взвешенных потерь, рассчитанную с учетом вероятностей возникновения частных потерь p_i. Для угроз t_i сопоставление величин взвешенных потерь

$$Q\ (t_i) = \sum_{r=1}^{m} q_{ri}\ p_{ri},\ i = \overline{1,n} \tag{23}$$

может привести к результатам ранжировки угроз, несколько отличным от ранее полученных. Однако взвешивание потерь по их вероятности позволяет более объективно оценить эффективность применяемых средств и методов защиты, проанализировать и сравнить возможные варианты контрмер. Для этого необходимо располагать сведениями об остаточных вероятностях потерь $[p_{ori}]$, зная которые можно по аналогии с выражением (23) рассчитать взвешенные остаточные потери $Q_o^*(t) = [\,Q_o^*(t_1),...,Q_o^*(t_n)]$.

На практике возможно возникновение различных ситуаций, допускающих упрощение условий исходной постановки общей задачи, комбинированное применение к её решению уже рассмотренных выше процедур и вариантов обработки данных, позволяющих корректно провести анализ информационных рисков.

VI Выводы

Предложена методика применения теоретико-вероятностного аппарата средних рисков для решения задач анализа и оценивания эффективности систем защиты информации. Разработана процедура преобразования исходных данных, получаемых при проведении аудита информационных систем, к виду, допускающему непосредственное вычисление функционала среднего риска. Получены основные расчетные соотношения. Приведены некоторые упрощенные варианты анализа эффективности систем защиты.

*Литература: **1**. Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. М.: Компания Ай Ти; ДМК Пресс, 2004. - 348 с. **2**. Симонов С. В. Методология анализа рисков в информационных системах// Конфидент. Защита информации. - №2. – 2001. – с. 48 – 53. **3**. Петренко С. А., Петренко А. А Аудит безопасности Intranet. – М.: ДМК Пресс, 2002. – 416 с. **4**. Астахов А. М. Аудит безопасности ИС // Конфидент. Защита информации. - №1. – 2003. – с. 63 – 67. **5**. Архипов О. Є., Ворожко В. П. Системний підхід до оцінювання ефективності захисту державної таємниці // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні// науково-техн. зб. – Київ, 2005. – Вип. 10. – с.18 – 22. **6**. Качинський А. Б. Безпеки, загрози і ризик: Наукові концепції та математичні методи. - К.: 2003.- 472 с. **7**. Алгоритмы и программы восстановления зависимостей / Под ред. В. Н. Вапника. – М.: Наука, 1984. – 816 с. **8**. Пугачев В. С. Теория вероятности и математическая статистика. – М.: Наука, 1979. – 496 с. **9.** Воробиенко П., Нечипорук О., Щербина Ю. Принципы построения модели угроз информационным ресурсам систем и сетей связи // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Вип. 7 – К.: 2003. - с. 11 – 13. **10.** Гостев И. М. Безопасность – бесполезная трата денег или их выгодное вложение?// Конфидент. Защита информации. - №5. – 2003. – с. 16 – 18. **11.** НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.*

УДК 681.3.06

МЕТОД ПОБУДОВИ S-БЛОКІВ З ВЛАСТИВІСТЮ КОРЕЛЯЦІЙНОЇ ІМУННОСТІ КООРДИНАТНИХ ФУНКЦІЙ

Олександр Дирда, Леонід Скрипник

Інститут спеціального зв'язку та захисту інформації НТУУ "КПІ"

Анотація: **Розглядаються методи побудови кореляційно-імунних булевих функцій та еластичних функцій для синтеза криптографічних алгоритмів. Запропоновано евристичний алгоритм побудови збалансованої кореляційно-імунної функції, а також метод побудови S-блоків з властивістю кореляційної імунності першого порядку координатних функцій.**

Summary: **Methods of construction of correlative-immune Boolean functions and resilient functions for synthesis of cryptographic algorithms are regarded. It is proposed heuristic algorithm of construction of balanced correlative-immune function, and also are proposed methods of construction of S-blocks with**

property of first-order correlative immunity of the coordinate functions.
Ключові слова: **S-блокі, криптографічні алгоритми, координатні функції, *булеве відображення.***

I Вступ

В сучасних криптографічних алгоритмах як нелінійні вузли ускладнення широко використовуються $n \times m$ S-блоки, які являють собою функцію $S : V_n \to V_m$, де $n \geq m$, а V_k – лінійний простір бітових векторів довжини k. S-блок розміру $n \times m$ може бути поданий як система з m булевих функцій від n змінних кожна, тобто, $S = (f_1, f_2, ..., f_m)$, де $f_j : V_n \to \{0, 1\}$, $j = \overline{1, m}$. Функції f_j, $j = \overline{1, m}$ носять назву координатних функцій.

На практиці, як правило, використовуються $n \times m$ S-блоки, які реалізують збалансовані булеві відображення, тобто, $\forall\, v \in V_m \quad \#\{u \in V_n \,|\, S(u) = v\} = 2^{n-m}$. Для таких відображень збалансованими (рівноймовірними, врівноваженими) є всі координатні функції, а також усі їх нетривіальні лінійні комбінації. Збалансоване булеве відображення при $n = m$ реалізує бієктивну (взаємно-однозначну) функцію, отже, $n \times n$ S-блок, за умовою збалансованості, реалізує підстановку на множині $\{0, 1, ..., 2^n - 1\}$. Це є найбільш типовим випадком при побудові криптографічних алгоритмів, зокрема, такі S-блоки використовуються в алгоритмах Lucifer, ГОСТ 28147-89, Serpent, SC2000, MISTY1, IDEA, Skipjack, Rijndael, Snow, Square, Shark, Twofish, RC2, RC4, MD2, Anubis, E2, Camellia, Crypton, CS, Khazad, Q, Safer+, Whirlpool, Magenta, Treyfer, Turing, Hierocrypt-3, Scream, HBB, Squafer, BelT, DESX, Торнадо тощо.

Від властивостей S-блоків суттєво залежить криптографічна стійкість шифрів, що диктує необхідність синтезу S-блоків, які є стійкими до сучасних методів криптографічного аналізу. Одним із шляхів підвищення криптографічної стійкості шифрів є застосування S-блоків, усі координатні функції яких задовольняють певним властивостям, які вибираються таким чином, щоб протистояти відомим методам криптографічного аналізу шифрів.

II Кореляційно-імунні та еластичні функції

Однією з важливих властивостей булевих функцій є кореляційна імунність (надалі – к.і.) [1]. Булева функція f має t-ий порядок кореляційної імунності, якщо вона статистично незалежна від будь-якої множини вхідних змінних потужності t. У загальному випадку функція f є кореляційно-імунною функцією порядку t тоді і тільки тоді, коли для будь-якого набору індексів $1 \leq i_1 < i_2 < ... < i_t \leq n$, а також значень $a_1, a_2, ..., a_t \in \{0,1\}$ виконується рівність $\left\| f_{i_1 i_2 ... i_t}^{a_1 a_2 ... a_t} \right\| = \dfrac{\|f\|}{2^{t+1}}$, де $f_{i_1 i_2 ... i_t}^{a_1 a_2 ... a_t}$ – підфункція функції f, яка утворюється при підстановці значень $a_1, ..., a_t$ замість змінних $x_{i_1}, ..., x_{i_t}$, $\|f\|$ – вага за Хемінгом функції f.

Окремим випадком кореляційної імунності t-го порядку є t-рівноймовірність булевої функції. Булева функція f від n змінних називається t-рівноймовірною, якщо всі її підфункції, отримані в результаті фіксації довільних t змінних довільними t константами, є рівноймовірними функціями. Збалансована кореляційно-імунна порядку t функція носить назву t-стійкої функції. Легко бачити, що поняття t-стійкості і t-рівноймовірності збігаються.

Нехай f – булева функція від n змінних, а $x^{(1)}, x^{(2)}, ..., x^{(n)}$ – незалежні випадкові величини з розподілом Бернуллі з параметром $p(x^{(i)} = 1) = 0.5$, $i = \overline{1, n}$. Двійкова випадкова величина $\gamma = f(x^{(1)}, x^{(2)}, ..., x^{(n)})$ має розподіл Бернуллі з параметром $p(\gamma = 1) = \dfrac{\|f\|}{2^n}$. Для к.і. функції f порядку t, $0 < t \leq n$, для будь-якого набору індексів $1 \leq i_1 < i_2 < ... < i_t \leq n$ випадкові величини $(x^{(i_1)}, x^{(i_2)}, ..., x^{(i_t)})$ і γ є незалежними. Така властивість к.і. функцій є вагомим аргументом щодо їх використання у нелінійних вузлах ускладнення криптографічних алгоритмів. Для вузлів, у яких

застосовуються к.і. функції, ускладнюється застосування кореляційних методів криптографічного аналізу, які засновані на обчисленні кореляції між "входом" та "виходом" функції.

Для к.і. функцій має місце нерівність Зігентайлера, а саме, для незбалансованих кореляційно-імунних порядку t функцій виконується нерівність $\deg(f) \le n - t$, а для t-стійких функцій – $\deg(f) \le n - t - 1$ [1]. Якщо в нерівності Зігентайлера досягається рівність, то функція носить назву оптимальної функції.

На теперішній час запропоновано цілий ряд підходів для побудови к.і. функцій [1 – 6]. Більшість з цих підходів є рекурсивними, тобто, для побудови к.і. функцій від більшої кількості змінних використовуються к.і. функції від меншої кількості змінних.

Як приклад, розглянемо два способи побудови к.і. функцій, які описані в [1].

1. Нехай $f_1(x_1,...,x_n)$ і $f_2(x_1,...,x_n)$ – к.і. функції порядку t, $\|f_1\| = \|f_2\|$.

   оді функція $f(x_1,...,x_{n+1}) = x_{n+1} f_1(x_1,...,x_n) \oplus (1 \oplus x_{n+1}) f_2(x_1,...,x_n)$ є к.і. функцією порядку t.

2. Нехай $g(x_1,...,x_n)$ – к.і. функція порядку t.

   Тоді функція $f(x_1,...,x_n,x_{n+1}) = g(x_1,...,x_n) \oplus x_{n+1}(g(x_1,...,x_n) \oplus g(x_1 \oplus 1,...,x_n \oplus 1))$ є к.і. функцією порядку $t+1$.

У роботі [6] показано, що можливо будувати збалансовані к.і. функції з нелінійністю, більшою за $2^{n-1} - 2^{\left\lceil \frac{n-1}{2} \right\rceil}$.

Ще один підхід щодо побудови к.і. функцій описано в [7]. В цій статті вводиться поняття c-регулярної функції. Нехай $0 \le c \le n$. Функція $f(x_1,...,x_n)$ носить назву c-регулярної функції, якщо $\forall a \in V_n$ виконується рівність $\#\{i \mid i = \overline{1,n},\ f(a) = f(a^i)\} = c$, де a^i – вектор, якій відрізняється від вектора a тільки i-ою координатою. У статті доводиться, що c-регулярна функція є кореляційно-імунною порядку $n - c - 1$ функцією. $(c+1)$-регулярна функція f від $2n+2$ змінних утворюється з двох c-регулярних функцій f_1 і f_2 від n змінних за формулою

$$f(x_1...,x_n,y_1,...,y_n,z_1,z_2) = \bigoplus_{i=1}^{n} x_i \oplus \bigoplus_{i=1}^{n} y_i \oplus z_1 \oplus (z_1 \oplus z_2)\left(f_1(x_1,...,x_n) \oplus \bigoplus_{i=1}^{n} x_i \right) \oplus$$
$$(z_1 \oplus z_2 \oplus 1)\left(f_2(y_1,...,y_n) \oplus \bigoplus_{i=1}^{n} y_i \right). \qquad (1)$$

В [7] доведено, що $N(f) \ge 2^{n+1}(N(f_1) + N(f_2))$, де $N(f)$ – нелінійність функції f. Крім того, якщо хоча б одна з функцій $f_1(x_1,...,x_n) \oplus \bigoplus_{i=1}^{n} x_i$ або $f_2(y_1,...,y_n) \oplus \bigoplus_{i=1}^{n} y_i$ є збалансованою, то $N(f) = 2^{2n} + 2^{n+1} \min\{N(f_1), N(f_2)\}$. За допомогою методу, який запропоновано в [7], побудована 29-стійка функція від 50 змінних, яка має алгебраїчний степінь 20.

