6. *Бахвалов Н.С., Жидков Н.П., Кобельков Г.М.* Численные методы.- М.: БИНОМ. Лаборатория знаний, 2006 г.-636 с.

7. *Парлетт Б.* Симметричная проблема собственных значений. Численные методы.- М.: Мир, 1983. 384 с.

8. *Кобозева А.А.* Стеганографический метод, основанный на преобразовании спектра симметричной матрицы // Журнал «Праці УНДІРТ».-2006.- №4(48).-С. 44-52.

9. *Кобозева А.А.* Исследование проблемы устойчивости стеганографического алгоритма, основанного на нормальном спектральном разложении матрицы // Збірник «Захист інформації».- 2007.-№1(32).-С.

10. *Кобозева А.А.* Применение сингулярного и спектрального разложения матриц в стеганографических алгоритмах // Вісник Східноукраїнського національного університету ім. В.Даля.-2006.-№9(103).- С.74-82.

**УДК 621.372.**

**Лєнков С.В., Іванов Ю.Д., Пампуха І.В., Боряк К.Ф.**

## ОСОБЛИВОСТІ КОРЕГУЮЧИХ ВЛАСТИВОСТЕЙ СТРУКТУРНО-ЛОГІЧНИХ КОДІВ

Структурно-логічні коди (СЛК) використовують природну логічну надлишковість інфимумних диз'юнктивних нормальних форм (ІДНФ) булевих функцій, які є основою побудови кодів СЛК, для виправлення помилок, які виникли при передачі даних по реальним дискретним каналам, окремо по каналам с незалежними помилками. Основною задачею даної роботи являється встановлення базисних співвідношень між реалізованої кодами СЛК логічної надлишковості і граничним значенням кратності незалежних помилок, що виправляються.

В [1] показано, що в межах мінімального інтервалу декодування (МІД) n-мірного куба $E^n$, в якості якого приймається грань, тобто підкуб $E^2$ куба $E^n$, можливо відновлення будь-якої із чотирьох вершин $E_1^0, E_2^0, E_3^0, E_4^0$, спотвореної помилками кратності $t=1,...,n$.

Обов'язковою умовою виправлення помилок в такій скривленій вершині є коректне визначення 3-х останніх із чотирьох вершин МІД.

Таким чином, в межах МІД можливе виправлення будь-якої $t \le n$ - кратної помилки на довжині n розрядів вершини $E^0$ куба $E^2$.

Якщо помилка кратності $n \ge t>1$ спотворює одночасно розряди двох сусідніх вершин, то така помилка виправлена бути не може, оскільки порушується обов'язкова умова коректності 3-х вершин МІД при виправленні четвертої вершини, тобто спотвореними стають 2 вершини МІД.

Пакетна помилка, окремим випадком якої є $t$-кратна помилка, починається і закінчується завжди, як і $t$-кратна помилка, помилковим бітом (розрядом). У загальному випадку для пакетної помилки характерна наявність безпомилкових біт у середині пакету помилок, в той час як при $t$ - кратній помилці безпомилкові біти відсутні.

Визначимо ймовірність помилки МІД для випадку, коли спотворена більш ніж одна вершина МІД. Нехай ймовірність неправильного прийому одного блоку (розряду) для каналу з незалежними помилками при рівномірному їх розподілі складе $p_0$.

При незалежних помилках ймовірність появи деякого числа спотворених біт в межах n розрядів вершини МІД не залежить від взаємного розташування спотворених біт і визначається тільки числом спотворених біт і вірогідністю помилки $p_0$ одного біта.

Ймовірність $p_0$ відповідає ймовірності 1-кратної помилки. Двократна помилка визначається наявністю 2-х помилкових біт одночасно що відповідає ймовірності $p_0(2)=p_0p_0=p_0^2$.

Ймовірність t-кратної помилки визначається виразом

$$p_0(t)=p_0^t, \quad t=1,...,n, \tag{1}$$

де n - розрядність кожної вершини МІД, визначеної в n-мірному кубі $E^n$.

З іншої сторони, ймовірність правильного прийому одного біта складе $p_п(1)=(1-p_0)$, а ймовірність правильного прийому двох біт - $p_п(2)=(1-p_0)^2$. Тоді ймовірність правильного прийому n біт складе

$$p_п(n)=(1-p_0)^n \tag{2}$$

Розглянемо варіанти помилкового прийому двох сусідніх n-розрядних вершин МІД на прикладі 4-х розрядних вершин. Якщо t-кратна помилка перевищує розрядність n хоча б на одиницю (t=n+1), то така помилка в межах МІД не може бути виправлена, оскільки помилками будуть задіяні 2 сусідніх вершини, як це показано на рис.1.

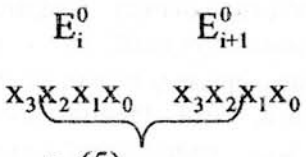

Рис.1.

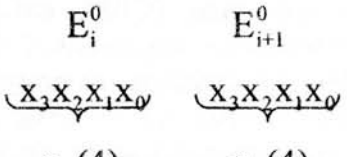

Рис.2.

Як видно з рис.1. 5-кратна помилка з ймовірністю $p_0(5)=p_0^{n+1}=p_0^5$, при n=4 зачіпає 2 сусідніх вершини.

У загальному випадку помилки кратності t>n не можуть бути виправлені в межах МІД.

Таким чином, ймовірність помилкового прийому 2-х вершин МІД, обумовлена дією помилки кратності t>n на довжині 2n біт вершин $E_i^0$ і $E_{i+1}^0$, з урахуванням виразу (1) і (2) складе

$$P(t>n)=\sum_{t=n+1}^{2n} C_{2n}^t p_0^t (1-p_0)^{2n-t} \tag{3}$$

У разі попадання n-кратної помилки (t=n) з ймовірністю $p_0(4)=p_0^n=p_0^4$ в межі тільки однієї вершини МІД вершина повністю відновлюється, тобто така помилка виправляється (рис.2). Інакше, коли помилка кратності $1<t\le n$ не потрапляє в межі тільки однієї вершини можливо декілька варіантів помилкового прийому двох сусідніх вершин МІД.

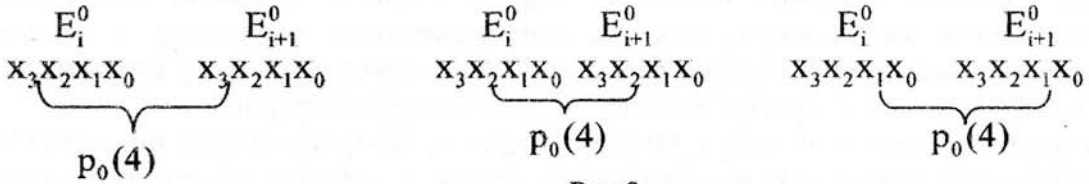

Рис.3.

Як видно з рис.3, який являє собою приклад одночасного спотворення двох вершин для t=n=4, число варіантів спотворення сусідніх вершин $E_i^0$ і $E_{i+1}^0$ визначається як $C_{2(t-1)}^t$. Це дійсно так, оскільки максимальне число помилкових біт t-1 в межах n біт однієї вершини обов'язкове пропонує хоча б 1 помилковий біт в межах n біт іншої вершини для забезпечення

одночасного спотворення вершин $E_i^0$ і $E_{i+1}^0$. Ймовірність появи t спотворених біт на довжині 2n біт рівна, як відомо, $p_0^t(1-p_0)^{2n-t}$. Звідси витікає, що ймовірність помилкового прийому 2-х вершин МІД в результаті дії помилки кратності $1<t\le n$ на довжині 2n біт з урахуванням числа варіантів спотворення складе

$$P(1<t\le n)=\sum_{t=2}^{n} C_{2(t-1)}^t p_0^t(1-p_0)^{2n-t} \qquad (4)$$

Вирази (3) і (4) дозволяють оцінити ймовірність помилки мінімального інтервалу декодування, обумовлену дією незалежних $1<t\le n$ і $t>n$ - кратних помилок одночасно на дві вершини $E_i^0$ і $E_{i+1}^0$ МІД в межах 2n біт.

