УДК 519.87

Д. О. Вадньов, здобувач,
Київський національний університет імені Тараса Шевченка, Київ

ПРО ВИКОРИСТАННЯ ЗАДАЧІ ПРО РЮКЗАК В ЯКОСТІ АЛГОРИТМУ ДЛЯ ШИФРУВАННЯ ДАНИХ

Розглянуто алгоритм шифрування даних на основі задачі про рюкзак. Визначено завдання про підвищення криптостійкості алгоритму. Запропоновано схему шифрування, побудовану з використанням простих чисел та операцій над ними спеціального вигляду. Проілюстровано використання алгоритму та його модифікації на прикладі конкретної текстової послідовності.

Ключові слова: задача про рюкзак, криптостійкість, алгоритм шифрування.

Одним з перших алгоритмів для узагальненого шифрування з відкритим ключем є алгоритм рюкзака, розроблений Ральфом Мерклом та Мартином Хелманом [1]. Даний алгоритм, що отримав назву алгоритму Меркла-Хелмана, спочатку використовувся лише для шифрування, але пізніше Аді Шамір [2] адаптував криптосистему для створення цифрового підпису. Безпека алгоритмів рюкзака зпирається на проблему вирішення задачі про рюкзак, яка є NP-повною проблемою.

Задача про рюкзак нескладна і добре відома. Припускається, що задано множину предметів різної ваги. Необхідно визначити, як можна покласти деякі з цих предметів у рюкзак таким чином, щоб вага рюкзака стала рівною наперед заданому значенню. Більш формально, для заданого набору значень M_1, M_2,….., M_n (n – потужність заданої множини) та величини S потрібно визначити значення b_i, $i = \overline{1,n}$, такі що

$$S = b_1M_1 + b_2M_2 + b_nM_n, \quad (1)$$

де b_i, $i = \overline{1,n}$, може бути або нулем, або одиницею. Одиниця показує, що предмет кладуть в рюкзак, а ноль – що не кладуть.

Наприклад, ваги предметів мають значення 1, 5, 6, 11, 14 та 20. Можна наповнити рюкзак таким чином, щоб його вага стала рівною 22, використавши величини 5, 6 і 11. З іншої сторони, неможливо упакувати рюкзак так, щоб його вага була рівною 24. У загальному випадку час, необхідний для вирішення цієї проблеми, з ростом кількості предметів в наборі росте експоненційно.

В основі алгоритму Меркла-Хелмана лежить ідея шифрувати повідомлення на основі ключа – послідовності ваг задачі про рюкзак (відкритий ключ). Предмети з набору обираються за допомогою блоку відкритого тексту, рівного за довжиною кількості предметів в наборі (біти відкритого тексту відповідають значенням b_i, $i = \overline{1,n}$), а шифротекст є отриманою сумою. Приклад шифротексту, отриманого за допомогою задачі про рюкзак, наведено у табл.1.

***Таблиця* 1**

Відкритий текст	111001	010110	000000	011000
Рюкзак	1 5 6 11 14 20	1 5 6 11 14 20	1 5 6 11 14 20	1 5 6 11 14 20
Шифротекст	1+5+6+20=32	5+11+14=30	0=0	5+6=11

Однак, виявилось, що ця схема є криптографічно нестабільною і, як наслідок, не набула популярності.

В якості суттєвого покращення базового алгоритму Меркла-Хелмана було запропоновано створення закритого ключа, який є перетвореною послідовністю ваг задачі про рюкзак спеціального вигляду. Даний варіант використовувався у двох модифікаціях: однотапній та багатоетапній. Але запропоновані вдосконалення не забезпечили криптостійкості алгоритму. Вперше про його небезпеку було повідомлено у роботі [2]. Більш того, схема алгоритму дозволяє визначити вхідну послідовність без використання будь-якого закритого ключа [3]. Тому зрозуміло, що практично одразу після створення розпочався пошук модифікацій запропонованого алгоритму, що забезпечують підвищений захист від зламу. Для подолання недоліків базової схеми Родні Гудман та Ентоні Маколі [4] розробили процедуру, що базується на модульних рюкзаках. Надалі з'ясувалось, що ця схема також небезпечна. Окрім використання модульних рюкзаків були запропоновані схеми використання інших видів рюкзака. У 1986 році Харальд Нідерайтер [5], опубліковав рюкзачну криптосистему на основі алгебраїчної теорії кодування, яка також була зламана, а у 1988 році Масакацу Морії та Масао Касахара [6] розробили криптосистему з використанням мультиплікативного рюкзака. Ця ідея виявилась вдалою і поки система на мультиплікативних рюкзаках не зламана. Також вдалою виявилась ідея Хусейна Алі Хусейна, Джафара Ваді Абдули Сада та М. Каліфа [7], які у 1991 році запропонували багатоетапну рюкзачну криптосистему. У ній фіксується рюкзачний вектор на кожному етапі, а вихід (зашифроване повідомлення) після кожної стадії алгоритму використовується у якості вхідних даних (тексту) на наступному етапі. Вдалої атаки на дану схему на поточний час невідомо. Продовжилися покращення і класичного алгоритма Меркла-Хелмана.