Перевагами рекурсивних методів побудови к.і. булевих функцій є, по-перше, велика швидкодія, по-друге, математична доведеність. Недоліком є те, що рекурсивні методи не дозволяють будувати оптимальні функції. Тому на практиці знайшли використання евристичні алгоритми побудови к.і. функцій [8. 9]. Ці алгоритми призначені для побудови к.і. функцій від порівняно невеликої кількості змінних. Розробка ефективних алгоритмів побудови к.і. функцій з високими показниками нелінійності є актуальною задачею сучасної криптографії.

III Підходи до побудови S-блоків з властивістю кореляційної-імунності координатних функцій

При використанні S-блоків під час побудови вузлів ускладнення потокових шифрів доцільно вимагати, щоб усі координатні функції підстановки задовольняли властивості кореляційної імунності. Це забезпечить стійкість шифрів відносно кореляційних методів криптографічного аналізу. Незбалансовані булеві відображення, координатні функції яких задовольняють властивості кореляційної імунності,

будуються досить легко шляхом набору координатних функцій з множини кореляційно-імунних функцій. Однак, поєднання вимог збалансованості булевого відображення та кореляційної імунності координатних функцій вимагає розробки спеціальних алгоритмів.

Одним із підходів побудови S-блоків з властивістю к.і. координатних функцій є еластичні функції (англ. – resilient function) [10]. Сутнісною властивістю еластичних функцій є здатність зберігати властивість збалансованості при обмеженнях спеціального виду на їх областях визначення. Нехай $S = (f_1, f_2, ..., f_m) : V_n \to V_m$ – булеве відображення. Функція S називається (n, m, t)-стійкою (або еластичною), якщо для будь-якого набору індексів $1 \le i_1 < i_2 < ... < i_t \le n$, а також значень $a_1, a_2, ..., a_t$ з множини $\{0, 1\}$ відображення $S_{i_1 i_2 ... i_t}^{a_1 a_2 ... a_t} = ((f_1)_{i_1 i_2 ... i_t}^{a_1 a_2 ... a_t}, ..., (f_m)_{i_1 i_2 ... i_t}^{a_1 a_2 ... a_t}) : V_{n-t} \to V_m$ є збалансованим. Легко бачити, що $(n, 1, t)$-еластична функція – це збалансована кореляційно-імунна порядку t-булева функція (t-стійка функція) від n змінних.

Теорема [10]. Функція S є (n, m, t)-еластичною функцією тоді і тільки тоді, коли будь-яка ненульова лінійна комбінація координатних функцій є $(n, 1, t)$-еластичною функцією.

У загальному випадку кореляційно-імунні функції та еластичні функції пов'язані з ортогональними таблицями [11, 12]. Як приклад, розглянемо зв'язок к.і. функцій і ортогональних таблиць. Ортогональною таблицею розміру $m \times n$, потужності t і індексу ν називається таблиця розміру $m \times n$ над скінченним полем $GF(2)$, у якій для будь-якої підмножини з t стовпців матриці будь-який з 2^t векторів лінійного простору V_t зустрічається в точності ν разів. Така таблиця позначається $OA_\nu(m, n, 2, t)$. Очевидно, що $m = \nu 2^t$. Для функції f через M_f позначимо матрицю розміру $\|f\| \times n$, рядками якої є ті набори векторів $a \in V_n$, для яких $f(a) = 1$. Функція f від n змінних є кореляційно-імунною порядку t функцією тоді і тільки тоді, коли M_f є ортогональною таблицею $OA(\|f\|, n, 2, t)$.

На теперішній час запропоновані тільки рекурсивні методи побудови (n, m, t)-еластичних функцій. Нижче наведені два приклади побудови еластичних функцій.

1. Нехай $F = (f_1, ..., f_m)$ - (n_1, m, t_1)-еластична функція, а $G = (g_1, ..., g_m)$ – (n_2, m, t_2)-еластична функція.

   Тоді функція $F(x) \oplus G(y) = (f_1(x) \oplus g_1(y), ..., f_m(x) \oplus g_m(y))$ є $(n_1 + n_2, m, t_1 + t_2)$-еластичною функцією.

2. Нехай $F = (f_1, ..., f_{m_1})$ – (n_1, m_1, t_1)-еластична функція, а $G = (g_1, ..., g_{m_2})$ – (n_2, m_2, t_2)-еластична функція.

   Тоді функція $P(z) = (f_1(x), ..., f_{m_1}(x), g_1(y), ..., g_{m_2}(y))$ є $(n_1 + n_2, m_1 + m_2, \min(t_1 + t_2))$-еластичною функцією.

Рекурсивні методи не дозволяють побудувати еластичні функції з високими степенями нелінійності координатних функцій, що є перешкодою для застосування таких алгоритмів під час синтезу S-блоків для криптографічних алгоритмів.

Таким чином, для побудови S-блоків з властивістю кореляційної імунності координатних функцій необхідно, по-перше, розробити ефективний алгоритм побудови збалансованих к.і. функцій, по-друге, розробити метод побудови збалансованого булевого відображення, в якому координатні функції вибираються з множини збалансованих к.і. функцій.

Надалі будемо розглядати кореляційну імунність першого порядку. Для таких функцій вихідні значення статистично не залежать від будь-якої її змінної.

Асимптотична оцінка ймовірності побудови к.і. функції першого порядку від n змінних при "випадковій" генерації булевої функції згідно [13] обчислюється за формулою

$$p_{к.і.}(n) \sim \frac{1}{2\exp\left(n\left(\ln\sqrt{\frac{\pi}{2}} + \left(\frac{n}{2} - 1\right)\ln 2\right)\right)}. \qquad (2).$$

Зокрема, $p_{к.і.}(8) \approx 10^{-6}$.

Емпірична оцінка ймовірності побудови 1-стійкої функції від n змінних при "випадковій" генерации збалансованої булевої функції наведена в табл. 1.

Таблиця 1

n	4	5	6	7	8
$p_{к.і.}(n)$	0.0174029	0.00134697	5.57267e-05	1.10605e-06	4.20106e-08

Наведені асимптотична та емпірична оцінки показують, що використання переборних алгоритмів для побудови S-блоків з властивістю 1-стійкості координатних функцій практично неможливе. При "випадковій" генерації 8×8 S-блоків імовріність події, що всі координатні функції будуть 1-стійкими, дорівнює $\sim 10^{-48}$.

З іншого боку, при "випадковому" наборі n збалансованих булевих функцій імовірність утворити підстановку обчислюється за формулою

$$\frac{\left(\left(2^{n-1}\right)!\right)^{2n}}{\left(\left(2^{n}\right)!\right)^{n-1}}.$$

Для $n = 8$ ця ймовірність приблизно дорівнює 10^{-99}. Отже, практично неможливо утворити підстановку при наборі n булевих функцій.

Для побудови підстановки, в якій усі координатні функції задовольняють властивості кореляційної імунності, можливо застосувати два підходи.

Перший підхід засновано на алгоритмі послідовного спрямованого перебору координатних функцій підстановки. Алгоритм складається з n кроків. На кроці $j = \overline{1,n}$ здійснюється побудова координатної функції f_j збалансованого булевого відображення $S = (f_1, f_2, ..., f_n)$. Ця функція будується за переборним алгоритмом, при цьому перебір здійснюється з урахуванням збалансованості відображення $S^{(1,2,...,j)} = (f_1, f_2, ..., f_j)$. При переборі перевіряється вимога кореляційної імунності для координатної функції f_j, $j = \overline{1,n}$. Алгоритмічна складність цього алгоритму дорівнює

$$C_T(n) = O\left(\frac{n}{p_{к.і.}(n)}\right),$$

де $p_{к.і.}(n)$ обчислюється за формулою (1).

Складність побудови 8×8 S-блоку за цим алгоритмом дорівнює $C_T(8) \approx 10^8$. Перевагою цього методу є те, що під час побудови S-блоку можливо висунути додаткові вимоги до координатних функцій, наприклад, вимоги „суворого лавинного критерію" [14].

Іншим підходом до побудови кореляційно-імунних S-блоків є послідовний набір координатних функцій з використанням деякого евристичного алгоритму побудови к.і. функцій. При цьому під час побудови 2, 3, ..., n координатної функції необхідно враховувати те, що координатні функції збалансованого булевого відображення задовольняють певним співвідношенням. Для реалізації такого підходу необхідно, по-перше, розробити ефективний евристичний алгоритм побудови к.і. функції, по-друге, поєднати цей алгоритм з алгоритмом послідовного створення збалансованого булевого відображення.

IV Метод побудови збалансованих S-блоків з властивістю 1-стійкості координатних функцій

Надалі розглянемо алгоритм побудови к.і. функцій, заснований на теоремі про ваги підфункцій к.і. функцій.

Теорема [15]. Збалансована булева функція $f(x_1, x_2, ...x_n)$ є кореляційно-імунною функцією порядку 1 (1-стійкоїою функцією) тоді і тільки тоді, коли $\forall\, i$, $1 \le i \le n$, $\left\| f_i^0 \right\| = \left\| f_i^1 \right\| = 2^{n-2}$, де $\left\| f_i^a \right\|$ – вага Хеммінга підфункції функції f, яка отримана шляхом підстановки значення a замість i-ої змінної.

Іншими словами, для 1-стійкої функції f рівноймовірними є всі підфункції, отримані шляхом фіксації однієї змінної. Як вже вказувалось раніше, такі функції носять назву 1-рівноймовірних функцій.

На першому кроці алгоритму генерується довільна збалансована булева функція f від n змінних. Далі послідовно аналізуються ваги підфункцій $f_1^1, f_2^1, ..., f_n^1$ функции f. У випадку, коли на i-ому кроці $\left\| f_i^1 \right\| \neq 2^{n-2}$, здійснюється $\left| \left\| f_i^1 \right\| - 2^{n-2} \right|$ транспозицій у вектор-стовпці значень функції f. Значения індексів для транспозиції вибираються таким чином, щоб не порушувати збалансованості підфункцій f_j^1, де $j < i$.

Для емпіричної оцінки складності алгоритму здійснена генерація 100 мільйонів 1-стійких функцій від 8 змінних. Гістограма кількості транспозицій наведена на рис. 1. Математичне очікування кількості транспозицій дорівнює 24.

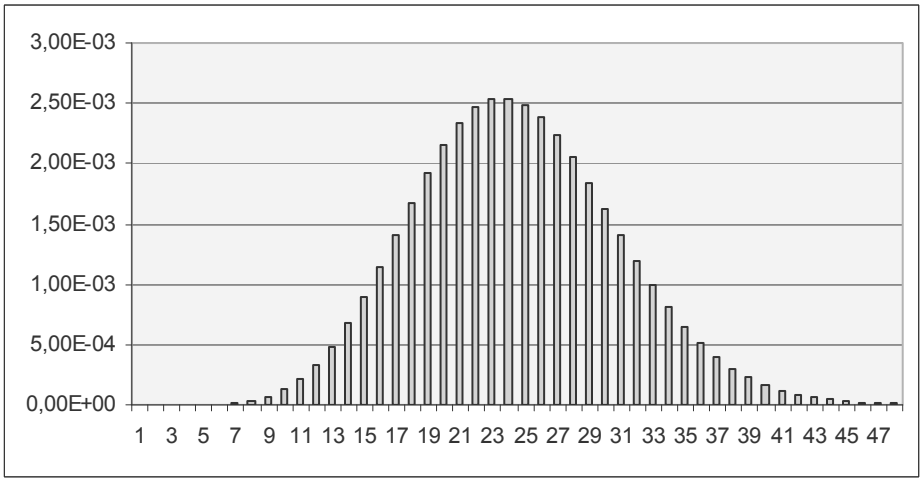

Рисунок 1 – Гістограма кількості транспозицій в алгоритмі побудови 1-стійкої функцій від 8 змінних

Цей метод побудови 1-стійкої функції реалізовано програмно мовою програмування С++. Час генерації одного мільйона 1-стійкої функцій від 8 змінних на ПЕОМ на базі процесора Intel Pentium 4 з частотою 2.4 МГц складає 23 секунди.

Надалі розглянемо метод впровадження цього алгоритму в алгоритм послідовного набору координатних функцій збалансованого булевого відображення. Під час побудови j-ої 1-стійкої координатної функції враховується збалансованість відображення $S^{(1,...j)} = (f_1,...f_j) : V_n \to V_{2^j}$, де $j = \overline{2,n}$.

Первісно генерується 1-стійка функція від n змінних, яка є першою координатною функцією f_1 S-блоку. Надалі за алгоритмом побудови к.і. функції, який описано вище, генерується друга 1-стійка координатна функція f_2 S-блоку, при цьому під час здійснення транспозицій перевіряється вимога збалансованості булевого відображення $S^{(1,2)} = (f_1, f_2) : V_n \to V_4$. Транспозиція здійснюється тільки у випадку, якщо вона не порушує збалансованості булевого відображення $S^{(1,2)}$. Якщо будь-яка з можливих транспозицій призводить до втрати збалансованості булевого відображення $S^{(1,2)}$, здійснюється перехід до першого кроку алгоритму, тобто, генерується нова координатна функція f_1. При успішній генерації функції f_2 здійснюється генерація третьої функції f_3 і т. д. Таким чином, на кроці j, де $j = \overline{2,n}$ генерується 1-стійка функція f_j, при цьому процес генерації гарантує збалансованість відображення $S^{(1,...,j)} = (f_1,..., f_j) : V_n \to V_{2^j}$. Результатом роботи алгоритму є $n \times n$ S-блок, кожна з координатних функцій якого є 1- стійкою булевою функцією.

V Приклад 8×8 S-блоку з властивістю 1-стійкості координатних функцій та аналіз його криптографічних властивостей

Приклад S-блоку, який згенеровано за описаним алгоритмом, наведено нижче. Почнachимо цей S-блок через S_{imm}. У шістнадцятковому записі S_{imm} має вид:

```
ec 6d f9 38 b6 01 f8 ad 9b 2a 13 82 f6 40 c5 a9
70 57 30 87 46 e3 37 be e8 8e fd d1 33 69 04 4f
f7 9d 8a 60 a6 de 58 1c 10 65 25 4a 3f 52 8d e6
21 49 09 db 16 b9 a2 54 4c 71 97 2c dd 7c c1 9a
7a fe 14 c4 83 8f 74 c8 0c bd c3 cb d5 15 06 b1
8b 99 18 05 dc 67 f2 cd c2 bc 6e b2 7b 00 73 88
ff 28 1f 4e 23 9e 50 ab 92 5f b5 62 6b f5 ba 5a
64 a0 47 d3 af 27 6f e1 34 ea 3b 56 24 11 d9 ae
0f 76 cf a7 68 31 e4 12 fa b8 84 9f 2e f1 41 7d
59 80 35 d7 eb 2b 3e e5 42 19 7e d2 03 cc 36 0a
53 2d df b0 ca 26 45 1a a3 4b 75 a8 95 c6 da 39
e0 72 ee 96 8c 9c 20 fb 5e 93 d4 85 0b ed bf 63
b3 51 29 3c 5b 17 c0 6a 1d d6 ef a5 ac 86 78 43
ce 94 3a c7 aa f0 55 5d fc 32 2f 22 c9 44 1b 3d
81 f3 a1 08 66 5c b7 79 4d 61 02 6c d0 1e 90 e7
89 0e 48 77 91 07 d8 98 e9 f4 a4 7f b4 bb 0d e2
```

Розглянемо ряд «криптографічних» параметрів S-блоку, а саме:

- $n_1, n_2, ..., n_8$ – нелінійність координатних функцій (відстань від класу аффінних функцій), $n_j = N(f_j),\ j = \overline{1,8}$, де $N(f) = \min\limits_{l \in A_n} \| f \oplus l \|$, A_n – клас афінних функцій від n змінних [16];
- N – нелінійність S-блоку, $N = N(S) = \min\limits_{a \in V_n \setminus 0,\ b \in \{0,1\}} N(a_1 f_1 \oplus ... \oplus a_n f_n \oplus b)$ [17];
- $d_1, d_2, ..., d_8$ – порядок нелінійності координатних функцій [18];
- v – порядок нелінійності (англ. – nonlinear order) S-блоку – мінімальний порядок нелінійності функцій, які є нетривіальними лінійними комбінаціями координатних функцій [18];
- $\gamma_j = \| g_j \|$, де $j = \overline{1,8}$, g_j – булева функція від n змінних, така, що $S(x) = (x_1 \oplus g_1, ..., x_n \oplus g_n)$;
- e – кількість одиничних циклів (нерухомих елементів) в підстановці, $e = \#\{x \in V_n \mid S(x) = x\}$;
- c – максимальне відхилення від 0.5 для корреляційних коефіцієнтів підстановки,
- $c = \left| 0.5 - \max\limits_{i,j=\overline{1,n}} c_{ij} \right|$, де $c_{ij} = p\left(x_i = 1 \Big/ f_j = 1 \right)$ – кореляційний коефіцієнт між j-м «виходом» та i-м «входом» S-блоку;
- p – кількість елементарних кон'юнкцій, які входять до мінімальних диз'юнктивних нормальних форм всіх координатних функцій.

Для S-блоку, який згенеровано, $n_1 = n_3 = n_4 = n_5 = n_7 = 112$, $n_2 = n_6 = n_8 = 108$, $N = 96$, $d_j = 6$, $\gamma_j = 128$, $j = \overline{1,8}$, $v = 6$, $e = 0$, $c = 0$, $p = 412$.

Значення $N = 96$ відповідає 13 лінійним комбінаціям координатних функцій, зокрема, $f_1 \oplus f_2 \oplus f_5$.

Параметр N може бути обчислено на основі таблиці лінійних апроксимацій (англ. – Linear Approximation Table) S-блоку. Для $n \times n$ S-блоку ця таблиця згідно [19] визначається як матриця розміру $2^n \times 2^n$, в якій елемент з номером (α, β) обчислюється за формулою

$$LAT(\alpha,\beta) = \#\{x \in V_n \mid \bigoplus_{i=1}^{n} x_i\alpha_i = \bigoplus_{i=1}^{n} y_i\beta_i\} - 2^{n-1}, \text{ де } y = S(x).$$

Стовпчик з номером β є статистичною структурою функції $F_\beta = \bigoplus_{i=1}^{n} f_i\beta_i$, тобто функції, яка є лінійною комбінацією координатних функцій S-блоку. Параметр N обчислюється за формулою $N = 2^{n-1} - \max_{\alpha,\beta \in V \setminus \{0\}} |LAT(\alpha,\beta)|$.

У табл. 2 наведені значення $|LAT(\alpha,\beta)|$, їх кількість у таблиці, а також імовірність лінійної апроксимації p_{LA}.

Таблиця 2

$\|LAT(\alpha,\beta)\|$	Кількість	p_{LA}
0	13079	0.5
4	22848	0.515625
8	15524	0.53125
12	8546	0.546875
16	3537	0.5625
20	1114	0.578125
24	296	0.59375
28	68	0.609375
32	13	0.625

Для S-блоків вводиться ще один параметр – λ, який визначається як максимальна за модулем кореляція між лінійними функціями і нетривіальними лінійними комбінаціями координатних функцій S-блоку. Кореляція між булевими функціями f та g визначається за формулою

$$c(f,g) = \frac{\#\{x \in V_n \mid f(x) = g(x)\}}{2^{n-1}} - 1 = 1 - \frac{\|f \oplus g\|}{2^{n-1}}.$$

Праметр λ пов'язаний з параметром N співвідношенням $\lambda = 1 - \frac{N}{2^{n-1}}$. Для S-блоку S_{imm} λ=0.25.

Значення статистичної структури за модулем та їх кількість для координатних функцій S-блоку наведені у табл. 3.

Таблиця 3

	0	4	8	12	16	20
f_1	51	87	60	33	25	0
f_2	58	81	60	35	18	4
f_3	52	79	64	41	20	0
f_4	52	85	60	35	24	0
f_5	50	94	52	34	26	0
f_6	59	76	64	34	21	2
f_7	60	83	46	45	22	0
f_8	57	87	52	42	11	7

Важливість статистичної структури для криптографічних застосувань пояснюється формулою $p(f(x) = (\alpha,x)) = \frac{1}{2} + \frac{\Delta_\alpha}{2^n}$, де Δ_α – значення статистичної структури, (α,x) – лінійна функція, $\alpha = \overline{0,2^n - 1}$. Нелінійність булевої функції та статистична структура пов'язані співвідношенням $N(f) = 2^{n-1} - \max_\alpha |\Delta_\alpha|$.

Значення параметрів d_j, $j=\overline{1,8}$ є максимально можливим для збалансованої кореляційно-імунної функції, тобто в нерівності Зігентайлера досягається рівність, отже, всі координатні функції підстановки S_{imm} є оптимальними двійковими функціями [1]. Для всіх координатних функцій алгебраїчний степінь за будь-якою змінною також дорівнює 6.

Нелінійність п'яти координатних функцій дорівнює 112, що є найкращою оцінкою для нелінійності 1-стійких функцій від 8 змінних, які мають степінь нелінійності 6 [20].

$c_{ij}=0.5$, де $i=\overline{1,8}$, $j=\overline{1,8}$. Як наслідок цього, $c=0$, а також $\gamma_j=128$, $j=\overline{1,8}$.

Показники, які визначають стійкість відносно диференційного методу криптографічного аналізу[21], позначимо через $R_{\oplus\oplus}$, R_{++}, $R_{\oplus+}$, $R_{+\oplus}$. Диференційні характеристики підстановки розглядаються для чотирьох можливих комбінацій операцій додавання за модулем 2 ($\oplus$) та додавання за модулем 2^n (+). Відносно бінарних операцій o_1 та o_2, які задані на V_n, максимальне значення у таблиці різниць підстановки обчислюється за формулою

$$R_{o_1o_2}=\max_{\alpha,\beta\in V_n,\alpha\neq 0}\sum_{x\in V_n} I\{S(x\,o_1\,\alpha)=S(x)\,o_2\,\beta\},\ \text{де } I\{\varepsilon\}\text{ – індикатор події }\varepsilon.$$

Для підстановки S_{imm} $R_{\oplus\oplus}$=10, R_{++}=7, $R_{\oplus+}$=8, $R_{+\oplus}$=9.

Значення у таблиці різниць підстановки (для $R_{\oplus\oplus}$) та їх кількість наведені у табл. 4.

Таблиця 4

Значення	0	2	4	6	8	10
Кількість	39745	19571	4968	869	109	18

Стійкість відносно диференційних методів криптографічного аналізу залежить також від параметра $t=\max_{x\in V_n}(\#\{y\in V_n \mid S(y)\oplus y=S(x)\oplus x\})$. Як приклад, під час побудови S-блоку геш-функції Whirlpool висувалась вимога $t=2$.

Таблиця значень $x\oplus S(x)$ S-блоку S_{imm} має вигляд:

```
0 1 0 1 1 0 1 1 1 1 0 1 0 1 1 1 0 3 1 2 3 1 0 1 0 2 1 0 0 1 1 1
0 1 2 1 2 3 0 1 0 1 1 0 0 3 1 1 0 1 2 0 1 2 2 0 2 1 1 3 1 0 1 0
0 2 0 2 2 1 2 1 3 2 1 1 3 2 0 0 3 2 2 0 0 0 2 0 2 0 0 0 1 1 1 0
2 2 1 1 0 1 0 0 0 0 0 1 2 0 3 1 0 0 2 1 3 0 0 0 1 1 0 0 1 2 3 2
2 0 2 2 2 0 0 2 2 2 1 0 3 0 0 2 1 0 0 2 2 2 3 1 1 2 2 0 0 0 1 3
1 0 1 1 1 2 1 2 3 1 1 0 0 2 0 0 0 0 1 0 1 0 1 1 0 1 1 0 1 1 1 1
0 0 0 1 0 1 0 1 1 2 2 1 1 0 0 1 0 2 1 0 1 1 0 2 0 0 1 2 1 0 0 2
0 1 2 1 1 1 1 1 3 1 0 3 2 0 0 0 1 0 2 3 1 1 1 1 0 1 2 3 0 0 2 3
```

Максимальне значення у таблиці дорівнює 3, отже, $t=3$.

Підстановка S_{imm} є непарною. Порядок підстановки дорівнює 43428. Циклова структура підстановки наведена в табл. 5.

Таблиця 5

Довжина циклу	3	7	11	14	42	47	132
Кількість циклів	1	1	1	1	1	1	1

Значення автокореляційної функції за модулем та їх кількість для координатних функцій S-блоку наведені в табл. 6.

Таблиця 6

	0	8	16	24	32	40	48	56	64	256
f_1	30	81	63	43	25	10	2	0	1	1
f_2	38	63	63	51	22	11	4	1	2	1
f_3	46	76	65	34	21	10	1	2	0	1
f_4	39	81	66	34	17	13	2	2	1	1

	0	8	16	24	32	40	48	56	64	256
f_5	43	71	70	30	21	13	5	2	0	1
f_6	33	70	68	48	16	14	6	0	0	1
f_7	32	88	64	31	21	13	6	0	0	1
f_8	41	71	55	41	18	20	5	2	2	1

Важливість цього параметру для криптографічних застосувань пояснюється формулою $p(f(x) \neq f(x \oplus a)) = \frac{1}{2} - \frac{r(a)}{2^{n+1}}$, де $r(a)$ – значення автокореляційної функції, $a = \overline{0,2^n - 1}$.

Кількість термів у алгебраїчній нормальній формі координатних функцій дорівнює 104, 133, 114, 122, 122, 125, 109, 115 відповідно. Кількість термів у алгебраїчній нормальній формі координатних функцій, які містять змінну x_i, $i = \overline{0,7}$, наведені в табл. 7.

Таблиця 7

	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7
f_1	41	51	51	56	49	49	47	54
f_2	63	64	68	69	66	67	70	68
f_3	49	54	63	58	55	51	54	57
f_4	65	59	63	61	62	55	56	65
f_5	60	65	67	63	52	53	60	60
f_6	63	60	56	59	66	60	66	58
f_7	47	57	52	57	56	55	50	49
f_8	57	52	55	56	56	53	53	62

Кількість термів степеню нелінійності $w = \overline{0,8}$ у алгебраїчній нормальній формі координатних функцій наведена в табл. 8.

Таблиця 8

	0	1	2	3	4	5	6	7	8
f_1	0	5	15	20	28	25	11	0	0
f_2	0	5	15	21	40	35	17	0	0
f_3	1	4	13	25	33	24	14	0	0
f_4	1	3	15	21	37	28	17	0	0
f_5	0	6	12	24	35	32	13	0	0
f_6	1	2	14	29	35	33	11	0	0
f_7	1	3	14	23	29	27	12	0	0
f_8	1	4	11	27	36	23	13	0	0

Коефіцієнт розповсюдження помилки (КРП) для всіх координатних функцій підстановки S_{imm} дорівнює 4. КРП функції f за змінною x_j називається величина $k_j^f = \frac{1}{2^n} \sum_x (f(x) \oplus f(x^j))$, де вектори $x, x^j \in V_n$ відрізняються тільки j-ою координатою. КРП функції f називається величина $K_f = \sum_{j=1}^{n} k_j^f$.Значення КРП координатних функцій за змінною x_i, $i = \overline{0,7}$ наведені в табл. 9.

Таблиця 9

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
x_0	0.515625	0.53125	0.53125	0.625	0.53125	0.5	0.59375	0.515625
x_1	0.546875	0.484375	0.609375	0.53125	0.515625	0.515625	0.53125	0.53125
x_2	0.53125	0.515625	0.515625	0.5625	0.515625	0.546875	0.515625	0.515625
x_3	0.515625	0.546875	0.515625	0.484375	0.453125	0.546875	0.546875	0.515625
x_4	0.5625	0.484375	0.5625	0.453125	0.5	0.59375	0.5625	0.546875
x_5	0.53125	0.515625	0.484375	0.5	0.59375	0.46875	0.5	0.484375
x_6	0.46875	0.53125	0.484375	0.515625	0.53125	0.5625	0.46875	0.5

x_7	0.484375	0.53125	0.515625	0.484375	0.546875	0.5	0.421875	0.5625

Для оцінки кореляційних властивостей S-блоку обчислюються матриця „залежностей" та матриця „відстаней" [22]. Стосовно $n \times n$ S-блоку матриця „залежностей" – це матриця A розміру $n \times n$, елемент a_{ij} якої дорівнює кількості вхідних векторів $x \in V_n$, для яких зміна i-го біта призводить до зміни j-го біта у векторі $y = S(x)$, а матриця „відстаней" – це матриця B розміру $n \times (n+1)$, елемент b_{ij} якої дорівнює кількості вхідних векторів $x \in V_n$, для яких зміна i-го біта призводить до зміни j бітів у векторі $y = S(x)$.

Для S-блоку S_{imm} матриця „залежностей" має вид:

```
132 136 136 160 136 128 152 132
140 124 156 136 132 132 136 136
136 132 132 144 132 140 132 132
132 140 132 124 116 140 140 132
144 124 144 116 128 152 144 140
136 132 124 128 152 120 128 124
120 136 124 132 136 144 120 128
124 136 132 124 140 128 108 144
```

Матриця „відстаней" має вид:

```
0  8 18 42 72 52 54 10 0
0 10 10 46 84 68 22 12 4
0  4 18 42 84 78 22  8 0
0  8 20 50 74 68 30  6 0
0  4 14 54 82 56 32 14 0
0 10 26 50 78 50 28 10 4
0 10 30 34 82 64 32  4 0
0  2 36 62 58 50 42  6 0
```

Згідно [23] ступінь „повноти" d_c обчислюється за формулою $d_c = 1 - n^{-2} \#\{a_{ij} \mid a_{ij} = 0\}$, ступінь „суворого лавинного критерію" d_{sa} – за формулою $d_{sa} = 1 - n^{-2} \sum_{i=1}^{n} \sum_{j=1}^{n} \left| \frac{2a_{ij}}{2^n} - 1 \right|$, ступінь „лавинного ефекту" d_a – за формулою $d_a = 1 - n^{-2} \sum_{i=1}^{n} \left| \frac{1}{2^n} \sum_{j=1}^{m} 2jb_{ij} - n \right|$. Для S-блоку S_{imm} $d_c = 1$, $d_{sa} = 0.931641$, $d_a = 0.956055$.

S-блоку S_{imm} не має лінійної структури, тобто $\bar{\exists} u \in V_n$ такого, що $S(x) \oplus S(x \oplus u) = const$.

За багатьма параметрами S-блок S_{imm}, який згенеровано за описаним методом, не поступається або має кращі показники, ніж S-блоки відомих криптографічних алгоритмів, зокрема, RC2, MD2, Safer+, Crypton, Twofish, Whirlool, CS, Anubis, Snow, Turing, DESX тощо, при цьому 1-стійкість та оптимальність усіх координатних функцій є унікальною властивістю [23].

За виключенням алгоритмів, S-блоки яких побудовані на основі операції x^{-1} у скінченному полі Галуа $GF(2^8)$, кращі показники нелінійності N мають S-блоки криптоалгоритмів Skipjack та BelT.

Слід відзначити, що підстановка S_{imm} утворює клас підстановок з аналогічними властивостями потужності $2^8 8! = 10321920$. З розглянутих параметрів можуть змінюватись тільки параметри e та t. Цей класс утворюється шляхом перестановки координатних функцій підстановки, а також їх інвертуванням.

VI Висновок

Запропонований метод побудови S-блоків з властивістю кореляційної імунності координатних функцій можна використовувати під час синтезу S-блоків криптографічних алгоритмів. Найбільш доцільним є використання таких S-блоків під час побудови потокових шифрів.

Література: ***1.*** *Siegenthaler T. Correlation immunity of non-linear combining functions for cryptographic applications. IEEE Trans. Inform. Theory, Vol.30, 1984. pp. 776-780.* ***2.*** *Денисов О. В. Асимптотическая формула для числа корреляционно-иммунных порядка k булевых функций, Дискретная математика, т. 3., вып. 2, 1991.* ***3.*** *Xiao G. Z. Correlation-immunity of Boolean functions // Electron. Lett. Vol.23. No.25. 1987.* ***4.*** *Yu. V. Tarannikov. On a method for the constructing of cryptographically strong Boolean functions. – Moscow State University, French-Russian Institute of Applied Mathematics and Informatics. Preprint No 6., Moscow, October 1999.* ***5.*** *Webster A. F., Tavers S. E. On the design of S-boxes, Advances in Cryptology, –Proc. Crypto'85, Springer-Verlag, 1986, pp. 523-534.* ***6.*** *Zhang X.-M., Zheng Y. Cryptographically Resilient Functions. // IEEE Trans. on Information Theory. 1997. Vol. 43. 5. pp. 1740-1747.* ***7.*** *Bierbrauer J., Gopalakrishnan K., Stinson D. R. Bounds on Resilient Functions and Orthogonal Arrays. // Advances in Cryptology: Crypto'94/ Lect. Notes in Comput. Sci. Vol. 839. New York: Springer-Verlag. 1994. pp. 247-256.* ***8.*** *Stinson D. R. Resilient Functions and Large Sets of Orthogonal Arrays. // Congressus Numerantium/ Vol. 92. 1993. pp. 105-110.* ***9.*** *Camion P., Carlet C., Charpin P., Sendrier N. On Correlation Immune Functions. // Advances in Cryptology: Crypto'91/ Lect. Notes in Comput. Sci. Vol. 576. New York: Springer-Verlag. 1992. pp. 86-100.* ***10.*** *Chee S., Lee S., Lee D., Sung S. H. On the Correlation Immune Functions and Their Nonlinearity. // Advances in Cryptology: ASIACRYPT'96/ Lect. Notes in Comput. Sci. Vol. 1163. New York: Springer-Verlag. 1996. pp. 232-243.* ***11.*** *Maitra S., Sarkar P. Highly Nonlinear Resilient Functions Optimizing Siegenthaler's Inequality. // Advances in Cryptology: Crypto'99/ Lect. Notes in Comput. Sci. Vol. 1666. New York: Springer-Verlag. 1999. pp. 198-215.* ***12.*** *Seberry J., Zhang X.-M., Zheng Y. On the Constructions and Nonlinearity of Correlation Immune Boolean Functions. // Advances in Cryptology: EUROCRYPT'93/ Lect. Notes in Comput. Sci. Vol. 765. New York: Springer-Verlag. 1994. pp. 181-199.* ***13.*** *Carlet C. Partially-bent functions. // Designs Codes and Cryptography. 1993. 3. pp. 135-145.* ***14.*** *Filiol E., Fontaine C. Highly Nonlinear Balanced Boolean Functions with a Good Correlation-Immunity. // Advances in Cryptology: EUROCRYPT'98/ Lect. Notes in Comput. Sci. Vol. 1403. New York: Springer-Verlag. 1998. pp. 475-488.* ***15.*** *Millan W., Clark A., Dawson E. Heuristic Design of Cryptographically Strong Balanced Boolean Functions. // Advances in Cryptology: EUROCRYPT'98/ Lect. Notes in Comput. Sci. Vol. 1403. New York: Springer-Verlag. 1998. pp. 489-499.* ***16.*** *Maitra S. Correlation Immune Boolean Functions with Very High Nonlinearity. // http://www.eprint.iacr.org No. 2000/054.* ***17.*** *Serf P. The degrees of completeness of avalanche effect and of strict avalanche criterion for MARS, RC6, Rijndael, Serpent and Twofish with reduct number of rounds. Siemens AG, ZT IK 3, April3, 2000.*

УДК 681.3

ОЦІНКА ЗАГРОЗ В РОЗПОДІЛЕНИХ МЕРЕЖАХ

Вячеслав Василенко

Національний авіаційний університет

Анотація: **Розглядаються питання захисту інформаційних ресурсів комунікаційної мережі зв'язку розподіленої обчислювальної мережі, наводяться характеристики й механізми реалізації загроз в розподілених мережах, наводиться їх класифікація і пропонується модель загроз.**

Summary: **The questions of defense of informative resources of communication network of the distributed computer network are examined, description and mechanisms of realization of threats in the distributed networks is pointed, their classification is pointed and the model of threats is offered.**

Ключові слова: **Загроза, порушник, ресурси, модель. комунікаційна мережа.**

Вступ

Розподілену обчислювальну мережу (РОМ) будемо розглядати як таку, яка складається з територіально рознесених програмно-технічних комплексів (ПТК) – вузлів РОМ, що входять до складу структурних підрозділів відомства (корпорації) і забезпечують функціонування РОМ. Будемо вважати, що структурно РОМ є ієрархічною трьохрівневою автоматизованою системою, в якій визначаються центральний, регіональний і місцевий рівні. В свою чергу, вузли різних рівнів РОМ взаємодіють між собою за визначеними правилами (протоколами) та технологією.

Основною особливістю такої розподіленої системи є те, що її компоненти розподілені в просторі й зв'язок між ними здійснюється фізично за допомогою мережних з'єднань і програмно за допомогою механізму повідомлень. При цьому всі управляючі повідомлення й дані, що пересилаються між об'єктами розподіленої обчислювальної системи, передаються мережними з'єднаннями в вигляді пакетів обміну. Ця