**Лема 1**

Ймовірність помилки МІД $n$-мірного куба $E^n$, обумовленої помилковим прийомом двох вершин завдовжки $2n$ біт, при дії незалежних помилок кратності $1<t\le n$ і $t<n$ визначається виразом

$$P_{мід}=P(t>n)+P(1<t\le n)=\sum_{t=n+1}^{2n} C_{2n}^t p_0^t(1-p_0)^{2n-t}+\sum_{t=2}^{n} C_{2(t-1)}^t p_0^t(1-p_0)^{2n-t} \qquad (5)$$

Вираз (5) дозволяє оцінити коректуючі властивості мінімального інтервалу декодування, яке є основою побудови єдиного кодованого формату (ЕКФ), тобто кодової комбінації коду СЛК. Оцінка базових коректуючих властивостей МІД дає можливість визначити коректуючі властивості коду СЛК в цілому для заданого каналу з незалежними помилками.

Для оцінки коректуючих властивостей МІД побудуємо залежність $P_{МІД}=f(p_0)$ при різній довжині n вершин.

При визначенні вірогідності помилки МІД $P_{МІД}(5)$ враховувалися тільки ті варіанти помилок t, які приводили до помилкового прийому, тобто по суті справи до неправильного декодування МІД, що визначається точніше як ймовірність помилки декодування фрагмента кодової комбінації СЛК, тобто ЕКФ.

Аналіз фрагментарного декодування СЛК, на основі залежності $P_{МІД}=f(p_0)$ при n=3,4,5 представленій на рис.4, показав, що вплив розрядності n вершин куба $E^n$ на ймовірність помилки декодування $P_{МІД}$ практично відсутнє. У достатньо важких каналах при $p_0=10^{-1}\div 5\cdot 10^{-2}$ фрагментарне декодування СЛК зіставно по ймовірності помилки декодування з загортковим кодом, що виправляє помилки $t\le 2$, що указує на можливість успішного використання кодів СЛК в реальних каналах передачі даних.

Використання МІД як єдиного кодуючого формату, тобто кодової комбінації СЛК, як це витікає з аналізу, не є достатньо ефективним, оскільки фрагментарне використання коду СЛК поступається по ймовірності помилки декодування відомим коректуючим коректованим кодом, зокрема згортковим кодом, в каналах з ймовірністю помилки $p_0=10^{-2}\div 10^{-5}$.

Нехай в якості ЕКФ прийнята послідовність вершин куба $E^3$, тобто n=3. Прийнятий куб $E^3$ містить два мінімальні інтервали декодування $МІД_1$ і $МІД_2$, що складаються з 4-х вершин кожен (рис.5).

Нехай всі вершини $МІД_1$ повністю відновлені, що указує на те, що було спотворене не більше однієї вершини в $МІД_1$. Тоді для повного відновлення всіх вершин в $МІД_2$, як це витікає з [1], необхідне знання відповідної змінної розгортання. Як видно з рис.5 для

визначення цієї змінної необхідно і достатньо, щоб тільки одна з 4-х вершин $МІД_2$ була б прийнята коректно, оскільки кожна з вершин $МІД_1$ пов'язана з відповідною вершиною $МІД_2$ по однаковій змінній (на рис.5 такою змінною виступає $x_2$). Тому для будь-якої з вершин $МІД_2$ (5,6,7,8), прийнятої коректно, можливо визначення змінної $x_2$, що розгортає $МІД_1$ в ЕКФ, тобто куб $E^3$.

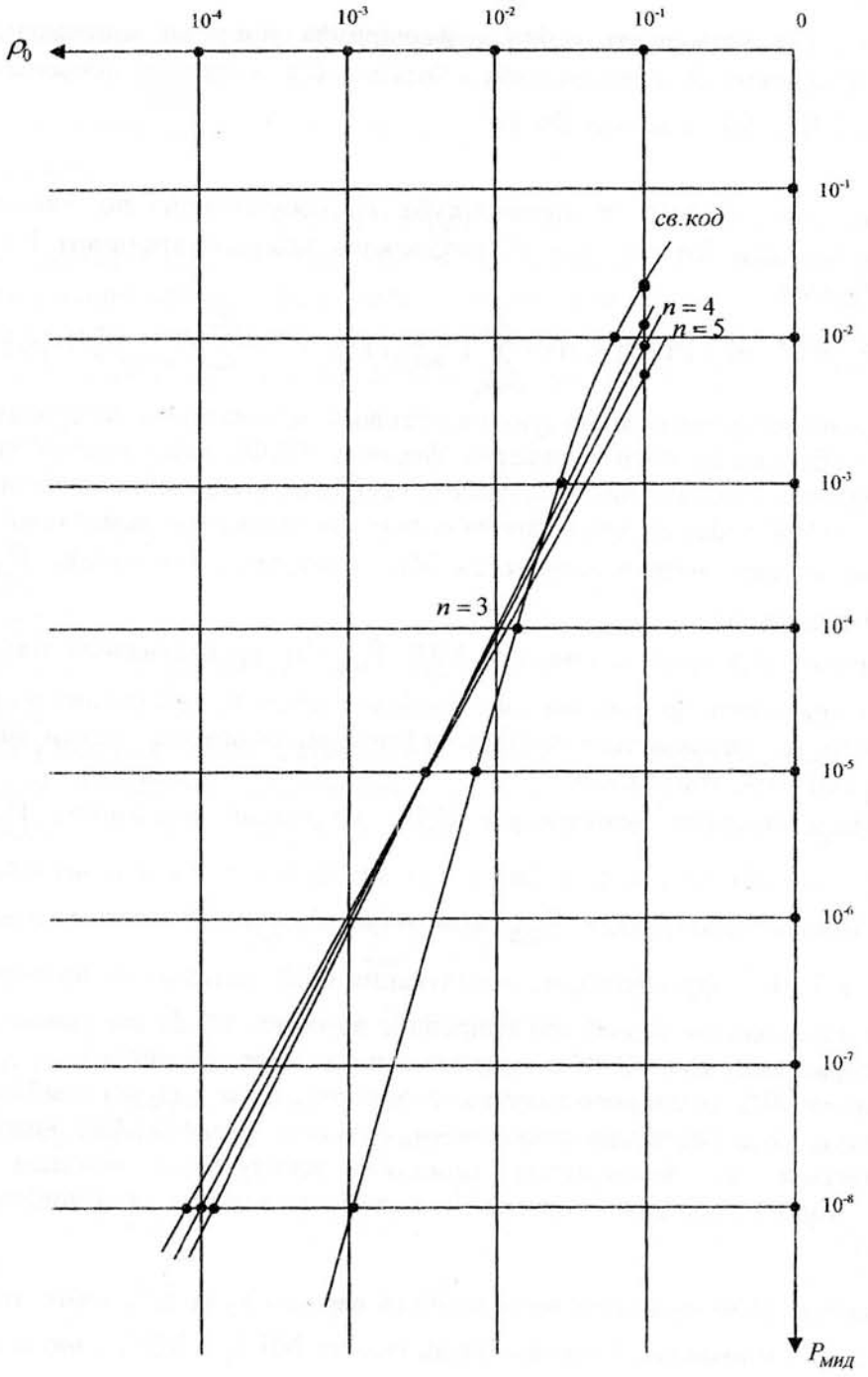


Рис.4

Інші три вершини $МІД_2$ можуть бути прийняті з помилками на етапі визначення змінної розгортання $x_2$, оскільки надалі на цьому етапі відновлення всі помилки у вершинах

$МІД_2$ виправляються. У межах МІД в якості породжуючих використовуються 2 змінні розгортання (у нашому прикладі це $x_0$ і $x_1$). Одна змінна, що залишилася ($x_2$ у нашому прикладі) використовується для повного відновлення всіх вершин в $МІД_2$, а отже і всього ЕКФ. Якби в якості ЕКФ виступав куб $E^n$, то, при повністю відновлених вершинах одного МІД, для правильного прийому всіх вершин ЕКФ необхідне знання відповідних змінних розгортання на кожному етапі перетворення МІД в ЕКФ кубів $E^3, E^4, E^5, \ldots E^n$.

В загальному випадку таких змінних повинно бути $n-2$, оскільки в МІД використовується 2 змінні розгортання з всієї кількості $n$. У зв'язку з вищевикладеним справедлива.

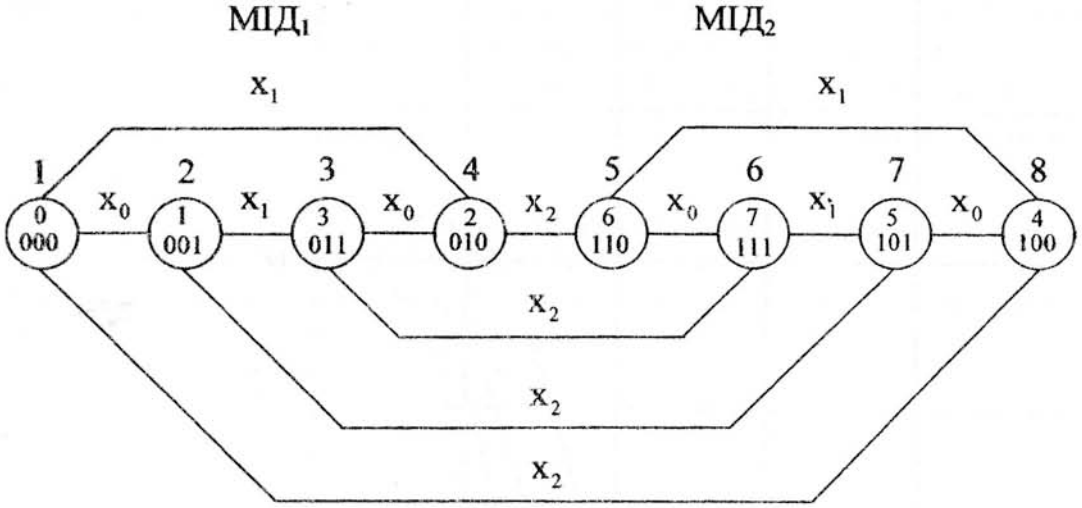


Рис.5.

**Лема 2**

Для повного відновлення всіх вершин ЕКФ куба $E^n$ необхідно і достатньо при коректно прийнятому одному МІД наявність хоч би однієї, прийнятої безпомилково вершини в межах відновлюваного куба $E^3, E^4, \ldots E^n$ *на кожному етапі перетворення.*

Це дійсно так, оскільки наявність однієї правильної вершини в межах відновлюваного куба, окрім відновлених вершин на попередніх етапах, дає можливість визначити змінну відновлення однозначно.

Для $n$-розрядної вершини ймовірність помилкового прийому з урахуванням одночасності збою і розрядів і правильного прийому $n$-і розрядів складе $p_0^i(1-p_0)^{n-i}$. Число варіантів збою і розрядів очевидно рівно $C_n^{ii}$. Зрозуміло, що кількість збитих розрядів в межах оцінки вершини може змінюватись від 1 до n. У такому разі ймовірність помилкового визначення змінної відновлення із-за неправильного прийому однієї вершини у межах відновлюваного n-мірного куба $E^n$ буде рівна

$$P'=\sum_{i=1}^{n} C_n^i p_0^i (1-p_0)^{n-i} \qquad (6)$$

Ймовірність $P'$ визначає, по суті справи, ймовірність помилкового декодування чергового відновлюваного МІД в межах ЕКФ куба $E^n$. Тоді ймовірність помилкового декодування ЕКФ куба $E^n$ з урахуванням ймовірності помилки $P_{МІД}(5)$ буде визначатися таким чином.