Підсумовуючи короткий огляд, можна зробити висновок, що, незважаючи на небезпеку алгоритму, варто вивчити його функціонування, тому що на прикладі цього алгоритму можна продемонструвати можливість застосування NP-повної проблеми в криптографії з відкритими та закритими ключами.

Проблеми шифрування на основі задачі про рюкзак. Розглядаючи зміст задачі про рюкзак, можна відмітити, що існує дві різні задачі, одна з яких вирішується за лінійний час, а інша, як вважається, – ні. Просту задачу можна перетворити у складну. Відкритий ключ представляє собою складну (важку) проблему, яку дуже просто можна використати для шифрування, але неможливо для дешифрування повідомлень. Закритий ключ є простою (легкою) проблемою, що надає простий спосіб дешифрування повідомлення. Тим, хто не знає закритий ключ, потрібно спробувати вирішити складну задачу про рюкзак.

Надзростаючі рюкзаки.

Означення. Надзростаючою послідовністю називається послідовність, кожний член якої більше суми усіх попередніх членів.

Наприклад, послідовність {1,3,6,13,27,52} є надзростаючою, а послідовність {1,3,4,9,15,25} – ні. В даному контексті варто згадати і добре відому послідовність чисел Фібоначчі, яка, незважаючи на швидке зростання елементів, не є надзростаючою.

Розглянемо просту проблему рюкзака. Якщо перелік ваг предметів у наборі є надзростаючою послідовністю, то отриману проблему рюкзака можна нескладно вирішити. Розв'язок надзростаючого рюкзака знаходиться наступним чином. Необхідно взяти повну вагу і порівняти його з найбільшим числом послідовності. Якщо повна вага менше цього числа, то його не кладуть у рюкзак. Якщо повна вага більше або рівна цього числа, то воно кладеться у рюкзак. Зменшимо вагу рюкзака на це значення і перейдемо до наступного за величиною числа послідовності. Будемо повторювати ці дії, доки процес не завершиться. Якщо повна вага зменшується до нуля, то розв'язок знайдено. У протилежному випадку – ні.

Покладемо для прикладу, що повна вага рюкзака має бути 70, а надзростаюча послідовність ваг {2,3,6,13,27,52}. Найбільша вага – 52, яка менше 70, тому 52 кладуть у рюкзак. Віднімаючи 52 від 70, отримуємо 18. Наступна вага - 27, більше 18, тому число 27 у рюкзак не кладуть. Наступну вагу 13, яка менше 18, кладуть у рюкзак. Віднімаємо 13 з 18 і отримуємо 5. Чергова вага – 6, більша за 5, не кладеться у рюкзак. Продовжуючи цей процес, отримаємо, що ваги 3 і 2 кладуть у рюкзак, і повна вага зменшується до 0, що свідчить про знайдений розв'язок. Якщо розглядати цю процедуру як блок шифрування методом рюкзака Меркла-Хелмана, відкритий текст, отриманий із значення шифротексту 70, був би рівний 110101.

Пошук заповнення нормальних рюкзаків послідовностями, які не є надзростаючими, представляють собою складну проблему. Швидкого алгоритму для вирішення даної задачі в реальному часу поки не знайдено. Єдиним відомим способом визначити, які предмети упаковано у рюкзаку, є методична перевірка можливих розв'язків до знаходження вірного. Найшвидкіший алгоритм, приймаючи до уваги різні евристики, має експоненційну залежність від кількості можливих предметів. Тому, якщо додати до послідовності ваг лише один елемент, знаходження розв'язку задачі стає вдвічі складніше. Це набагато важче надзростаючого рюкзака, в якому, якщо додати один предмет до послідовності, складність пошуку розв'язку зростає на одну операцію.

Алгоритм Меркла-Хелмана базується на цій властивості. Закритий ключ є послідовністю ваг задачі надзростаючого рюкзака. Відкритий ключ – це послідовність ваг проблеми нормального рюкзака з тим самим розв'язком. Р. Меркл та М. Хелман [1], застосовуючи цілочислову арифметику, розробили спосіб перетворення проблеми надзростаючого рюкзака в проблему нормального рюкзака.

Створення відкритого ключа з закритого. Розглянемо роботу алгоритму, не заглиблюючись в теорію чисел. Для отримання нормальної послідовності рюкзака візьмемо надзростаючу послідовність рюкзака, наприклад наведену раніше $\hat{E}$ ={2,3,6,13,27,52}, і домножимо всі значення на число $\grave{O}$ за модулем N. Значення модуля повинно бути більше суми всіх чисел послідовности, тобто утворювати з заданою послідовністю надзростаючу послідовність. Оберемо, наприклад, N =105. Множник $\grave{O}$ повинен бути взаємно простим числом з модулем N, тобто НСД (N ,T) =1. Покладемо, наприклад, $\grave{O}$ =31. Нормальною послідовністю рюкзака у цьому випадку буде {62,93,81,88,102,37}, де 62=2*31 mod 105; 93=3*31 mod 105; 81=6*31 mod 105; 88=13*31 mod 105 ; 102=27*31 mod 105 ; 37=52*31 mod 105.

Надзростаюча послідовність рюкзака разом з числами N та T {2,3,6,13,27,52; 105, 31} є закритим ключем, а нормальна послідовність рюкзака {62,93,81,88,102,37} – відкритим.

Шифрування. Для шифрування повідомлення розбивається на блоки, що за довжиною дорівнюють кількості елементів послідовності рюкзака. Далі, вважаючи, що одиниця відповідає присутності члена послідовності, а ноль - його відсутності, обчислюємо повні ваги рюкзаків - по одному для кожного блоку повідомлень.

Якщо припустити, що повідомлення у бінарному вигляді подається як 011000110101101110, то шифрування, яке використовує попередню послідовність рюкзака, буде здійснюватися таким чином:

Вхідне повідомлення у блочному вигляді = 011000 110101 101110, звідки

011000 відповідає числу 93 + 81 = 174;

110101 відповідає числу 62 + 93 + 88 + 37 = 280;

101110 відповідає числу 62 + 81 + 88 + 102 = 333.

У результаті шифротекстом повідомлення 011000110101101110 є числова послідовність 174,280,333.

Дешифрування. Законний отримувач даного повідомлення знає закритий ключ: оригінальну надзростаючу послідовність, а також значення N та T , які використовувалися для перетворення її в нормальну послідовність рюкзака. Для дешифрування повідомлення отримувач визначає мультиплікативне обенене T^{-1}, таке що $T*(T^{-1}) \pmod{N}$ = 1. Кожне значення шифротексту домножується на $T^{-1} \bmod N$, а потім розгортається в суму за допомогою закритого ключа, щоб отримати значення відкритого тексту.

У нашому прикладі надзростаюча послідовність {2,3,6,13,27,52}, N = 105, T = 31. Шифротекстом є послідовність 174,280,333. У цьому випадку T^{-1} дорівнює 61 (31*61 mod 105=1891 mod 105=1), тому значення шифротексту домножуються на величину 61 mod 105.

Маємо 174*61 mod 105 = 9 = 3 + 6, що відповідає 011000;

280*61 mod 105 = 70 = 2 + 3 + 13 + 52, що відповідає 110101;

333*61 mod 105 = 48 = 2 + 6 + 13 + 27, що відповідає 101110.

Розшифрованим відкритим текстом є бінарні послідовності 011000 110101 101110, що повністю відповідає вхідному повідомленню.

Підвищення крипостійкості алгоритму шифрування. Сучасні дослідження по вдосконаленню алгоритму здійснюються за двома основними напрямками. Перший з них об'єднує роботи, що спрямовано на використання різних варіантів задачі про рюкзак. Інший напрямок досліджує застосування різних додаткових схем та процедур, що підвищують захищеність алгоритму.

Запропонуємо модифікацію базової схеми на основі нечіткого підходу [8] та послідовностей простих чисел спеціального вигляду.

Позначимо, $P_k(a)$ – k-те просте число, що не менше цілого $a \geq 0$, $k = 0,1,2,...$.

Нескладно перевірити, що

1) $P_0(0)=0$, $P_0(1)=1$, $P_1(0)=1$;

2) $P_k(a)=P_1(P_{k-1}(a))=...=P_{k-1}(P_1(a))$, $k=1,2,3,...$, $a\geq 0$;

3) $P_k(a)\leq P_l(a)$ для будь-яких $k\leq l$, $k=0,1,2,...$, $l=0,1,2,3,...$, $a\geq 0$.

Крім традиційних арифметичних операцій додавання, віднімання, множення та ділення, на послідовності чисел $P_k(a)$, $a\geq 0$, $k=0,1,2,...$, введемо операцію зсуву на m, $m\in N\cup\{0\}$, простих чисел у вигляді

$$P_k(a)\oplus m=P_{k+m}(a)=P_m(P_k(a)), \tag{2}$$

яка не виводить за межі заданої послідовності, та операцію p - кратної композиції ($p\in N$) відношення двох чисел $P_k(a)$ та $P_l(a)$, $k=0,1,2,...$, $l=0,1,2,3,...$, у вигляді

$$P_k(a)\big/P_l(a)\circ p=P_k(a)\oplus p\big/P_l(a)\oplus p=P_{k+p}(a)\big/P_{l+p}(a)=P_p(P_k(a))\big/P_p(P_l(a)). \tag{3}$$

Числа, що входять до відкритого ключа $K=\{r_1,...,r_n\}$, є довільними цілими числами. Традиційне поняття нечіткості [8], яке визначає міру належності конкретного числового значення до нечіткої множини, в даному випадку може інтерпретуватися як рівень складності кодування кожного числа $r_j\in K, j=\overline{1,n}$.

Для визначення величини складності доповнимо відкритий ключ двома довільними значеннями k та l, $k\leq l$, $k=0,1,2,...$, $l=1,2,3,...$, за якими з послідовності простих чисел визначаються величини $s=P_k(a)$, $q=P_l(a)$ для деякого числа $a\geq 0$. За таких умов отримуємо, що $0\leq s/q\leq 1$. Ця величина може служити показником складності кодування, а за допомогою значень s та q можна змінити ваги відкритого ключа K та величини N та T, наприклад, за наступною схемою:

- для чисел T та N, які є взаємно простими числами, обчислюються числа $P_s(T)$ та $P_q(N)$ відповідно, де $s=P_k(a)$, $q=P_l(a)$;
- для цілих чисел $r_j\in K, j=\overline{1,n}$, які входять до ключа K, обчислюються величини $u_j=P_s(r_j)-r_j$ та $v_j=P_q(r_j)$, $j=\overline{1,n}$, $s=P_k(a)$, $q=P_l(a)$;
- формується вектор пар елементів $\bar{K}=\{(u_1,v_1),...,(u_n,v_n)\}$, який буде новим значенням відкритого ключа *K*. Величини $P_s(T)$, $P_q(N)$ та вектор $\bar{K}$ передаються отримувачу разом з зашифрованим за допомогою елементів v_j, $j=\overline{1,n}$, повідомленням.

Зрозуміло, що дана схема допускає різні модифікації. В якості основних можна розглядати:

- схему з кодуванням лише чисел N та T,
- паралельне кодування чисел N, T та чисел ключа K,
- послідовне кодування чисел N та T у числа $P_s(T)$ та $P_q(N)$, відповідно, з подальшим перетворенням елементів ключа $K=\{r_1,...,r_n\}$ за традиційною процедурою $r_j * P_s(T) \bmod P_q(N)$, $j=\overline{1,n}$, $s=P_k(a)$, $q=P_l(a)$ і кодуванням отриманих значень вектором пар елементів $\bar{K}=\{(u_1,v_1),...,(u_n,v_n)\}$.

Іншою важливою рисою запропонованої схеми є можливість динамічно змінювати значення $s=P_k(a)$ і $q=P_l(a)$. Використовуючи операцію зсуву для зміни чисел s та q, у вхідній ключовій послідовності задається величина зсуву m, $m\in N\cup\{0\}$, яка дозволяє обчислити нові прості числа $P_k(a)\oplus m$ та $P_l(a)\oplus m$ за формулою (2). Отримані значення можна розглядати як нові параметри процедур шифрування та дешифрування текстових повідомлень.

Для демонстрації дії розробленої схеми повернемося до наведеного вище прикладу. Покладемо a =1. Припустимо, що k =4, l =7. Відповідні прості числа s =7, q =17. Для елементів відкритого ключа *K*={62,93,81,88,102,37} та величин N =105, T =31 обчислимо відповідні значення u_1 =35, v_1=149, u_2 =34, v_2 =179, u_3 =28, v_3 =167, u_4 =25, v_4 =173, u_5 =35, v_5 =191, u_6 =30, v_6 =109, $P_7(31)$ =61, $P_{17}(105)$ =193. Тоді новим відкритим ключем буде множина пар значень $\bar{K}=\{(35,149),(34,179),(28,167),(25,173),(35,191),(30,109)\}$. Величини $P_s(T)$ =61 та $P_q(N)$ =193 є зашифрованими значеннями T =31, N =105. При цьому необхідно відмітити, що усі отримані значення нескладно дешифруються у попередній стан за допомогою простих чисел s =7, q =17.

Зашифровані елементи вхідного повідомлення 011000 110101 101110 з новим відкритим ключем будуть мати вигляд:

011000 задається числом 179 + 167 = 346;
110101 задається числом 149 + 179 + 173 + 109 = 610;
101110 задається числом 149 + 167 + 173 + 191 = 680,

а шифротекстом повідомлення 011000110101101110 є числова послідовність 346,610,680.

Запропонований підхід дозволяє ускладнити процедуру шифрування вхідних повідомлень, що збільшує криптостійкість алгоритму Меркла-Хелмана.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ralph Merkle, Martin Hellman. Hiding information and signatures in trapdoor knapsacks // IEEE Trans. Information Theory. – 1978. – V.24(5) – P.525–530.
2. Adi Shamir. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem// CRYPTO-1982. – P.279–288.
3. Ernest F. Brickell. Breaking iterated knapsacks / G. R. Blakley, David C. Chaum. Advances in cryptology// Lecture Notes in Computer Science. CRYPTO-1984. – Springer, Berlin, 1985. – V. 196. – P. 342–358.

4. Rodney M. F. Goodman, A. J. McAuley. New trapdoor-knapsack public-key cryptosystem// IEE Proceedings, 1985. – V. 132, Pt. E. – № 6. – P. 289–292.
5. Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory// Problems of Control and Information Theory, 1986. – V. 15. – P. 159–166.
6. Masakatu Morii, Masao Kasahara. New public key cryptosystem using discrete logarithm over GF(p)// IEICE Transactions, 1988. – V. J71-D. – № 02. – P. 448–453.
7. Hussain Ali Hussain, Jafar Wadi Abdul Sada, Saad M. Kalipha. New multistage knapsack public-key cryptosystem// International Journal of Systems Science, 1991. – V. 22. – №11. – P. 2313–2320. 8. Zadeh L.A. Fuzzy sets // Inf. Contr., 1965. – V.8. – P. 338–353.

Надійшла до редколегії 25.08.14

Ваднев Д. А., соискатель,
Киевский национальный университет имени Тараса Шевченко, Киев

ОБ ИСПОЛЬЗОВАНИИ ЗАДАЧИ О РЮКЗАКЕ В КАЧЕСТВЕ АЛГОРИТМА ДЛЯ ШИФРОВАНИЯ ДАННЫХ

Рассмотрен алгоритм шифрования данных на основе задачи о рюкзаке. Сформулирована задача повышения криптоустойчивости алгоритма. Предложена схема шифрования, построенная с использованием простых чисел и операций над ними специального вида. Проиллюстрирована работа алгоритма и его модификации на примере конкретной текстовой последовательности.

Ключевые слова: задача о рюкзаке, криптоустойчивочть, алгоритм шифрования.

Vadnev D.A., researcher,
Taras Shevchenko National University of Kyiv

ON THE USE KNAPSACK PROBLEM AS ALGORITHM FOR DATA ENCRYPTION

In this paper a data encryption algorithm based on the problem of the knapsack is considered. The problem of algorithm's crypto resistance increasing is defined. It is proposed an encryption scheme, based on the use of prime numbers and operations on them by special form. The use of the algorithm and its modifications are illustrated on the test example of a text sequence.

Key words: knapsack problem, algorithm's crypto resistance, encryption algorithm.

УДК 517.929.4

Гаркуша Н. І., канд. екон. наук
Київський університет імені Тараса Шевченка, Київ

ДИНАМІКА ОДНІЄЇ ЕКОЛОГІЧНОЇ МОДЕЛІ "ХИЖАК-ЖЕРТВА" БЕЗ ВРАХУВАННЯ ВІКОВОЇ СТРУКТУРИ

Розглядається математична модель екології, що описує ріст популяції і взаємодії хижак-жертва. Модель представлена системою двох нелінійних диференціальних рівнянь із запізненням, що визначає час статевого дозрівання популяції. Одержано умови, при виконанні яких рівноважний стан кількості хижаків і жертв є стійким.

Ключові слова: система диференціальних рівнянь, положення рівноваги, запізнення, стійкість.

Екологія – це наука, що вивчає умови існування живих організмів у взаємозв'язку між організмами і середовищем, в якому вони мешкають. Спочатку екологія розвивалася як складова частина біологічної науки в тісному зв'язку з іншими природничими науками [1,2]. Головний об'єкт екології – екосистеми, що представляють собою єдині комплекси, утворені живими організмами і середовищем їх проживання. Крім того, в область її досліджень входить вивчення окремих видів організмів, їх популяцій, тобто сукупностей особин одного виду, біотичних співтовариств, тобто сукупностей популяцій і біосфери в цілому. В даний час екологія вийшла за рамки суто біологічної науки і перетворилася на міждисциплінарну науку, що вивчає найскладніші проблеми взаємодії людини з навколишнім середовищем.

Одними із завдань екологічної науки є:

- розробка теорії і методів оцінки стійкості екологічних систем всіх рівнів;
- дослідження проблем популяційної екології, екології біотичних співтовариств, збереження біорізноманіття в природі, регулюючого впливу біоти на навколишнє середовище;
- оцінка стану і динаміки природних ресурсів та екологічних наслідків їх споживання;
- розробка і вдосконалення методів управління якістю навколишнього середовища.

Дана робота присвячена розробці та аналізу математичних моделей динаміки екологічних процесів з використанням різницевих, диференційно-різницевих рівнянь з післядією. Крім того, в ній розглядаються питання дослідження стійкості та одержання оцінок збіжності усталених режимів досліджуваних моделей екології, стабілізації положень рівноваги систем, описуваних рівняннями з післядією [3,4].

1. Модель взаємодії популяцій. В роботі розглядається математична модель росту популяції і взаємодії "хижак-жертва" з наступними припущеннями [5, стор.29].

1. Щільність даного виду, тобто число особин на одиницю площі, може бути повністю описана за допомогою однієї змінної, тобто нехтуємо віковими, статевими та генетичними відмінностями.
2. Зміни щільності можуть бути адекватно описані детерміністськими рівняннями.
3. Результати взаємодії в межах виду і між видами відбуваються миттєво.

Тоді модель може бути представлена системою двох диференціальних рівнянь виду [5, стор.38]

$$\dot{x}(t) = ax(t) - bx^2(t) - cx(t)y(t), \quad \dot{y}(t) = ey(t) - f\frac{y^2(t)}{x(t)}.$$

Або у вигляді "з виділеною квазілінійною частиною"

$$\dot{x}(t) = \left[a - bx(t) - cy(t)\right]x(t), \quad \dot{y}(t) = \left[e - f\frac{y(t)}{x(t)}\right]y(t). \qquad (1.1)$$

Рівняння для жертви ідентично для рівняння В. Вольтера з демпфуючим елементом. Рівняння для "хижака" подібно до логістичного рівняння, але другий член змінений, щоб враховувати щільність "жертви".