varnothing}} 2^{-2r_y} (2^{-1}p)^{n-s_y} (1-p)^{s_y}, \quad (11)$$

де останнє співвідношення випливає з того факту, що для будь-якого $y \in \{0,1,*\}^n$ існує точно 2^{r_y} повідомлень $s \in V_k$ з властивістю $A(y) \cap G_s \neq \varnothing$ (см. лему 1). Далі, на підставі формули (11) отримаємо, що

$$p(G) = \sum_{l=0}^{n} (1-p)^l (2^{-1}p)^{n-l} \sum_{\substack{y \in \{0,1,*\}^n: \\ s_y = l}} 2^{-r_y} = \sum_{l=0}^{n} (1-p)^l (2^{-1}p)^{n-l} \sum_{\substack{A \subseteq \overline{1,n}: \\ \#A = l}} 2^{-r(A)} \#\{y \in \{0,1,*\}^n \mid S_y = A\} =$$

$$= \sum_{l=0}^{n} (1-p)^l (2^{-1}p)^{n-l} 2^{n-l} \sum_{\substack{A \subseteq \overline{1,n}: \\ \#A = l}} 2^{-r(A)} = \sum_{l=0}^{n} \rho_l \binom{n}{l} (1-p)^l\, p^{n-l}.$$

Отже, рівність (9) доведено. Нерівності (10) випливають безпосередньо з формули (9) та співвідношень (4) – (6). Твердження доведено.

Отримаємо більш просту верхню оцінку ймовірності $p(G)$, що є справедливою за додаткових обмежень щодо параметрів коду G. Нагадаємо [8], що секретна пропускна здатність $C_{\text{секр}}$ системи з випадковим кодуванням, що розглядається, дорівнює $1-p$. Припустимо зараз, що

$$(n-d')n^{-1} < 1-p. \quad (12)$$

Зауважимо, що згідно з межею Сінглтона, дуальна відстань будь-якого двійкового $(n, n-k)$-коду G задовольняє нерівності $d' \le n-k$ [5],

звідки випливає, що за умови (12) швидкість передачі інформації в системі з випадковим кодуванням кодом G є менше величини $C_{\text{секр}}$. Використовуючи оцінки (10), (12), отримаємо, що

$$p(G) \le \sum_{l=0}^{d-1} 2^{-l} p_{n,l} + \sum_{l=d}^{n-d'} 2^{-(d-1)} p_{n,l} + \sum_{l=n-d'+1}^{n} 2^{-k} p_{n,l} \le 2^{-k} + \sum_{l=0}^{n-d'} p_{n,l}, \quad (13)$$

звідки на підставі нерівності Чернова [4] випливає таке співвідношення:

$$p(G) \le 2^{-k} + \exp\left\{-2n\left(\frac{d'}{n} - p\right)^2\right\}. \quad (14)$$

Нагадаємо [1, 8], що послідовність кодів $G_{n,n-k}$ з параметрами $(n, n-k)$ називається асимптотично досконалою, якщо виконується рівність $p(G_{n,n-k}) = 2^{-k}(1+o(1))$, $k, n \to \infty$.

Отже, на підставі нерівності (14) справедливе таке твердження.

Твердження 2. Нехай R, δ' є дійсними числами, і $G_{n,n-k}$ є $(n, n-k)$-кодом з дуальною відстанню $d' = d'(n,k)$ такою, що $k/n \le R < \frac{2}{\ln 2}(\delta' - p)^2$, $d'/n \ge \delta' > p$. Тоді послідовність кодів $G_{n,n-k}$ є асимптотично досконалою.

В табл.1 наведені чисельні значення параметра $\theta_G(p) = \sum_{l=0}^{n-d'} p_{n,l}$, розраховані для двох лінійних кодів G. Як видно з таблиці та формули (13), для достатньо великої ймовірності стирання $(1-p \ge 0{,}8)$ та малої швидкості передачі $(kn^{-1} \le 0{,}2)$ ймовірність правильного відновлення повідомлень у відвідному каналі є близькою до ймовірності їх відгадування 2^{-k}.

Таблиця 1

Результати застосування аналітичної оцінки (13)

Параметри коду G	$n = 256$, $k = 53$, $d' = 84$, $kn^{-1} = 0{,}2070$				
Ймовірність p	0,1	0,12	0,15	0,17	0,20
Значення $\theta_G(p)$	$2{,}11 \cdot 10^{-23}$	$2{,}11 \cdot 10^{-18}$	$8{,}42 \cdot 10^{-13}$	$5{,}65 \cdot 10^{-10}$	$1{,}00 \cdot 10^{-6}$
Ймовірність p	0,25	0,30	0,35	0,40	0,45
Значення $\theta_G(p)$	$3{,}04 \cdot 10^{-3}$	$1{,}80 \cdot 10^{-1}$	$8{,}87 \cdot 10^{-1}$	$9{,}92 \cdot 10^{-1}$	$9{,}97 \cdot 10^{-1}$
Параметри коду G	$n = 256$, $k = 27$, $d' = 106$, $kn^{-1} = 0{,}1054$				
Ймовірність p	0,1	0,12	0,15	0,17	0,20
Значення $\theta_G(p)$	$2{,}11 \cdot 10^{-39}$	$1{,}88 \cdot 10^{-32}$	$2{,}08 \cdot 10^{-24}$	$3{,}57 \cdot 10^{-20}$	$4{,}74 \cdot 10^{-15}$
Ймовірність p	0,25	0,30	0,35	0,40	0,45
Значення $\theta_G(p)$	$6{,}71 \cdot 10^{-9}$	$6{,}95 \cdot 10^{-5}$	$1{,}95 \cdot 10^{-2}$	$3{,}45 \cdot 10^{-1}$	$8{,}89 \cdot 10^{-1}$

Наведемо ще одну верхню оцінку параметра $p(G)$, яка може бути корисною у випадку, коли код G має достатньо велику мінімальну відстань.

Твердження 3. Нехай $d \ge d_0$, де d_0 є натуральним числом, що задовольняє нерівності $d_0 < n\frac{1-p}{1+p} + 1$. Тоді

$$p(G) \le 2^{-(d_0-1)} + \left(\frac{1+p}{2}\right)^n \exp\left\{-2n\left(\frac{1-p}{1+p} - \frac{d_0-1}{n}\right)^2\right\}. \quad (15)$$

Доведення. Використовуючи верхню межу (10) та нерівності $d_0 - 1 \le d - 1 \le k$, отримаємо, що

$$p(G) \le \sum_{l=0}^{d_0-1} 2^{-l} p_{n,l} + 2^{-(d_0-1)} \sum_{l=d_0}^{n} p_{n,l} \le 2^{-(d_0-1)} + \sum_{l=0}^{d_0-1} 2^{-l} \binom{n}{l} (1-p)^l p^{n-l} =$$

$$= 2^{-(d_0-1)} + \left(\frac{1+p}{2}\right)^n \sum_{l=0}^{d_0-1} \binom{n}{l} \left(\frac{1-p}{1+p}\right)^l \left(1 - \frac{1-p}{1+p}\right)^{n-l}.$$

Звідси на підставі нерівності Чернова [4] випливає справедливість формули (15).

Твердження доведено.

Як приклад застосування оцінки (15), розглянемо систему з випадковим кодуванням кодом G, який будується на основі розширеного коду Ріда-Соломона з параметрами $(2^m, K, 2^m - K + 1)$ за допомогою додаткової перевірки на парність [5, с. 291]. Код G має параметри $n = 2^m(m+1)$, $n - k = Km$, $d \geq d_0 = 2(2^m - K + 1)$, де $1 \leq K \leq 2^m - 1$, $m \geq 2$.

Отже, за умови $K > 2^m - \frac{1}{2}\left(\frac{n(1-p)}{1+p} + 1\right) + 1$ ймовірність правильного відновлення повідомлень в системі, що розглядається, задовольняє нерівності (15).

Результати розрахунків за формулою (15) при $m = 8$, $K = \left\lfloor \frac{(1-R)n}{m} \right\rfloor$ показують, що при $1/2 < R < 1$, $0{,}1 \leq p \leq 0{,}45$ верхня межа параметра $p(G)$ майже не відрізняється від $2^{-(d_0-1)}$ та є достатньо малою для забезпечення практичної стійкості захисту інформації у відвідному каналі (при цьому швидкість передачі інформації в системі є не менше ніж R). Зокрема, при $R = 0{,}9$ ймовірність правильного відновлення випадкового рівноймовірного повідомлення S довжини $k = 2080$ не перевищує 2^{-457} для усіх значень p, $0{,}1 \leq p \leq 0{,}45$.

Висновки. Основними результатами статті є твердження 1 – 3, що встановлюють точний вираз, а також аналітичні оцінки параметра, який характеризує практичну стійкість систем з лінійним випадковим кодуванням у ДКС: ймовірності правильного відновлення повідомлень у відвідному каналі. На відміну від результатів попередніх робіт [7, 8], отримані оцінки є неасимптотичними та можуть бути застосовані до усіх двійкових лінійних кодів фіксованої довжини. Вони дозволяють сформулювати критерії вибору кодів для побудови практично стійких та ефективних систем з випадковим кодуванням у ДКС та встановити достатню умову асимптотичної досконалості таких систем.

Застосування отриманих оцінок до певних конкретних кодів показує, що для достатньо великої ймовірності стирання $(1 - p \geq 0{,}8)$ та малої швидкості передачі $(kn^{-1} \leq 0{,}2)$ ймовірність правильного відновлення повідомлень у відвідному каналі може бути близькою до ймовірності їх відгадування 2^{-k}.

ЛІТЕРАТУРА

[1]. Алексейчук А.Н. Условия "практической эффективности" и "асимптотической совершенности" кодовой защиты случайных равновероятных сообщений / А.Н. Алексейчук // Защита информации: сборник научных трудов. – Київ: НАУ, 2002. – Вып. 2(9). – С. 48 – 54.

[2]. Алексейчук А.Н. Нелинейное случайное кодирование в системах передачи информации по каналу связи с отводом / А.Н. Алексейчук, С.В. Гришаков // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. 8. – Київ: 2004. – С. 133 – 140.

[3]. Горицький В.М. Спосіб запису двійкової інформації на магнітний носій / В.М. Горицький, Ю.В. Сергієнко // Деклараційний патент на винахід. – UA 98126913 від 28. 12. 1998 р.

[4]. Дискретная математика и математические вопросы кибернетики / Васильев Ю.Л., Ветухновский Ф.Я., Глаголев В.В. и др. – Т. 1. – М.: Наука, 1974. – 311 с.

[5]. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки: Пер. с англ. – М.: Связь, 1979. – 743 с.

[6]. Bellare M. A cryptographic treatment of the wiretap channel / M. Bellare, S. Tesarro, A. Vardy / http://eprint.iacr.org/2012/015.

[7]. Osarov L.H. Wire-tap channel II / L.H. Osarov, A.D. Wyner // Bell Syst. Techn. J. – 1984. – Vol. 63. – pp. 2135 – 2157.

[8]. Thangaraj A. On the application of LDPC codes to a novel wire-tap channel inspired by quantum key distribution / A. Thangaraj, S. Dihidar, A.R. Calderbank, S. McLaughlin, J.-M. Merolla / http://eprint.arXiv:cs.IT/0411003v2. – 24 Okt., 2005.

[9]. Wyner A.D. The wire-tap channel / A.D. Wyner // Bell Syst. Techn. J. – 1975. – Vol. 54. – pp. 1355 – 1388.

REFERENCES

[1]. Alekseychuk A. N. Conditions of "practical effectiveness" and "asymptotic perfectness" of the code security of random equiprobable messages / A.N. Alekseychuk // Zakhist Inform. – 2002. – No. 2(9). – pp. 48 – 54.

[2]. Alekseychuk A. N., Gryshakov S. V., "Nonlinear random coding for information transmission systems with the wire-tap"/ A. N. Alekseychuk, S. V. Gryshakov // Legal, regulatory and metrological support information security system in Ukraine. – Vol. 8. – 2004. – pp. 133 – 140.

[3]. Goritsky V.M. A method of binary information recording on a magnetic medium / V.M. Goritsky, Yu.V. Serhiienko // Declaration patent for an invention. – UA 98126913 from 28. 12. 1998.

[4]. Discrete Mathematics and Mathematical Problems of Cybernetics / Vasiliev Yu.L., Vetukhnovsky F.Ya., Glagolev V.V. – Vol. 1. – 1974. – 311 P.

[5]. MacWilliams F.J., Sloane N.J.A. (1977), "The theory of error-correcting codes", North Holland, Amsterdam.
[6]. Bellare M. A cryptographic treatment of the wiretap channel / M. Bellare, S. Tesarro, A. Vardy / http://eprint.iacr.org/2012/015.
[7]. Osarov L.H. Wire-tap channel II / L.H. Osarov, A.D. Wyner // Bell Syst. Techn. J. – 1984. – Vol. 63. – pp. 2135 – 2157.
[8]. Thangaraj A. On the application of LDPC codes to a novel wire-tap channel inspired by quantum key distribution / A. Thangaraj, S. Dihidar, A.R. Calderbank, S. McLaughlin, J.-M. Merolla / http://eprint.arXiv:cs. IT/0411003v2. – 24 Okt., 2005.
[9]. Wyner A.D. The wire-tap channel / A.D. Wyner // Bell Syst. Techn. J. – 1975. – Vol. 54. – pp. 1355 – 1388.

НЕАСИМПТОТИЧЕСКИЕ ОЦЕНКИ ВЕРОЯТНОСТИ ПРАВИЛЬНОГО ВОССТАНОВЛЕНИЯ СООБЩЕНИЙ В ДВОИЧНОМ ОТВОДНОМ КАНАЛЕ СО СТИРАНИЕМ

Исследуется система передачи информации, состоящая из безызбыточного источника двоичных сообщений, идеального основного канала между отправителем и законным получателем и отводного канала со стиранием между отправителем и противником. Для надежной защиты информации в отводном канале используется известный метод случайного кодирования сообщений двоичными линейными кодами. В статье получены точное выражение и неасимптотические оценки параметра, характеризующего практическую стойкость указанных систем: вероятности правильного восстановления сообщений в отводном канале. Полученные оценки применимы к широкому классу двоичных линейных кодов с известными значениями длины, размерности и минимального (или дуального) расстояния. Они позволяют сформулировать критерии выбора кодов для построения практически стойких и эффективных систем со случайным кодированием в двоичном канале со стиранием, а также установить достаточное условие асимптотической совершенности таких систем. Полученные результаты могут быть использованы в криптографических приложениях, основанных на применении модели канала связи с отводом.
Ключевые слова: криптографическая защита информации, канал связи с отводом, канал со стиранием, случайное кодирование, вероятность правильного восстановления сообщений, обоснованная стойкость.

NON-ASYMPTOTIC ESTIMATES FOR THE PROBABILITY OF CORRECT MESSAGES RECOVERING IN THE BINARY ERASURE WIRETAP CHANNEL

We consider an information transmission system which consists of an irredundant source of binary messages, an ideal main channel between the sender and the legitimate receiver, and an erasure wiretap channel between the sender and the adversary. A known method of random messages coding by binary linear codes is used to ensure reliable information security in the wiretap channel. We obtain the exact expression and non-asymptotic estimates for the probability of correct messages recovering in the wiretap channel. This parameter characterizes practical security of the above mentioned systems. Obtained estimates are applicable to a wide class of binary linear codes with known values of length, dimension and minimal (or dual) distance. They allow us to formulate criteria for choosing codes to construct practically secure and effective systems with random coding in the binary erasure channel and to set sufficient condition of asymptotic perfectness of such systems. The results can be applied for cryptographic applications based on the use of the wiretap channel model.
Keywords: cryptographic information security, wiretap channel, erasure channel, random coding, probability of correct messages recovering, provable security.

Олексійчук Антон Миколайович, доктор технічних наук, доцент, завідуючий кафедри Кібербезпеки Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»
E-mail: alex-dtn@ukr.net
Алексейчук Антон Николаевич, доктор технических наук, доцент, заведующий кафедры Кибербезопасности Института специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского»
Alekseychuk Anton, Doctor of Technical Sciences, Assistant professor, Head of Cybersecurity Department of The Institute of Special Communication and Information Protection of National technical university of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»

Сергієнко Юрій Васильович, начальник науково-дослідного центру Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»
E-mail: syv69@ukr.net
Сергиенко Юрий Васильевич, начальник научно-исследовательского центра Института специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского»
Serhiienko Yurii, Head of Research and Development Department of The Institute of Special Communication and Information Protection of National technical university of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute».