УДК 004.021:004.027:004.6:004.77

[1]**А. О. Ігнатович,** [2] **Р.-А. Д. Іванців,** [3]**Н. Я. Павич**
Національний університет "Львівська політехніка",
[1]кафедра електронних обчислювальних машин,
[2] кафедра систем автоматизованого проектування,
[3] кафедра програмного забезпечення

КРИТЕРІЙ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ КОМПОНЕНТІВ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ

Проаналізовано сучасний стан оцінювання ефективності компонентів безпеки комп'ютерних систем та мереж. Встановлено, що таке оцінювання ефективності все ще недостатньо забезпечене фундаментальною теорією та методологією і значною мірою суб'єктивне. Запропоновано використання узагальненого критерію ефективності. Розглянуто технологію використання такого критерію на тестовому прикладі для блокових шифрів. Показано, що використання запропонованого критерію підвищує об'єктивність оцінювання ефективності компонентів безпеки комп'ютерних систем та мереж.

Ключові слова: оцінювання ефективності, критерій ефективності, компоненти безпеки, комп'ютерні системи.

[1]**A. Ihnatovych,** [2]**R. Ivantsiv,** [3]**N. Pavych**
Lviv Polytechnic National University,
[1]Computer Engineering Department
[2]Department of Computer-Aided Design
[3]Department of Software

EFFICIENCY EVALUATION CRITERION OF SECURITY COMPONENTS OF COMPUTER SYSTEMS

Current situation of efficiency evaluation of security components of computer systems and networks is analyzed. It is founded that mentioned in the article effectiveness assessment methods are not sufficiently provided with fundamental theory and methodology and to great extent are subjective. Usage of generalized efficiency evaluation criterion is proposed. Methodology of usage of such criterion on the test case with block ciphers is overviewed. In the article is shown that usage of the proposed criterion increases the objectivity of the process of the efficiency evaluation of security components of computer systems and networks.

Key words: efficiency evaluation, criterion for evaluating the effectiveness, security components, computer systems.

Вступ

Сучасне застосування комп'ютерних систем та мереж сприяє виконанню величезної кількості процесів обміну інформацією. У багатьох випадках необхідно забезпечувати такі режими обміну інформацією, щоб вона була доступною обмеженому колу користувачів, тобто необхідно

забезпечувати безпеку інформації. Реалізація цієї проблеми покладається на компоненти безпеки комп'ютерних систем та мереж. Відомо багато методів захисту інформації [1–3], однако під час вибору конкретних компонентів безпеки для певного прикладного застосування виявляється багато проблем. У кожному конкретному випадку є свої особливості застосування методів та засобів захисту інформації і виникає проблема оцінювання їх ефективності. Загальновизнані універсальні критерії оцінювання ефективності компонентів безпеки поки що відсутні. Тому актуальні дослідження, спрямовані на формулювання узагальнених критеріїв ефективності компонентів безпеки.

Аналіз останніх досліджень та публікацій

Під інформаційною безпекою переважно розуміють захищеність інформації та телекомунікацій від випадкових або навмисних дій, природних чи штучних, що можуть завдати неприйнятних збитків суб'єктам інформаційних відносин [1–3]. Захист інформації – це комплекс заходів, спрямованих на забезпечення інформаційної безпеки. Оцінювання ефективності компонентів безпеки комп'ютерних систем та мереж сьогодні недостатньо забезпечене фундаментальною теорією та методологією і значною мірою суб'єктивне. Для оцінювання ефективності засобів захисту інформації найчастіше використовують фактор, який характеризує складність зламування використаного методу шифрування. Тоді за критерій ефективності можна прийняти час, потрібний для прочитання шифрованого тексту і знаходження ключа шифрування [1–3]. У таких випадках необхідно буде враховувати обсяг шифрованого тексту, кваліфікацію криптографа, що складно реалізувати практично. Для порівняльної характеристики використовуваних заходів шифрування інформації запропоновано оцінювати зменшення середнього інтегрального відхилення частоти вживання символів [4–7]. Однак такий підхід не можна вважати універсальним, оскільки він реалізовує оцінювання тільки одного показника. Аналіз ефективності захисту інформації на основі криптографічних перетворень з використанням маскованого подання даних [8] також є частковим і використовує один показник. Трапляються й інші пропозиції – використовувати для порівняння продуктивність шифрування, зручність, вартість, яка витрачається на шифрування інформації, збитки у разі, якщо зловмисник прочитає інформацію. Поки що недостатньо досліджено методологію об'єднання різних показників ефективності в узагальнений критерій ефективності, який з достатньою мірою повноти міг би оцінювати якість безпеки конкретної комп'ютерної системи.

Мета статті

Мета досліджень – окреслити універсальні підходи до оцінювання ефективності компонентів безпеки комп'ютерної системи і запропонувати узагальнений критерій ефективності, який можна використовувати в різних прикладних задачах.

Основні результати дослідження

Оцінювання будь-якого технічного параметра комп'ютерної системи є найоб'єктивнішим, коли результатом є числова величина. Для багатьох параметрів таке оцінювання методологічно складне, а в окремих випадках неможливе. Оцінювання ефективності компонентів безпеки комп'ютерних систем можна зарахувати до методологічно складних.

Оцінювання ефективності доцільно виконувати для однотипних компонентів безпеки комп'ютерних систем, оскільки воно дещо спрощує методологію та може надати об'єктивні результати. В літературних джерелах фахівці оцінюють ефективність шифрувальної системи за кількістю варіантів ключа, який може забезпечити ця система. В деяких випадках розраховують час для "зламування" шифрувальної системи за умови використання сучасних технічних і програмних засобів. Оскільки технічні параметри обчислювальних і математичних засобів змінюються швидше, ніж публікують такі результати, то зрозуміло, що бажано знайти такі підходи для оцінювання ефективності, які не залежали би від часу, стану обчислювальної техніки, інших факторів впливу. В деяких випадках рекомендовано враховувати вартість "зламування" порівняно із вартістю закритої

інформації. Складність задачі – знайти універсальний підхід до визначення ефективності – полягає ще в тому, що, формуючи оцінки, необхідно об'єднати в один критерій різні параметри за природою, розмірністю, фізичними величинами.

Запропоновано використовувати такі параметри, як показники ефективності та критерій ефективності. За такого підходу показник визначає часткову ефективність, критерій – узагальнену, повну ефективність. Тоді повну ефективність компонентів безпеки можна оцінювати за узагальненим критерієм ефективності E як функцією певної сукупності показників ефективності E_i

$$E = f(E_i) \quad , \quad i = \overline{1,n} \ ,$$

де n – загальна кількість показників ефективності, за якими оцінюється узагальнений критерій ефективності.

Поки що відсутній загальноприйнятий та уніфікований аналітичний вираз для обчислення критерію ефективності компонентів безпеки комп'ютерних систем. Одним із варіантів такої оцінки може бути вираз

$$E = \left(\sum_{j=1}^{n} E_j \right) : n \quad , \quad j = \overline{1,n} \ ,$$

де E_j – параметр, що визначається як відносна нормована величина j-го показника ефективності, що може прямувати до максимального значення 1.

Нормований показник ефективності можна обчислити за виразом:

$$E_j = E_{jo} : E_{jm.}$$

де E_{jo} – оцінений j-й показник ефективності для конкретного засобу безпеки; E_{jm} – максимальне (чи оптимальне) значення j-го показника ефективності.

Показники ефективності можуть бути прямими, коли збільшення їх значення приводить до покращення ефективності, чи інверсними, якщо зменшення їх значення сприяє поліпшенню ефективності компонентів безпеки. Тому, оцінюючи ефективність, потрібно погоджено використовувати прямі чи обернені значення відповідних показників ефективності.

До найпоширеніших показників ефективності компонентів безпеки можна зарахувати: E_1 – надійність використаних засобів; E_2 – стійкість криптографічних засобів; E_3 – продуктивність у роботі із засобами безпеки; E_4 – оцінку зменшення середнього інтегрального відхилення частоти вживання символів для запропонованих засобів захисту; E_5 – ймовірність зменшення частоти повторень у шифрованому тексті, які відповідають повторенням відкритого тексту; E_6 – кількість можливих варіантів ключів; E_7 – відношення вартості засобів безпеки до вартості захищеного продукту.

Розглянемо основні особливості цих показників:

E_1 – надійність використаних засобів визначається використаним алгоритмом роботи елементів захисту, доступом до його модифікацій, складністю математичних перетворень, простотою використання (унеможливлення помилок у роботі). E_2 – стійкість криптографічних засобів визначається часом, за яким можна відкрити ключ і шифрований текст за допомогою доступних засобів (обчислювальних засобів, програмного забезпечення, кваліфікованих спеціалістів). E_3 – продуктивність роботи із засобами безпеки визначається часом, який витрачає оператор на застосування засобів безпеки. E_4 – оцінка зменшення середнього інтегрального відхилення частоти вживання символів для запропонованого засобу захисту. E_5 – ймовірність зменшення частоти повторень у шифрованому тексті, які відповідають повторенням відкритого тексту. E_6 – кількість можливих варіантів ключів визначає значною мірою стійкість криптографічних засобів, однак за завищених можливостей їх реалізація стає проблемною, а обмежена кількість ускладнює вибір ключів за певними правилами. E_7 – відношення вартості засобів безпеки до вартості захищеного продукту визначається кількістю криптографів, що працюють, вартістю додаткової апаратури, часу, витраченого на виконання захисних функцій.

Окрім перерахованих показників, є ще декілька величин, які варто аналізувати під час вибору інструментів захисту інформації. Важливий параметр – швидкість зміни ключів на боці як

передавача, так і приймача (з урахуванням проблем синхронізації використовуваних ключів). Також необхідно враховувати вимоги до параметрів апаратної частини, наприклад для ПК та серверів – об'єм оперативної пам'яті, операційну систему, швидкодію, прикладне математичне забезпечення тощо. В деяких випадках необхідно враховувати обсяг трудозатрат під час підготовки даних. Отже, тільки в кожному конкретному випадку можна говорити про пріоритети й ефективні параметри, які необхідно аналізувати і враховувати.

Без сумніву, кожний окремий випадок застосування компонентів безпеки має свої особливості. Оцінюючи ефективність, можна виключати деякі параметри, які не мають великої ваги для конкретної ситуації, або додавати важливіші. Доцільно розглядати різні підходи зі зведенням параметрів, які впливають на ефективність, до одного логічного ряду. Ці підходи (нормованість показників ефективності, різні залежності, "дзеркальна інверсія", "мультиплікативна інверсія", вживання рівнів пріоритету, використання методу експертних оцінок...) дають можливість оцінювати в одному ряді величини, які на перший погляд несумісні.

Отже, ефективність – це складний параметр і його використання для класифікації ефективності компонентів безпеки потребує конкретизації багатьох параметрів. У деяких умовах стійкість засобів захисту може визначатися десятками секунд, чи хвилин, або годин. В інших – десятками і сотнями років. За великих обсягів роботи велике значення має продуктивність компонентів безпеки, а в інших випадках перевагу надають стійкості.

У разі використання тих самих засобів захисту в різних умовах експлуатації їх критерій ефективності буде відрізнятися. Пріоритети повинен надавати замовник, котрий їх використовує, і його оцінки мають переважати. Тільки замовник надає перевагу засобам безпеки і самостійно визначає міру їх ефективності для виконання завдання захисту.

Отже, використання пріоритетів замовника вирішальне, оскільки тільки він може визначити, наскільки підходять засоби безпеки для розв'язання задачі, і як ця задача в результаті розв'язана.

З урахуванням пріоритетів замовника критерій ефективності засобів безпеки можна оцінювати за таким виразом

$$E = \left(\sum_{j=1}^{n} P_j \cdot E_j \right) : n \ , \ j = \overline{1,n},$$

де p_j – рівень пріоритету замовника (p_j може змінюватися від 0 до 1 і надавати перевагу тим елементам ефективності, які є найпріоритетнішими); n – кількість врахованих показників.

Визначення ефективності є достатньо об'єктивним у разі порівняння оцінювального засобу з відомим пристроєм шифрування. Але є деякі початкові умови, які бажано виконати під час оцінювання. Це однаковий відкритий текст, алгоритми шифрування одного класу, використання аналогічних технічних засобів (комп'ютери, операційні системи, прикладні програми...).

Методологію використання узагальненого критерію ефективності розглянемо на прикладі визначення ефективності пристрою шифрування з маскувальними елементами [7]. Аналогом взято пристрій, який використовує класичний метод шифрування Хілла з форматом і ключем, які використані в досліджуваному пристрої, а також однаковими рівнями пріоритету [4–7].

Оцінимо ефективність пристрою шифрування з маскувальними символами [4–7] (формат 3х3, режим використання маскувальних символів статичний, формат $\{v_i; m_i; v_i;\}$, де m_i – маскувальний символ, v_i – символ ВТ (відкритого тексту) за такими параметрами: E_1 – надійність використаних засобів, E_2 – стійкість криптографічних засобів, E_3 – продуктивність користувача під час роботи із засобами безпеки, E_4 – оцінка зменшення середнього інтегрального відхилення частоти вживання символів для запропонованих засобів захисту, E_5 – ймовірність зменшення частоти повторень у шифрованому тексті, які відповідають повторенням відкритого тексту.

$$E = (p_1 * E_1 + p_2 * E_2 + p_3 * E_3 + p_4 * E_4 + p_5 * E_5) : 5.$$

Для розрахунку використаємо такі експертні значення рівнів пріоритету замовника: p_1 – 0,5, p_2 – 0,9, p_3 – 0,7, p_4 – 0,6, p_5 – 0,5.

Під час розрахунку надійності використаних засобів враховують такі параметри (надійність використаних засобів визначається алгоритмом роботи елементів захисту, доступом до його

модифікацій, складністю математичних перетворень, простотою використання, недопущенням помилок у роботі), які не завжди можна розрахувати, в цьому випадку варто використати метод експертних оцінок. Якщо залучити сім експертів і їхні оцінки параметра надійності: 0,4, 0,4, 0,5, 0,7, 0,7 0,8, 0,8, то експертна оцінка буде такою

$$E_1 = (0{,}4 + 0{,}4 + 0{,}5 + 0{,}7 + 0{,}7 + 0{,}8 + 0{,}8) : 7 = 0{,}61.$$

Під час розрахунку стійкості криптографічних засобів (E_2) розраховуємо максимальну кількість можливих варіантів ключів. Для формату 3х3 кількість можливих символів, які можуть використовуватися – 26 (кількість символів англійського алфавіту) за дев'яти символів у одному ключі. В цьому випадку кількість можливих варіантів буде $A_n^k = (n!) : (n – k)!$.

$$k = 9,\ n = 26.\ A_{26}^{9} = (26!) : (26 – 9)! = 19 \cdot 10^{12}.$$

Якщо відкинути всі "небажані" комбінації (комбінації, які складаються з усіх однакових цифр, вилучити матриці, які не мають оберненої, тощо), то кількість комбінацій може істотно зменшитись. І в разі використання всього 0,01 % можливої кількості комбінацій їх кількість для цього формату буде близько $2 \cdot 10^8$.