**Лема 3**

Ймовірність помилкового декодування ЕКФ визначається ймовірністю помилки МІД $P_{МІД}$ і ймовірністю помилки змінної відновлення $P'$

$$P_{ЕКФ} = P_{МІД} \cdot (P')^{n-2} \tag{7}$$

де $P_{МІД}$ - ймовірність помилки МІД $n$-мірного куба $E^n$, $P'$ - ймовірність помилки змінної відновлення (6).

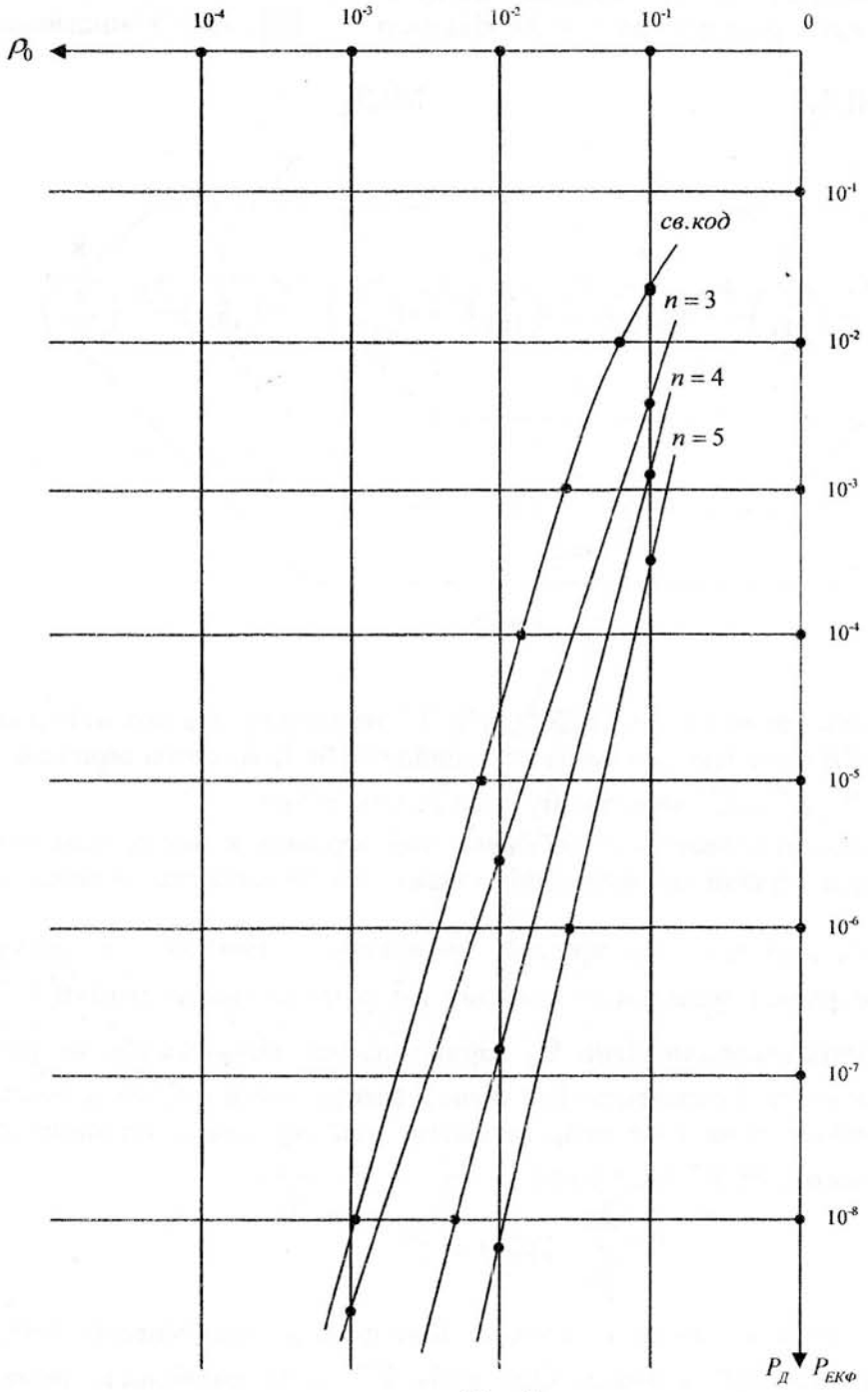


Рис.6

Порівнюючи $P_Д$ для згорткового коду і $P_{ЕКФ}$ для n=3,4,5 помічаємо, що для n=3 при $p_0=10^{-2}$ (ймовірність збою біта в каналі з незалежними помилками) виграш складає в першому наближенні 1 порядок ($P_Д=2\cdot10^{-5}$,$P_{ЕКФ}=2\cdot10^{-6}$). Для n=4 виграш складає 2 порядки ($P_Д=2\cdot10^{-5}$, $P_{ЕКФ}=1{,}5\cdot10^{-7}$) а для n=5 - більш, чим 3 порядки ($P_Д=2\cdot10^{-5}$,$P_{ЕКФ}=8\cdot10^{-9}$). У важкому каналі з $p_0=10^{-1}$ виграш в завадостійкості для СЛК коду складає від 0,5 порядку (n=3) до 1,5 порядку (n=5). Крім того, із зменшенням вірогідності помилки в каналі $p_0$ до $10^{-3}\div10^{-4}$ виграш в завадостійкості для коду СЛК, принаймні, не зменшується, особливо для n=4,5, тобто як нахил прямих декодування до осі абсцис в порівнянні з згортковим кодом зменшується. Таким чином, використання структурно-логічних кодів в каналах з незалежними помилками забезпечує істотні переваги в завадостійкості, особливо у важких каналах з $p_0=10^{-1}\div5\cdot10^{-2}$ і каналах середньої тяжкості з $p_0=10^{-2}\div10^{-4}$.

**Список літератури**

1. *Іванов Ю.Д., Пампуха І.В., Захарова О.С., Якимов В.В.*
Основні положення декодування структурно-логічних кодів // Збірник наукових праць. ВІКНУ ім. Т.Шевченка – Вий.7.-Київ: ВІКНУ, 2007. – с.110-116.

**УДК 65.012.8: 004.492**

**Гроздов Г.Г.**

## СПОСОБ ФОРМИРОВАНИЯ ЭФФЕКТИВНОЙ КОМПЛЕКНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ МЕТОДОВ МАТЕМАТИЧЕСКОЙ ТЕОРИИ ИГР

В настоящее время актуальна задача построения и оценки эффективности механизмов защиты информации в различных комплексных системах защиты информации (КСЗИ) автоматизированных систем (АС).

Можно выделить такие классы информации, защита которых должна обеспечиваться механизмами защиты информации (ЗИ), входящими в состав КСЗИ: информация, составляющая коммерческую и военную тайну. В АС указанных классов могут иметь приоритетное значение различные требования к механизмам ЗИ [1, 4].

В научно-технической литературе рассматриваются два аспекта эффективности системы ЗИ. С одной стороны, система защиты информации должна эффективно противодействовать угрозам [2]. С другой стороны, она должна быть адекватной – расходы на безопасность не должны превышать стоимости самой информации и размера возможных потерь, вызванных успешной реализацией угроз [4].

### Существующие методики формирования эффективной системы защиты информации, их недостатки

К наиболее известным методикам формирования эффективной КСЗИ относятся метод ожидаемых потерь [1] и методика совокупной стоимости владения [12, 13], способ, основанный на применении методов нелинейного программирования [5]. Несмотря на свои достоинства, указанные методики имеют ряд недостатков: