УДК 025.7/19
© Ю. Наконечний[1], П. Гаранюк[1], Т. Луковський[1], Я. Кавин[2], 2012

ЕФЕКТИВНІСТЬ РЕАЛІЗАЦІЇ НЕЙРОМЕРЕЖЕВОЇ ТЕХНОЛОГІЇ ЗАХИСТУ БЛАНКІВ ЦІННИХ ПАПЕРІВ

Проведений аналіз моделі для реалізації нейромережевої технології захисту бланків цінних паперів яка містить базові компоненти симетричної системи шифрування, що використовується для збереження конфіденційності інформації в секретних системах.

The analysis of the model for realization of fuzzy-logic technology of forms deence of securities papers have been conducted, the model contains base components of the enciphering of symmetric system used for maintenance of information confidentiality in the secret systems.

1. ВСТУП

При детальному аналізі систем передачі інформації (систем зв'язку) та систем криптографічного захисту (секретних систем), прослідковується низка аналогій, що дозволяє ототожнювати розглянуті системи. Зокрема, розглянувши принцип впливу завад в каналі зв'язку на інформацію та дію алгоритму шифрування на повідомлення, можна стверджувати, за Шенноном, про шифртекст як аналог спотвореного сигналу. Проте, дані системи мають ряд розбіжностей, що полягають у складності процесу шифрування, природі ключа та спеціалізованому захисті характеристик інформації.

Розглянемо структуру секретної системи (рис.1.1) для обґрунтування розробленого алгоритму шифрування, що базується на поєднанні основ процесу шифрування та принципів навчання нейронної мережі.

Секретна система визначається абстрактно як деяка множина відображень одного простору (множини можливих повідомлень) в інший простір (множину можливих шифртекстів). Кожне відображення з цієї множини відповідає способу шифрування за допомогою ключа.

[1] Національний унівеситет «Львівська політехніка»
[2] Українська академія друкарства

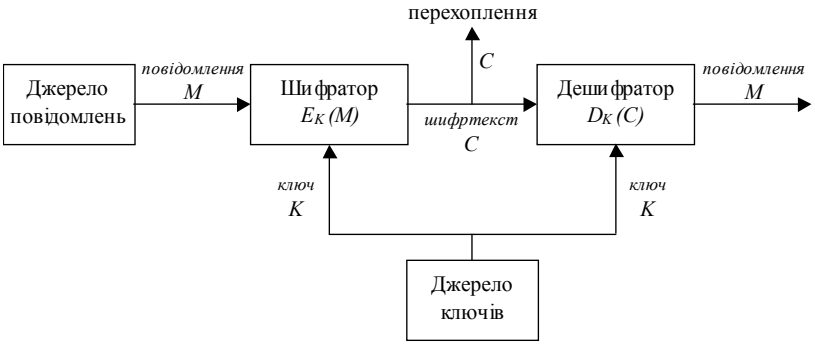

Рис. 1. Схема загальної секретної системи

Для функціонування секретної системи (згідно рис.1) обирається деякий ключ для шифратора/дешифратора. Вибір ключа визначає певне відображення з множини відображень (алгоритм шифрування), що складають систему. Вибирається повідомлення і за допомогою вибраного відображення формується відповідний шифртекст. Цей шифртекст передається по каналу зв'язку та може бути перехоплений. Після передачі за допомогою оберненого відображення з шифртексту відновлюється початкове повідомлення.

Секретна система оперує наступними об'єктами:

Алфавіт A, в якому записуються повідомлення (відкриті тексти). Повідомлення M є словом в цьому алфавіті (яке може складатись з багатьох слів у звичайному лінгвістичному розумінні), тобто $M \in A^*$, де A^* – простір повідомлень.

Алфавіт B, в якому записуються шифртексти. Відповідно, $C \in B^*$, де C – шифртекст, B^* – простір шифртекстів.

Простір ключів K^*, що складається із слів деякого алфавіту.

Шифруюче відображення $E_K : A^* \to B^*$, $K \in K^*$ відбувається за допомогою базових операцій над відкритим текстом: підстановки, перестановки, циклічного зсуву, додавання та множення за модулем, причому послідовність таких операцій становить алгоритм шифрування.

Дешифруюче відображення $D_K : B^* \to A^*$, $K \in K^*$ перетворює шифртекст у вихідний відкритий текст.

В схемі секретної системи припускається, що відображення є взаємно–однозначними для одержання єдиного результату шифруван-

ня/дешифрування. Також відображення повинні задовольняти наступній рівності:

$$D(K, E(K, M)) = M, \ \forall M \in A^*, \ K \in K^*$$

Таку властивість можна сформулювати іншим чином: відображення $D_K : B^* \to A^*$ є оберненим зліва до відображення $E_K : A^* \to B^*$. З теореми про обернене відображення отримаємо умову ін'єктивності E_K, яка рівнозначна можливості дешифрування. І навпаки, на підставі тієї ж теореми довільна родина ін'єктивних відображень $\{E_K : A^* \to B^*\}_{K \in K^*}$ може розглядатись як шифруюча в тому плані, що для них існують обернені зліва відображення $\{D_K : B^* \to A^*\}_{K \in K^*}$, які можуть вважатись дешифруючими.

Шифруюче відображення, крім ін'єктивності може також володіти і сюр'єктивністю, коли дешифруюче відображення є оберненим до E_K також і справа. Тобто, в такому випадку E_K та D_K представляються взаємно оберненими:

$$D(K, E(K, M)) = E(K, D(K, M)) = M.$$

Зазначимо, що коли елементи A та Q належать одному алфавіту, згадані вище відображення називаються *моноалфавітними*, в протилежному випадку – *поліалфавітними*. Якщо E_K та D_K реалізуються алгоритмами шифрування із високими показниками швидкодії, система вважається *ефективною*.

2. АНАЛІЗ ШИФРУЮЧОГО ПЕРЕТВОРЕННЯ

Актуальним практичним питанням на всьому етапі розвитку криптографії було створення *абсолютно стійких* (або досконалих) шифрів. Основні вимоги, які висуваються до досконалого шифру, полягають в забезпеченні неможливості успішного криптоаналізу.

На сьогоднішній день відомим абсолютно стійким шифром можна вважати шифр Вернама (або шифр одноразового блокноту). Проте, практична реалізація цього шифру ускладнюється внаслідок ідентичності довжин ключа та відкритого тексту; відповідно із збільшенням об'єму вихідної інформації збільшується розмір ключа. Необхідно зазначити, що в основі стійкості шифру Вернама лежить принцип, який був пізніше формально доведений Шенноном .

Для детального обґрунтування визначення стійкості шифру введемо поняття невизначеності повідомлення.

Нехай можливо відправити q_0 – повідомлень. Тоді мірою невизначеності довільного повідомлення є величина

$$H(M) = -\sum_{i=1}^{q_0} p_i^0 \log_2 p_i^0 ,$$

де p_i^0 – імовірність відправлення *i*–го повідомлення. Фізичний зміст даної величини полягає в необхідній кількості інформації для усунення невизначеності .

Якщо, крім розміру повідомлення *l*, ніякої апріорної інформації про повідомлення не існує, то всі можливі з 2^l варіантів вважаються рівноімовірними і тоді

$$H(M) = -2^l \cdot 2^{-l} \cdot \log_2 \left(2^{-l}\right) = l = |M| .$$

Після перехоплення шифртексту міра невизначеності стає апостеріорною умовною невизначеністю:

$$H(M) = -\sum_{i=1}^{q_0} p(M_i|C) \log_2 p(M_i|C).$$

Одною з найважливіших характеристик якості шифру є кількість інформації про вихідний текст:

$$I = H(M) - H(M|C).$$

Зауважимо, що для абсолютно стійкого шифру виконується $I = 0$. При доведенні існування досконалих шифрів, Шенноном була одержана необхідна умова абсолютної стійкості:

$$H(E) \geq H(M),$$

де $H(E)$ – невизначеність алгоритму шифрування, що має зміст тільки для імовірнісних систем шифрування. Якщо шифр повністю невизначений для криптоаналітика, то $H(E) = \infty$, тобто виконується умова (1.1).

Отже, надійність шифру залежить виключно від його секретності і не залежить від інших властивостей. З другого боку, аналіз практичних досліджень показав неможливість забезпечення абсолютної стійкості шифру, тому до сьогоднішнього часу використовують принципи наближення до абсолютної стійкості.

Загалом шифр, наближений до досконалого, повинен задовольняти наступним вимогам:

– криптоаналіз зашифрованих даних не повинен давати жодних відомостей про внутрішню будову шифру (статистичні закономірності в шифртексті не повинні прослідковуватись);

– алгоритм має передбачати можливість перебудови (якщо опис алгоритму, програмна чи апаратна реалізація стануть загальновідомими, тоді в алгоритмі шифрування необхідно буде замінити тільки параметри).

Дотримання цих вимог зробило можливим поява правила Кірхгофа, яке стало загальноприйнятим при створенні сучасних надійних шифрів. Даний принцип полягає у визначенні шифру як параметризованого алгоритму, що складається з процедурної частини та параметрів. Процедурна частина містить опис шифрування і порядок виконання операцій над даними, причому розкриття цієї частини не повинно впливати на секретність шифру. Параметри містять елементи даних, що використовуються при криптографічних перетвореннях. Оскільки секретність процедурної частини шифру не вимагається, то таємницю мають становити тільки параметри, а саме ключ шифру.

Використання правила Кірхгофа дозволяє отримати наступні переваги при побудові шифрів:

– розповсюдження конкретного шифру (алгоритму і ключа) не приводить до необхідності повної заміни реалізації всього алгоритму, достатньо замінити лише ключ;

– ключі можна зберігати окремо від решти компонентів системи шифрування та використовувати по потребі і тільки на час шифрування – це підвищує надійність системи загалом;

з'являється можливість для точної оцінки стійкості алгоритму шифрування, яка дорівнює невизначеності ключа, що використовується:

$$H(E_K) = H(K).$$

Оскільки максимально можлива невизначеність блоку даних фіксованого розміру досягається при рівноімовірних значеннях цього блоку і дорівнює його розміру, то невизначеність ключа не перевищує його довжини:

$$H(K) \le |K|.$$

З врахуванням сказаного вище, одержується необхідна умова абсолютної стійкості для шифрів, що задовольняють правилу Кірхгофа

$$|K| \ge H(K) = H(E_K) = H(E) \ge H(M) = |M|.$$

В основу сучасного розвитку алгоритмів шифрування покладений розглянутий принцип обмеженої секретності, згідно з яким цінність представляє тільки ключ, за допомогою якого відбувається перетворення вихідної інформації. З другого боку, з умови абсолютної стійкості шифрів випливає необхідність наближення довжини ключа до розмірності вихідного тексту, що в свою чергу спричиняє погіршення умов реалізації. Поява систем шифрування з відкритим ключем вирішила тільки задачу забезпечення секретності ключа (шляхом викорис-

тання важкооборотних функцій для розділення ключа на відкритий та секретний).

Отже, збільшення розмірності ключа наближає шифр до абсолютно стійкого, одночасно ускладнюючи виконання правила Кірхгофа для нього та обмежуючи практичну реалізацію.

З появою алгоритмів шифрування з відкритим ключем набуло актуальності питання оцінки переваг та недоліків двох типів алгоритмів з метою визначення більш ефективного. Необхідно зазначити, що доцільність та ефективність використання того чи іншого алгоритму повністю визначається задачею, яку необхідно розв'язати. Якщо використати критерії оцінки якості алгоритму шифрування, попередньо наведені, та дані з табл. 1 і табл. 2, можна зробити висновок, що великий об'єм ключової інформації, необхідний для асиметричного шифрування, наближається до критерію стійкості в обчислювальному сенсі, одночасно ускладнюючи та уповільнюючи сам процес шифрування.

Таблиця 1

Еквівалентність довжин ключів симетричного та асиметричного шифрування

Довжина секретного ключа (біт)	Довжина відкритого ключа (біт)
56	384
64	512
80	768
112	1792
128	2304

Збільшення обсягів ключової інформації також призводить до істотного зростання об'єму шифртексту. З невирішених проблем асиметричного шифрування, як порівняно нової галузі, можна виділити задачу управління відкритим ключем, враховуючи численні недоліки існуючих засобів її вирішення.

Сучасні дослідження стійкості алгоритмів шифрування показали, що великі обсяги ключової інформації, які виступають перевагою асиметричних алгоритмів, не гарантують їм стійкості у випадках довгострокового зберігання конфіденційної інформації. *На сьогоднішній день довжина ключа для забезпечення адекватного захисту не повинна бути менше 75 бітів з подальшим* збільшенням *до 90 бітів впродовж ближніх 20 років.*

Таблиця 2

Швидкодія процесу повного перебору ключів спеціальними апаратними (1) та програмними (2) засобами

Роки	Довжина ключа в бітах							
	40		56		64		128	
	1	2	1	2	1	2	1	2
1995	0,2 с.	33 хв.	3,6 год.	3 р.	38 дн.	10^3 р.	10^{18} р.	10^{22} р.
2000	0,02 с.	3,3 хв.	21 хв.	115 дн.	4 дн.	100 р.	10^{17} р.	10^{21} р.
2005	2 мс.	20 с.	2 хв.	15 дн.	9 год.	10 р.	10^{16} р.	10^{20} р.
2010	0,2 мс.	2 с.	13 с.	1,5 дн.	1 год.	1 р.	10^{15} р.	10^{19} р.
2015	0,02 мс.	0,2 с.	1 с.	3,6 год.	5,5 хв.	38 дн.	10^{14} р.	10^{18} р.
2020	2 мкс.	0,02 с.	0,1 с.	21 хв.	33 с.	4 дн.	10^{13} р.	10^{17} р.
2025	0,2 мкс.	2 мс.	0,01 с.	2 хв.	3 с.	9 год.	10^{12} р.	10^{16} р.
2030	0,02 мкс.	0,2 мс.	1 мс.	13 с.	0,3 с.	1 год.	10^{11} р.	10^{15} р.

Якщо припустити, що оптимальним методом атаки на алгоритм шифрування буде метод прямого перебору всіх можливих ключів, то його швидкодія буде повністю визначатись довжиною ключа та потужністю обчислювальних засобів. Враховуючи тенденцію стрімкого зростання потужності комп'ютерних технологій, можна припустити, що оптимальне дешифрування перехопленого повідомлення необхідно починати в момент, коли часові затрати на нього будуть мінімальними.

Тобто, стійкість алгоритмів шифрування, які проектуються та існуючі можна оцінювати за новим об'єктивним критерієм.

Нехай $x(t)$ – неперервна функція, що показує швидкодію обчислювальних засобів в момент часу *t*. Виходячи з припущення, що потужність комп'ютерних технології зростає в 10 разів за кожні 5 років та взявши за початкову точку відліку 1946 рік (поява першого комп'ютера, $t = 0$), функція виглядає наступним чином $x(t) = C_0 \cdot 10^{t/5}$, де $C_0 = 100$ – потужність першого комп'ютера.

Робоча модель для розрахунку часу життя ключа складається з двох діючих факторів: моменту початку дешифрування та складності дешифрування. Мінімум цієї функції будемо називати максимальним часом життя

$$t_{\max} = \left[t + \frac{\left| K^* \right|}{2 \cdot x(t) \cdot C_1} \right] \to \min ,$$

де $\left|K^*\right|$ – потужність множини ключів; $C_1 = 31\ 536\ 000$ – коефіцієнт для переходу від операцій/секунду до операцій/рік.

В результаті розв'язку та спрощення отримаємо значення моменту часу t_{op} , в якому досягається мінімум функції $t_{\max}$:

$$t_{op} = 5 \lg \left[\frac{\left|K^*\right| \cdot \ln(10)}{10 \cdot C_1} \right].$$

Величина t_{op} визначає оптимальний момент початку дешифрування перехопленого повідомлення та фактично служить показником завершення життєвого циклу ключа.

3. ВИСНОВОК

Симетричні криптографічні системи володіють рядом переваг в порівнянні із несиметричними, такі як можливість довгострокового збереження інформації, що представляє собою актуальне питання для сучасних систем документообігу, зокрема при оперуванні цінними паперами. Аналіз структури та дослідження процесів навчання нейромереж показали нові можливості для захисту інформації і стали основою нового алгоритму шифрування.

1. Вербіцький О.В. Вступ до криптології.– Львів: В–во наук.–техн. літ–ри, 1998.– 247с. 2. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах.– К.: Корнейчук, 2000.– 152 с. 3. Grzywak A. Bezpieczenstwo systemow komputerowych.– Gliwice: Wydawnictwo pracowni komputerowej jacka skalmierkiego, 2000.– 326p. 4. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C.– New York: 2d ed., John Wiley&Sons Inc., 1996.– 675p. 5. Грицик В.В., Томашевський О.М. Нейромережевий підхід до забезпечення захисту інформації з високими показниками завадостійкості при передачі // Доповіді Національної академії України.– 2003.– №3.– С.62–68. 6. Hrytsyk V.V., Aizenberg N.N., Tkachenko R.O. and other. The neural and neural–like networks: synthesis, realization, application and future // Інформаційні технології і системи.– 1998.– №1/2.– С.15–55. 7. Ткаченко Р.О. Неітераційне навчання штучних нейронних мереж прямого поширення // Технічні вісті.– 1999.– №1(8), 2(9).– С.41–42. 8. Томашевський О.М. Нейромережева криптосистема з таємним ключем // Інформаційні технології і системи.– 1999.– Т.2, №1.– С.143–150. 9. Томашевський О. Захист середовища передачі даних в оперативному поліграфічному комплексі // Комп'ютерні технології друкарства.– Зб. наукових праць. - №5.– Львів: УАД. - С.368–375.