У разі використання маскувальних елементів кількість можливих комбінацій істотно збільшиться. Мінімально ця величина збільшиться на порядок. Отже, для повного перегляду всіх можливих ключів необхідно перебрати достатньо велику кількість комбінацій. Якщо використати як інструмент комп'ютер з аналізом біграм, триграм і пошуком ймовірних слів за допомогою їх порівняння зі словником, то цей процес може тривати доволі довго. Для однієї комбінації (вибір ключа, дешифрація 80–100 символів, порівняння їх з можливими словами зі словника) необхідно витратити 3–5 секунд. Для повного перебору всіх можливих комбінацій необхідно витратити $(20 \cdot 10^9 \cdot 3) = 60 \cdot 10^9$ секунд. Якщо врахувати, що, ймовірно, розв'язок буде на середній комбінації, можна допустити, що ключ буде знайдений за $30 \cdot 10^9$ секунд. Це час близько 30 тисяч років. Це теоретична прямолінійна оцінка. Сучасні підходи з використанням спеціалізованих груп та криптоаналітиків, які працюють погодженими алгоритмами в спільному полі пошуку, можуть істотно скоротити розв'язання задачі.

Якщо врахувати, що перший матричний алгоритм шифрування реалізовано в форматі 6х6, а для сьогоднішніх комп'ютерних засобів формат 8×8, 9×9 чи 10×10 цілком реальний, то очевидно, що можна досягти значних показників стійкості. Тому вибираємо для нашого випадку максимальний коефіцієнт – 0,99.

E_3 – продуктивність користувача під час роботи із засобами безпеки доволі висока. Якщо раніше доводилось використовувати "ручну" технологію, то використання комп'ютерної техніки забезпечує високі показники під час шифрування і дешифрування. Тому цей коефіцієнт також буде максимальним – 0,99.

E_4 – оцінку зменшення середнього інтегрального відхилення частоти вживання символів [5] для запропонованих засобів захисту розраховують за формулою:

$$s = \left[\frac{1}{2}\sum_{i=1}^{n}\frac{(x_{imax} - x_i)}{x_{imax}}\right] \times 100\ \%,$$

де x_i – статистичний параметр для і-го символу тексту, який виражається кількістю випадків використання символу в досліджуваному тексті; x_{imax} – максимальне значення x_i для символу, який найчастіше трапляється у досліджуваному тексті.

Для формату 3х3 отримано середнє інтегральне відхилення ШТ методом Хілла без маскувальних символів, що дорівнює 27,3 %, а ШТ (шифрований текст) з маскувальними символами дорівнює 19,6 %. Отже, середнє інтегральне відхилення зменшилось в 1,4 разу. $K_{св}$ (коефіцієнт, який залежить від зменшення середнього інтегрального відхилення) можна розрахувати за формулою:

$$K_{св} = 1 – \sigma_1 : \sigma_2,$$

де σ_1 – середнє інтегральне відхилення для методу з маскувальними символами; σ_2 – середнє інтегральне відхилення для методу Хілла, який прийнятий за базовий алгоритм для порівняння;

$$E_4 = K_{св} = 1 – 19{,}6 : 27{,}3 = 1 – 0{,}72 = 0{,}28.$$

Важливо зазначити, що за певних співвідношень σ_1 і σ_2 значення E_4 може бути як додатним, так і від'ємним. Отже, враховується відхилення середньоінтегрального відхилення як в один бік, так і в інший.

E_5 – ймовірність зменшення частоти повторень у шифрованому тексті, які відповідають повторенням відкритого тексту. Для відкритого тексту на k =100 символів біграми можуть трапитися n = 5 раз з ймовірністю γ_1 = 0,5. Для формату 3х3 з використанням маскувальних символів ймовірність визначатиметься такими параметрами:

– δ_1 – ймовірність попадання біграм в аналогічні місця в блоки шифрованого тексту;

– δ_2 – ймовірність ідентичності маскувальних символів у блоках, в яких є біграми відкритого тексту.

δ_1 становить 0,2 – 0,3. δ_2 становить 0,05 – 0,1. E_5 – ефективність від зменшення частоти повторень у шифрованому тексті, визначатиметься формулою:

$$E_5 = 1 – \{(\delta_1 \cdot \delta_2 \cdot \gamma_1 \cdot n) : k\} : \{(\delta_1 \cdot \gamma_1 \cdot n) : k\} = 0,90.$$

Як випливає із формули, значення E_5 може бути як додатним, так і від'ємним. Це не суперечить логіці, тому що за певних обставин можливі як збільшення частоти повторень у шифрованому тексті, так і зменшення. Це допускає і логіка аналізу, і аналітичний вираз для показника E_5.

Числові значення для визначення ефективності можна знайти для конкретного застосування статистичним способом. За алгоритмом побудови виходить, що використання маскувальних елементів істотно зменшує ймовірність повторень у шифрованому тексті порівняно із аналогом. Повторення у шифрованому тексті є важливою особливістю криптографа, який працює над визначенням алгоритму шифрування і ключа шифру.

Для запропонованого компонента безпеки ефективність буде

$$E = (0,5 \cdot E_1 + 0,9 \cdot E_2 + 0,7 \cdot E_3 + 0,6 \cdot E_4 + 0,5 \cdot E_5) : 5 =$$
$$= (0,5 \cdot 0,61 + 0,9 \cdot 0,99 + 0,7 \cdot 0,99 + 0,6 \cdot 0,28 + 0,5 \cdot 0,9) : 5 = 0,5014.$$

Визначимо ефективність для аналогу компонентів безпеки системи захисту інформації, яка побудована з використанням класичного методу шифрування інформації шифром Хілла за тих самих початкових умов.

Розрахунок виконаємо за формулою

$$E_a = (p_{1a} \cdot E_{1a} + p_{2a} \cdot E_{2a} + p_{3a} \cdot E_{3a} + p_{4a} \cdot E_{4a} + p_{5a} \cdot E_{5a}) : 5.$$

Для розрахунку використаємо такі значення рівнів пріоритету замовника (як і для першого випадку): p_{1a} – 0,5, p_{2a} – 0,9, p_{3a} – 0,7, p_{4a} – 0,6, p_{5a} – 0,5.

Для розрахунку надійності використаємо аналогічні підходи і цифрові значення, як і для першого випадку.

$$E_{1a} = (0,4 + 0,4 + 0,5 + 0,7 + 0,7 + 0,8 + 0,8) : 7 = 0,61.$$

Під час розрахунку стійкості криптографічних засобів (E_2) розраховуємо максимальну кількість можливих варіантів ключів. Всі доведення справедливі для першого і другого випадків. Тому вибираємо для другого випадку також максимальний показник E_{2a} – 0,99.

E_{3a} – продуктивність користувача під час роботи із засобами безпеки доволі висока для першого і другого варіантів. Тому цей показник також буде максимальним – 0,99.

E_{4a} – оцінка зменшення середнього інтегрального відхилення частоти вживання символів для другого варіанта дорівнюватиме 0.

$$E_{4a} = 1 – \sigma_1 : \sigma_2 = 1 – 27,3 : 27,3 = 1 – 1 = 0.$$

За базовий варіант приймаємо класичний метод шифрування інформації шифром Хілла, що спричиняє відсутність середнього інтегрального відхилення частоти вживання символів.

E_{5a} – ймовірність зменшення частоти повторень у шифрованому тексті, які відповідають повторенням відкритого тексту. δ_2 – ймовірність ідентичності маскувальних символів у блоках, в яких є біграми відкритого тексту, приймаємо 0.

$$E_{5a} = 1 – \{(\delta_1 \cdot \gamma_1 \cdot n) : k\} : \{(\delta_1 \cdot \gamma_1 \cdot n) : k\} = 1 – 1 = 0.$$

Отже, використання маскувальних символів істотно зменшує ймовірність повторень у шифрованому тексті. Повторення в шифрованому тексті є важливим елементом криптографа, який працює над визначенням алгоритму шифрування і ключа шифру.

Для другого випадку кількісно критерій ефективності становитиме

$$E_a = (0{,}5 \cdot E_{1a} + 0{,}9 \cdot E_{2a} + 0{,}7 \cdot E_{3a} + 0{,}6 \cdot E_{4a} + 0{,}5 \cdot E_{5a}) : 5 =$$
$$= (0{,}5 \cdot 0{,}61 + 0{,}9 \cdot 0{,}99 + 0{,}7 \cdot 0{,}99 + 0{,}6 \cdot 0 + 0{,}5 \cdot 0) : 5 = 0{,}3778.$$

Порівнюючи перший і другий варіанти (методу шифрування з маскувальними елементами і класичний метод шифрування Хілла), отримуємо підвищення ефективності у 1,327 разу, або на 32,7 %. Таке оцінювання істотно підвищує об'єктивність отриманого результату.

Розглянуту методологію можна застосувати для оцінювання узагальненого критерію ефективності компонентів безпеки переважної більшості комп'ютерних систем та мереж.

Висновки

Сучасне оцінювання ефективності компонентів безпеки комп'ютерних систем та мереж. недостатньо забезпечене фундаментальною теорією та методологією і значною мірою суб'єктивне. Запропоновано використання узагальненого критерію ефективності. Розглянуто методологію використання такого критерію на тестовому прикладі для блокових шифрів. Показано, що використання запропонованого узагальненого критерію підвищує об'єктивність оцінювання ефективності компонентів безпеки комп'ютерних систем та мереж. Оцінювання за узагальненим критерієм доцільно застосовувати для компонентів безпеки переважної більшості комп'ютерних систем та мереж. Результати з великою мірою об'єктивності будуть одержані, якщо для різних варіантів реалізації користуватися одним алгоритмом визначення ефективності. В цьому випадку можна побудувати об'єктивний ряд, за числовими значеннями якого можна робити висновки про значення критерію ефективності оцінюваних компонентів безпеки.

1. Verbytskyj O. V. Vstup do kryptologii / O. V. Verbytskyj. – Lviv: Vydavnytstvo naukovo-tehnichnoi literatury, 1998. – P. 248. 2. Viljam S. Kryptografija i zastchita setej: printzypy i praktika, 2-e izd. / Viljam S. – M.: Viljame, 2001. – P. 672. 3. Jemets V. Suchasna kryptografija: osnovni ponjattja / V. Jemets, A. Melnyk, R. Popovych. – Lviv: BAK. – 2003. – P. 144. 4. Ignatovych A. O. Kryterij efektyvnosti dlja vyznachennja stijkosti blokovych schyfriv / A. O. Ignatovych // Visnyk Hmelnytskogo natsionalnogo universytetu, serija: Tehnichni nauky. – 2015. – Vyp. 3. – No. 225. – P. 233–236. 5. Ignatovych A. O. Modeli pidvystchennja efektyvnosti ta nadijnosti blokovych schyfriv / Ignatovych A. O., Pavych N. Ja. // Zbirnyk naukovyh prats. Visnyk Lvivskogo derzhavnogo universytetu bezpeky zhyttjedijalnosti MNS Ukrainy. – 2015, No. 11. – P. 101–110. 6. Ignatovych A. O. Metody schyfruvannja informatsii iz vykorystannjam maskujuchyh symvoliv / A. O. Ignatovych, Ja.S Paramud // Visnyk Natsionalnogo universytetu "Lvivska Politehnika". Zbirnyk naukovyh prats. Serija"Kompjuterni nauky ta informatsijni tehnologii". – 2015. No. 826. – P. 21–27. 7. Patent Ukrainy na korysny model No. 99073, "Sposib schyfruvannja informatsii", zajavka No. a201500619 vid 26.01.2015, Ignatovych A. O., Ivantsiv V. R., Ivantsiv R.-A. D., Pavych N. Ja., opublikovano bjuleten No. 9 vid 12.05.2015 r. 8. Jakymenko I. Z. Analiz efektyvnosti zahystu informatsii na osnovi kryptografichnyh peretvoren z vykorystannjam maskovanogo predstavlennja danych / Jakymenko I. Z., Bozhyk S. V. // ASIT'5. "Suchasni kompjuterni informatsijni tehnologii". TNEU. – Ternopil, 22–23 travnja 2015. – P. 182–184.