MATERIAŁY V MIĘDZYNARODOWEJ NAUKOWI-PRAKTYCZNEJ KONFERENCJI

«EUROPEJSKA NAUKA XXI POWIEKĄ – 2009»

07 - 15 maja 2009 roku

Volume 11
Matematyka
Nowoczesne informacyjne technologie
Fizyka

Przemyśl
Nauka i studia
2009

MATERIAŁY

V MIĘDZYNARODOWEJ NAUKOWI-PRAKTYCZNEJ KONFERENCJI

«EUROPEJSKA NAUKA XXI POWIEKĄ – 2009»

07 - 15 maja 2009 roku

Volume 11
Matematyka
Nowoczesne informacyjne technologie
Fizyka

Przemyśl
Nauka i studia
2009

Wydawca: Sp. z o.o. «Nauka i studia»

Redaktor naczelna: Prof. dr hab. Sławomir Górniak.

Zespół redakcyjny: dr hab.Jerzy Ciborowski (redaktor prowadzący), mgr inż. Piotr Jędrzejczyk, mgr inż Zofia Przybylski, mgr inż Dorota Michałowska, mgr inż Elżbieta Zawadzki, Andrzej Smoluk, Mieczysiaw Luty, mgr inż Andrzej Leśniak, Katarzyna Szuszkiewicz.
Redakcja techniczna: Irena Olszewska , Grażyna Klamut.
Dział spredaży: Zbigniew Targalski

Adres wydawcy i redacji:
37-700 Przemyśl , ul. Łukasińskiego 7
tel (0-16) 678 33 19
e-mail: praha@rusnauka.com

Druk i oprawa:
Sp. z o.o. «Nauka i studia»

Cena 54,90 zł (w tym VAT 22%)

Materiały V Międzynarodowej naukowi-praktycznej konferencji «Europejska nauka XXI powieką - 2009»
Volume 11. Matematyka. Nowoczesne informacyjne technologie. Fizyka.: Przemyśl. Nauka i studia - 112 str.

W zbiorze ztrzymają się materiały V Międzynarodowej naukowi-praktycznej konferencji «Europejska nauka XXI powieką - 2009».
07 - 15 maja 2009 roku po sekcjach: Matematyka. Nowoczesne informacyjne technologie. Fizyka

ISBN 978-966-8736-05-6

Разумеется, просто привлечь посетителей – недостаточно. Во-первых, необходимо привлекать посетителей целевых, то есть тех, которые с относительно высокой долей вероятности конвертируются в покупателей. Во-вторых, необходимо создать условия, максимально содействующие конверсии посетителей в покупателей. Наконец, в большинстве случаев очень важно обеспечить определенный уровень приверженности – чтобы ваши покупатели возвращались к вам вновь и вновь. Но без широкого и хорошо регулируемого потока целевых посетителей это бессмысленно.

В грядущем столетии всем так или иначе придется иметь дело с сетевыми и информационными технологиям. И от понимания того, какие задачи намерена решать компания, приобретая средства доступа в Интернет, структурированные кабельные системы, серверы, рабочие станции и программное обеспечение, зависит, насколько успешным будет ее бизнес, основы которого, несмотря ни на что, остаются прежними.

Юпин Р.Є., Дахно С.В., Черненко Р.В., Рудаков К.С.
Черкаський державний технологічний університет, Україна

ОБРАЗНО-ЗНАКОВА МОДЕЛЬ ЗАХИСТУ ІНФОРМАЦІЇ НА БАЗІ ВДОСКОНАЛЕНОГО МЕТОДУ ПЕРЕСТАНОВКИ

Швидкий ріст новітніх інформаційних технологій обумовлює створення нових ефективних засобів захисту інформації, які будуть більш стійкими до вторгнень та завад.

Існує багато методів та засобів захисту інформації програмної та апаратурної реалізації. Питанням побудови надійних засобів захисту інформації присвячено ряд робіт А.А. Молдовяна, Н.А. Молдовяна, Н.Д. Гуца, Б.В. Ізотова, В.А. Герасименко, А.Н. Шніперова та ін.[1-3]. Проте розвиток сучасної мікро-, нанотехнологій дозволяє переглянути існуючі методи та засоби захисту інформації з метою їх вдосконалення.

В таблиці 1 наведені найбільш розповсюджені та прості в реалізації методи захисту інформації, їх принципи побудови та відображено основні характеристики, що знижують захищеність інформації.

Таблиця 1

Основні сучасні методи захисту інформації

Метод захисту інформації	Принцип побудови	Характеристики, які знижують захищеність інформації
Символьної заміни або підстановки	Символи вхідного тексту заміняються на символи іншого (або того ж) алфавіту за заздалегідь визначеною схемою, яка і слугує ключем даного шифру	- одні й ті ж статистичні характеристики оригінального та зашифрованого повідомлень
Символьної перестановки	Символи оригінального тексту міняються місцями за визначеним принципом, що являється таємним ключем	- збільшення об'єму пам'яті; - однотипний алгоритм перестановки
Гамування	Символи вхідного тексту складаються з символами деякої псевдовипадкової послідовності (ПВП)	- збільшення інтервалу часу для генерації зашифрованої інформації, збільшує імовірність появи помилок

З таблиці видно, що інтерес представляє метод перестановки. А.Н. Шніперовим було запропоновано метод керованої перестановки двох розрядів, який достатньо простий в реалізації.

При цьому імовірність розкриття одного байта зашифрованого сигналу можна визначити за формулою [4 – 5].

$$\begin{aligned} P(n) &= p(n)^m \\ p(n) &= \frac{1}{N} \\ N &= P_n = n! \\ m &= \frac{8}{n} \end{aligned}, \qquad (1)$$

де $P(n)$ – імовірність розкриття одного байту, n – кількість розрядів, що переставляються одним блоком, $p(n)$ – імовірність розкриття одного блоку, N – кількість перестановок, що реалізує один блок, m – кількість блоків, що використовуються для шифрування одного байта.

Для метода [3] керованої перестановки двох розрядів імовірність розкриття згідно формули (1) становить

$$P(2) = \left(\frac{1}{2!}\right)^{\frac{8}{2}} = \left(\frac{1}{2}\right)^4 = \frac{1}{16} = 0{,}0625 \qquad (2)$$

З формули (2) видно, що величина імовірності має недостатній рівень для забезпечення захисту інформації.

Тому на основі аналізу методів захисту інформації (табл. 1) пропонується вдосконалений метод, що включає сукупність деяких принципів символьної перестановки та гамування, а засобами є нові елементи (рис. 1), що забезпечують керування в часі перестановкою вхідної інформації $x_1, \ldots, x_4$.

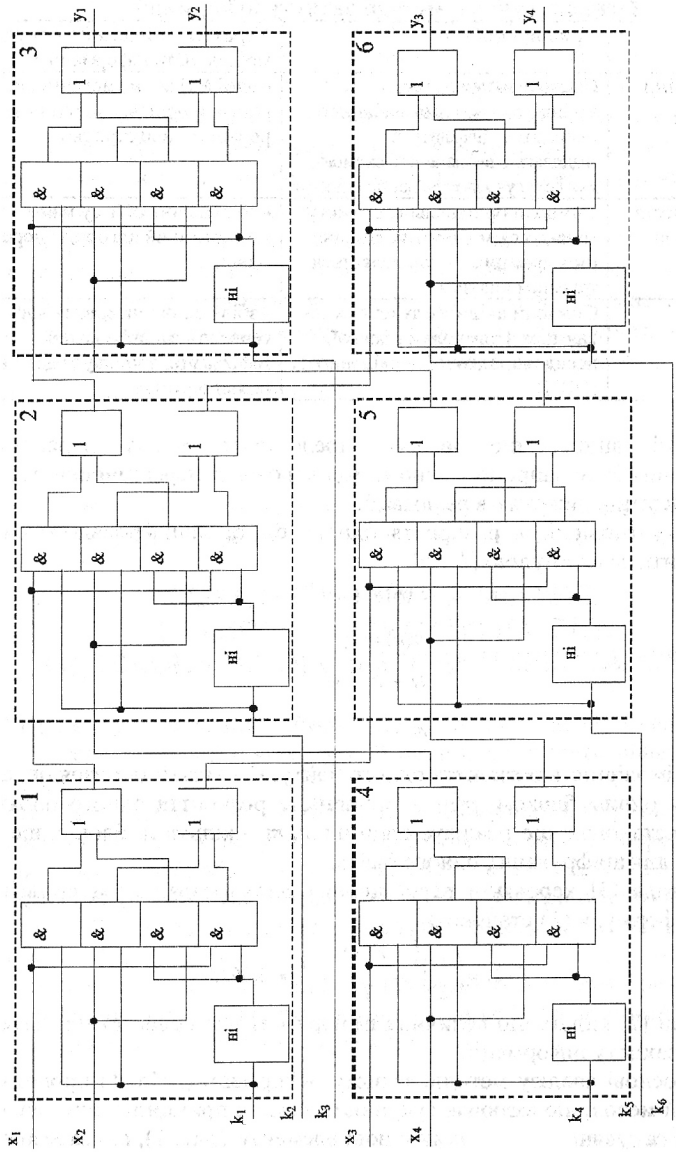

Рисунок 1 – Образно-знакова модель керованої перестановки чотирьох розрядів

Вдосконалення дає можливість змінювати порядок перестановки розрядів $x_1,\ldots, x_4$ завдяки керуванню в часі ключовою інформацією $k_1,\ldots, k_6$.

В приведеній схемі перестановкою вхідних розрядів $x_1,\ldots, x_4$ керують розряди ключової інформації $k_1,\ldots, k_6$. Кожен розряд ключової інформації керує окремим блоком перестановки 1,..., 6 відповідно. Наприклад, при надходженні на розряд ключової інформації k_1 логічної одиниці вихідна інформація x_1, x_2 даного блоку 1 буде еквівалентною вхідній інформації x_1, x_2. В протилежному випадку відбудеться перестановка цих розрядів, тобто вихідною інформацією блоку 1 буде відповідно x_2, x_1.

Залежність вихідних інформаційних сигналів образно-знакової моделі керованої перестановки чотирьох розрядів приведено в формулі:

$$\begin{cases} y_1 = x_1k_1k_2k_3 \vee x_2\overline{k_1}k_2k_3 \vee x_3\overline{k_2}k_3k_4 \vee x_4\overline{k_2}k_3\overline{k_4} \vee \\ \quad \vee x_2k_1\overline{k_3}k_5 \vee x_1\overline{k_1}\,\overline{k_3}k_5 \vee x_4\overline{k_3}k_4\overline{k_5} \vee x_3\overline{k_3}\,\overline{k_4}\,\overline{k_5} \\ y_2 = x_2k_1k_3k_5 \vee x_1\overline{k_1}k_3k_5 \vee x_4k_3k_4\overline{k_5} \vee x_3k_3\overline{k_4}\,\overline{k_5} \vee \\ \quad \vee x_1k_1k_2\overline{k_3} \vee x_2k_1k_2\overline{k_3} \vee x_3k_2\overline{k_3}k_4 \vee x_4k_2k_3\overline{k_4} \\ y_3 = x_3k_2k_4k_6 \vee x_4k_2\overline{k_4}k_6 \vee x_1k_1\overline{k_2}k_6 \vee x_2\overline{k_1}\,\overline{k_2}k_6 \vee \\ \quad \vee x_4k_4k_5\overline{k_6} \vee x_3\overline{k_4}k_5\overline{k_6} \vee x_2k_1\overline{k_5}\,\overline{k_6} \vee x_1\overline{k_1}k_5\overline{k_6} \\ y_4 = x_4k_4k_5k_6 \vee x_3\overline{k_4}k_5k_6 \vee x_2k_1\overline{k_5}k_6 \vee x_1\overline{k_1}k_5k_6 \vee \\ \quad \vee x_3k_2k_4\overline{k_6} \vee x_4k_2\overline{k_4}\,\overline{k_6} \vee x_1k_1\overline{k_2}\,\overline{k_6} \vee x_2\overline{k_1}\,\overline{k_2}\,\overline{k_6} \end{cases} \qquad (3)$$

Варто відзначити, що вихідний інформаційний сигнал зчитується в короткий проміжок часу Δt, це забезпечує виграш в $T/\Delta t$ разів, де T – час спостереження.

Використовуючи формулу (1) визначаємо імовірність розкриття одного байта для керованої перестановки чотирьох розрядів.

$$P(4) = \left(\frac{1}{4!}\right)^{\frac{8}{4}} = \left(\frac{1}{24}\right)^2 = \frac{1}{576} \approx 0{,}001736 \qquad (4)$$

Ефективність запропонованої моделі можна оцінити з порівняння результатів розрахунків за формулами (2) і (4)

$$P(2)/P(4) = 0{,}0625/0{,}00174 \approx 36 \qquad (5)$$

Отже імовірність розкриття інформації в один байт для запропонованої моделі зменшується в 36 разів.

Крім того, запропонована образно-знакова модель на базі вдосконаленого методу забезпечує:

- підвищення криптостійкості системи за рахунок збільшення кількості розрядів для перестановки;
- отримання виграшу в $T/\Delta t$ разів;
- однорідність модульності структури спрощує процеси виготовлення, тестування, ремонту та підвищує відсоток виходу придатних кристалів, що зменшує загальну собівартість пристрою.

Литература:

1. Криптография. Скоростные шифры. / А. А. Молдовян, Н. А. Молдовян, Н. Д. Гуц, Б. В. Изотов – СПб.; БХВ, 2002. – 293 с.

2. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. – М.: Энергоатомиздат, 1994. – 576 с.

3. Шниперов А.Н. Использование управляемых битовых перестановок в криптографии / Научно-практический журнал «Информационное противодействие угрозам терроризма» №4, 2005. – С. 154-158.

4. М.Ф. Бондаренко, Н.В. Білоус, А.Г. Руткас. Комп'ютерна дискретна математика: Підручник / Харків: «Компанія СМІТ», 2004 – 480 с.

5. А.М. Яглом, И.М. Яглом. Вероятность и информация. Главная редакция физико-математической литературы издательства «Наука», 1973.

Герасимов К.О., Ябанжи С.С., Кравченко Н.М.
Київський Національний авіаційний університет, Україна

ПЛАНУВАННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ МЕРЕЖІ

З метою технічного забезпечення системи диференційованого обслуговування з гарантованим сервісом у ТЛК-системах загального користування створюється та підтримується в актуальному стані **служба підтримки якості обслуговування** (служба QoS). Головне призначення цієї служби – забезпечувати пріоритезацію різних видів трафіка, необхідну смугу пропускання для них, керування величинами затримок та варіацій затримок протокольних блоків даних (PDU), а також зменшення відсотку втрат PDU під час передавання.

Для того щоб потоки трафіка обслуговувалися мережею з максимально можливою ефективністю, необхідно виконувати певну попередню роботу щодо вибору та інсталяції параметрів обладнання мережі з урахуванням умов, що містяться в сервісних угодах – як тих, що вже набули чинність, так і тих, що плануються до реалізації. Таку роботу називають «планування роботи мережі».

Планування роботи мережі починають з аналізу сервісних угод. Під час такого аналізу слід визначити:

1) усі користувальницькі потоки даних та їхні можливі маршрути;

SPIS

MATEMATYKA

DYFERENCJALNE I INTEGRALNE ZRYWNANIE

TEORIA PRAWDOPODOBIECSTW I MATEMATYCZNA STATYSTYKIEM

STOSOWANA MATEMATYKA

MATEMATYCZNE MODELOWANIE

NOWOCZESNE INFORMACYJNE TECHNOLOGIE

KOMPUTEROWA INŻYNIERIJA

OBLICZENIOWA TECHNIKA I PROGRAMOWANIE

PROGRAMOWE ZABEZPIECZENIE

INFORMACYJNE BEZPIECZECSTWO

FIZYKA

FIZYKA CIAŁA STAŁEGO

OPTYKA